ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Φωτονικές Τεχνολογίες Για Την Ασφαλή Διαχείριση Δεδομένων

Μαριαλένα Ακριώτου

Η παρούσα διδακτορική διατριβή υλοποιήθηκε με υποτροφία του ΙΚΥ η οποία χρηματοδοτήθηκε από την Πράξη «Ενίσχυση του ανθρώπινου ερευνητικού δυναμικού μέσω της υλοποίησης διδακτορικής έρευνας» από πόρους του ΕΠ «Ανάπτυξη Ανθρώπινου Δυναμικού, Εκπαίδευση και Δια Βίου Μάθηση», 2014 - 2020 με την συγχρηματοδότηση του Ευρωπαϊκού Κοινωνικού Ταμείου (Ε.Κ.Τ) και του Ελληνικού Δημοσίου»

ΑΘΗΝΑ

ΔΕΚΕΜΒΡΙΟΣ 2023

NATIONAL AND KAPODISTRIAN UNIVERSITY OF ATHENS

SCHOOL OF SCIENCES
DEPARTMENT OF INFORMATICS AND TELECOMMUNICATIONS

PROGRAM OF POSTGRADUATE STUDIES

PhD THESIS

Photonic Technologies For Secure Data Management

Marialena Akriotou

This PhD was implemented by scholarship from the IKY (State Scholarships Foundation) act "Reinforcement of research potential through doctoral research", funded by the Operational Programme "Human Resources Development, Education and Lifelong Learning", 2014-2020, co-financed by the European Union and Greek state funds.

ATHENS

DECEMBER 2023

ΔΙΔΑΚΤΟΡΙΚΗ ΔΙΑΤΡΙΒΗ

Φωτονικές τεχνολογίες για την ασφαλή διαχείριση δεδομένων

Μαριαλένα Ακριώτου

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Δημήτριος Συβρίδης, Καθηγητής ΕΚΠΑ

ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ:

Δημήτριος Συβρίδης, Καθηγητής ΕΚΠΑ
Αγγελική Αραπογιάννη, Καθηγήτρια ΕΚΠΑ
Παναγιώτης Ριζομυλιώτης, Αναπληρωτής Καθηγητής Χαροκόπειου Πανεπιστημίου

ΕΠΤΑΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Δημήτριος Συβρίδης,
Καθηγητής ΕΚΠΑ

Αγγελική Αραπογιάννη,
Καθηγήτρια ΕΚΠΑ

Παναγιώτης Ριζομυλιώτης
Αναπληρωτής Καθηγητής Χαροκόπειου

Ιωάννης Σταυρακάκης,
Καθηγητής ΕΚΠΑ

Κωνσταντίνος Χατζηκοκολάκης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Ιωάννης Παναγάκης,
Αναπληρωτής Καθηγητής ΕΚΠΑ

Έκτορας Νισταζάκης,
Καθηγητής ΕΚΠΑ

Ημερομηνία εξέτασης 08/12/2023

PhD THESIS

Photonic technologies for secure data handling

Marialena Akriotou

SUPERVISOR: Dimitris Syvridis, Professor UoA

THREE-MEMBER ADVISORY COMMITTEE:

Dimitris Syvridis, Professor UoA
Angeliki Arapoyanni, Professor UoA
Panagiotis Rizomiliotis, Associate professor HUA

SEVEN-MEMBER EXAMINATION COMMITTEE

Dimitris Syvridis,
Professor UoA

Angeliki Arapoyanni,
Professor UoA

Panagiotis Rizomiliotits,
Associate professor HUA

Ioannis Stavrakakis,
Professor UoA

Konstantinos Chatzikokolakis,
Associate Professor UoA

Ioannis Panagakis,
Associate Professor UoA

Hector Nistazakis,
Professor UoA

Examination Date 08/12/2023

ΠΕΡΙΛΗΨΗ

Στο πλαίσιο της παρούσας διδακτορικής διατριβής με τίτλο «Φωτονικές Τεχνολογίες Για Την Ασφαλή Διαχείριση Δεδομένων» διερευνήθηκε η χρήση των φωτονικών μη-κλωνοποιήσιμων φυσικών συναρτήσεων (Physical Unclonable Functions - PUF), ως κεντρικά στοιχεία για την ανάπτυξη μιας νέας γενιάς συστημάτων, τα οποία θα επιτρέπουν την παραγωγή κρυπτογραφικών κλειδιών «τη αιτήσει» και σε πραγματικό χρόνο.

Η διερεύνηση αυτή κινήθηκε σε 3 βασικούς άξονες: Ο πρώτος άξονας αφορούσε στη μελέτη υλικών και τεχνικών για τον εντοπισμό του βέλτιστου συνδυασμού αυτών που επιτυγχάνει τις μέγιστες επιδόσεις ασφάλειας ενός τέτοιου συστήματος. Ο δεύτερος εστιάστηκε στην εξέταση της αξιοπιστίας των εν λόγω υλικών και τεχνικών καθόσον αφορά στην σταθερότητα τους σε περιβαλλοντικούς παράγοντες και στην ανθεκτικότητά τους σε υπολογιστικές επιθέσεις. Τέλος ο τρίτος άξονας επικεντρώθηκε στην συγκριτική αξιολόγηση των επιδόσεών τους, η οποία πραγματοποιήθηκε με αλγόριθμους επεξεργασίας και ανάλυσης πειραματικών δεδομένων και με μεθόδους προσομοίωσης των σχετικών φαινομένων.

Αναλυτικότερα, στο παρόν πόνημα αρχικά παρουσιάζεται το αριθμητικό μοντέλο που αναπτύχθηκε για την προσομοίωση των φυσικών διεργασιών που διέπουν την πλειοψηφία των φωτονικών PUFs. Το εν λόγω αριθμητικό μοντέλο, το οποίο βασίζεται κυρίως στην βαθμωτή θεωρία για την περίθλαση και στην κλασσική θεωρία των speckle patterns, χρησιμοποιήθηκε επιτυχώς για τον σχεδιασμό όλων των πειραματικών διατάξεων που υλοποιήθηκαν στο πλαίσιο της παρούσας διατριβής και για την εκτίμηση της αναμενόμενης απόδοσής τους. Κατόπιν, περιγράφεται η υπολογιστική διαδικασία που αναπτύχθηκε για την επεξεργασία των πειραματικών δεδομένων, μέσω των οποίων επιτεύχθηκε η εξαγωγή των ζητούμενων κρυπτογραφικών κλειδιών από τις διαθέσιμες αποκρίσεις εκάστης διάταξης. Η υπολογιστική αυτή διαδικασία περιλαμβάνει διάφορες τεχνικές επεξεργασίας σήματος και συναρτήσεις κατακερματισμού εικόνων (Hash Functions), οι οποίες, σε συνδυασμό με έναν κώδικα διόρθωσης λαθών (Error Correction Code - ECC) που χρησιμοποιείται στα πλαίσια ενός ασαφούς εξαγωγέα (Fuzzy Extractor), οδηγούν σε τυχαίες και απαλλαγμένες από σφάλματα, που προκαλούνται λόγω του αναπόφευκτου θορύβου παρατήρησης, δυαδικές ακολουθίες. Τέλος, παρουσιάζονται τα πειραματικά αποτελέσματα που προέκυψαν από τρεις διαφορετικές διατάξεις φωτονικών PUFs, οι οποίες υλοποιήθηκαν με σκοπό να δοκιμαστούν τρεις εναλλακτικές μέθοδοι παραγωγής διεγέρσεων και δύο διαφορετικά υποψήφια υλικά. Από τα εν λόγω πειραματικά αποτελέσματα αξιολογήθηκαν και τα κυριότερα χαρακτηριστικά ασφαλείας κάθε διάταξης, τα οποία αφορούν στην ευρωστία (Robustness), στην φυσική μη - κλωνοποιησιμότητα (Physical Unclonability) και στην φυσική μη - προβλεψιμότητα (Physical Unpredictability) των παραγόμενων κλειδιών τους.

Εν κατακλείδι, προϊόν της παρούσας διδακτορικής διατριβής είναι μιας πλήρως αξιόπιστη φωτονική PUF, βασικός πυρήνας της οποίας αποτελεί ένας συμβατικός οπτικός διαχύτης. Η εν λόγω PUF, η οποία χρησιμοποιεί ένα Digital Micromirror Device (DMD) για την παραγωγή των απαιτούμενων διεγέρσεων εξάγει δυαδικές ακολουθίες με πειραματικά αποδεδειγμένη επαναληψιμότητα που ξεπερνά τον έναν μήνα συνεχούς λειτουργίας και κρυπτογραφικής ασφάλειας έγκυρα πιστοποιημένης μέσω των ευρέως αποδεκτών ελέγχων τυχαιότητας του NIST. Τα ευρήματα μάλιστα των δραστηριοτήτων που οδήγησαν στην υλοποίηση αυτή εκτιμάται ότι προσδιορίζουν σε ικανοποιητικό βαθμό τις κυριότερες προδιαγραφές για την σχεδίαση ενός ολοκληρωμένου εργαστηριακού πρωτοτύπου μιας φωτονικής PUF. Η βιομηχανοποίηση του πρωτοτύπου αυτού αναμένεται να υποσκελίσει, σε επιδόσεις ασφαλείας, τις ήδη διαθέσιμες συμβατικές

γεννήτριες τυχαίων αριθμών (Random Number Generator - RNG), καθώς δύναται να οδηγήσει σε φορητές, χαμηλού κόστους και άμεσης εμπορικής εκμετάλλευσης συσκευές

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Πρωταρχικά δομικά στοιχεία ασφάλειας υλικού

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Φωτονική μη-κλωνοποιήσιμη φυσική συνάρτηση, γεννήτρια τυχαίων αριθμών, speckle pattern

ABSTRACT

In the context of this doctoral dissertation titled "Photonic Technologies for Secure Data Management", the use of photonic unclonable physical functions (Physical Unclonable Functions - PUF) was explored, as central elements for the development of a new generation of systems which will allow the production of cryptographic keys "on demand" and in real time.

This investigation was conducted along 3 main axes: The first axis involved the study of materials and techniques to identify the optimal combination of those, which achieves the maximum security performance of such a system. The second focused on the examination of the reliability of these materials and techniques with regard to their stability to environmental factors and their resistance to computational attacks. Finally, the third axis focused on the comparative evaluation of their performance, which was carried out using algorithms for processing and analysing the experimental data, and through simulation of the relevant phenomena.

More specifically, this thesis initially presents the numerical model that was developed for the simulation of the physical processes that govern the majority of photonic PUFs. This numerical model, which is mainly based on the scalar theory for diffraction and the classical theory of speckle patterns, was successfully used for the design of all experimental setups that were implemented in the context of this dissertation, and for the estimation of their expected performance. Following that, the computational process that was developed for the processing of experimental data is described, through which the extraction of the required cryptographic keys from the available responses of each arrangement was achieved. This computational process includes various signal processing techniques and image hashing functions (Hash Functions), which, in combination with an error correction code (Error Correction Code - ECC) used within the frame of a fuzzy extractor, lead to random and free of errors – caused by the inevitable observation noise – binary sequences. Finally, the experimental results obtained from three different photonic PUF arrangements are presented, which were implemented in order to test three alternative excitation production methods and two different candidate materials. From these experimental results, the main security features of each arrangement were evaluated, which relate to robustness, physical unclonability, and physical unpredictability of their generated keys.

In conclusion, the product of this doctoral dissertation is a fully reliable photonic PUF, the core of which is a conventional optical diffuser. This PUF, which uses a Digital Micromirror Device (DMD) for the production of the required excitations, extracts binary sequences with experimentally proven repeatability that exceeds one month of continuous operation, and cryptographic security certified through the widely accepted NIST randomness tests. The findings of the activities that led to this implementation are estimated to effectively determine the main specifications for the design of a complete laboratory prototype of a photonic PUF. The industrialization of this prototype is expected to overlap, in terms of security performance, the already available conventional random number generators (RNG), as it can lead to portable, low-cost devices of immediate commercial value.

SUBJECT AREA: Hardware security primitives

KEYWORDS: Photonic physical unclonable function, random number generator, speckle pattern

ΛΙΣΤΑ ΔΗΜΟΣΙΕΥΣΕΩΝ

"Photonic Physical Unclonable Functions as a Secure Key Generator for Cryptographic Applications", C. Mesaritakis, A. Kapsalis, **M. Akriotou**, D. Syvridis, 3rd International Conference on Cryptography, Cyber Security and Information Warfare (3rd CryCyblW), 26-27 May 2016, Athens, Greece, (oral presentation)

"Physical Unclonable Function based on a Multi-Mode Optical Waveguide", C. Mesaritakis, **M. Akriotou**, A. Kapsalis, E. Grivas, C. Chaintoutis, T. Nikas, D. Syvridis, Scientific Reports volume 8, Article number: 9653 (2018)

"Random Number Generation from a Secure Photonic Physical Unclonable Hardware Module", **M. Akriotou**, C. Mesaritakis, E. Grivas, C. Chaintoutis, A. Fragkos, D. Syvridis, First International ISCIS Security Workshop 2018, Euro-CYBERSEC 2018, London, UK, February 26-27, 2018, Revised Selected Papers

Laser Induced Speckle as a Foundation for Physical Security and Optical Computing", C. Mesaritakis, **M. Akriotou**, D. Syvridis, Photonics in Switching and Computing Confrence PSC 2018, Limassol, Cyprus

"Optical PUFs as physical root of trust for blockchain-driven applications",C. Chaintoutis, **M. Akriotou**, C. Mesaritakis, I. Komnios, D. Karamitros, A. Fragkos, D. Syvridis, in IET Software, vol. 13, no. 3, pp. 182-186, 6 2019

"Photonic physical unclonable functions: from the concept to fully functional device operating in the field", **M. Akriotou**, A. Fragkos, D. Syvridis, Proceedings Volume 11274, Physics and Simulation of Optoelectronic Devices XXVIII; 112740N (2020)

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα μελέτη υποβλήθηκε ως διδακτορική διατριβή στον Τομέα Επικοινωνιών και Επεξεργασίας Σήματος, στο τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών. Η εργασία πραγματοποιήθηκε στο εργαστήριο Φωτονικών Τεχνολογιών, υπό την επίβλεψη του κου Συβρίδη Δημητρίου, καθηγητή του τμήματος Πληροφορικής και Τηλεπικοινωνιών του Ε.Κ.Π.Α., με τη συνδρομή των κου Ριζομυλιώτη Παναγιώτη, αναπληρωτή καθηγητή του Χαροκόπειου Πανεπιστημίου Αθηνών, και της κας Αραπογιάννη Αγγελικής, καθηγήτριας στο τμήμα Πληροφορικής και Τηλεπικοινωνιών του Ε.Κ.Π.Α.

Σε αυτό το σημείο θα πρέπει να ευχαριστήσω θερμά τον καθηγητή μου, κ. Δημήτριο Συβρίδη, ο οποίος ανέλαβε την επίβλεψη της διδακτορικής μου διατριβής.

Θα ήθελα να απευθύνω θερμές ευχαριστίες προς τα υπόλοιπα μέλη της Επταμελούς Εξεταστικής Επιτροπής, κο Σταυρακάκη Ιωάννη, κο Χατζηκοκολάκη Κωνσταντίνο, κο Παναγάκη Ιωάννη, καθηγητές του τμήματος Πληροφορικής και Τηλεπικοινωνιών, και τον κο Νισταζάκη Έκτορα, καθηγητή του τμήματος Φυσικής του Ε.Κ.Π.Α., ενώπιον των οποίων πραγματοποιήθηκε η προφορική υποστήριξη της διδακτορικής μου διατριβής.

Ευχαριστίες θα ήθελα να δώσω και στους συναδέλφους μου, με τους οποίους συνεργάστηκα κατά την εκπόνηση της παρούσης διατριβής, Παναγιώτη Τσώτση, Χρήστο Βεϊνίδη, Νικόλαο Ράπτη, και Χάρη Μεσαριτάκη, η πολύτιμη συμβολή των οποίων υπήρξε καθοριστική στην ολοκλήρωσή της.

Τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου και τους φίλους μου που με ανέχονται τόσα χρόνια.

1. ΕΙΣΑΓΩΓΗ

Η καθολική χρήση πληροφοριακών συστημάτων για τη συλλογή και διαχείριση ψηφιακών δεδομένων έχει επιφέρει αναμφισβήτητα ριζικές αλλαγές σε κάθε πτυχή της σύγχρονης ζωής, προσφέροντας έναν γρήγορο και αποδοτικό τρόπο αποθήκευσης, επεξεργασίας και μετάδοσης της πληροφορίας. Ωστόσο, η επαρκής διασφάλιση της ακεραιότητας και της εμπιστευτικότητας των δεδομένων καθιστά επιτακτική την ανάγκη ανάπτυξης ολοένα και πιο περίπλοκων μηχανισμών ασφαλείας, οι οποίοι θα πρέπει αφενός να ικανοποιούν τις αυξανόμενες ανάγκες της σύγχρονης αγοράς, αφετέρου να προηγούνται και των πλέον προηγμένων μεθόδων επιβουλής.

Εν προκειμένω, μια από τις πιο διαδεδομένες στρατηγικές προστασίας πληροφοριακών συστημάτων αποτελεί η πιστοποίηση δύο παραγόντων (two factor authentication), κατά την οποία η «ψηφιακή υπογραφή» ενός χρήστη παράγεται μέσω μιας μοναδικής προσωπικής συσκευής [1]. Συνδυασμένη με κλασσικά πρωτόκολλα κρυπτογραφίας, η μέθοδος αυτή εν γένει δύναται να παρέχει υψηλά επίπεδα ασφαλείας, τα οποία όμως δυστυχώς υπονομεύονται από την καθιερωμένη χρήση ψευδοτυχαίων ακολουθιών. Συγκεκριμένα, έχει ήδη αποδειχθεί [2] ότι τα κλειδιά που προκύπτουν από συμβατικές γεννήτριες ψευδοτυχαίων αριθμών συνήθως κρίνονται προβλέψιμα και επισφαλή, αφού εμφανίζουν επαναλαμβανόμενα μοτίβα και αποδεικνύονται ιδιαίτερα ευαίσθητα στην αποκάλυψη της αλγοριθμικής τους «σποράς» (seed). Επομένως, δεν είναι καθόλου τυχαίο ότι τα τελευταία χρόνια παρατηρείται μια συστηματική προσπάθεια ανάπτυξης εναλλακτικών διαδικασιών που θα μπορούσαν να εξασφαλίζουν την παραγωγή τυχαίων κλειδιών, με το επίκεντρο της προσοχής να εστιάζεται στις λεγόμενες μη-κλωνοποιήσιμες φυσικές συναρτήσεις.

Συνοπτικά, μια μη-κλωνοποιήσιμη φυσική συνάρτηση (Physical Unclonable Function - PUF) αποτελεί ένα σύστημα υλικού (hardware), η οποία αξιοποιώντας την εγγενή τυχαιότητα μιας φυσικής διεργασίας, οδηγεί στη ντετερμινιστική παραγωγή τυχαίων αριθμών πλήρως απαλλαγμένων από τις προαναφερθείσες ευπάθειες. Το επίπεδο ασφαλείας που επιτυγχάνεται είναι ανάλογο της εσωτερικής πολυπλοκότητας του φυσικού μηχανισμού του συστήματος, η οποία καθιστά αδύνατη την κατασκευή ακριβών αντιγράφων ή την προσομοίωση της συμπεριφοράς του [3]. Ως εκ τούτου, καθώς ο συνολικός μηχανισμός μίας PUF θεωρείται απρόσβλητος από την πλειοψηφία των ενδεχόμενων φυσικών ή υπολογιστικών απειλών και σε συνδυασμό με το γεγονός ότι δύναται να υλοποιηθεί με χαμηλού κόστους, μικρού μεγέθους αλλά και ευρείας διαθεσιμότητας εξαρτήματα, καθίσταται ιδανικός για ένα μεγάλο φάσμα εφαρμογών ασφαλείας όπως η παραγωγή κρυπτογραφικών κλειδιών, η αυθεντικοποίηση οντοτήτων ή η διασύνδεση υλικού-λογισμικού [4]-[7].

1.1 Θεωρητικό Πλαίσιο

Μία PUF ορίζεται ως ο μονόδρομος μαθηματικός μετασχηματισμός, ο οποίος αντιστοιχεί σε ένα σύνθετο φυσικό σύστημα. Ως είσοδο, το σύστημα αυτό δέχεται μία εξωτερική διέγερση (challenge) και παράγει μία μοναδική απόκριση (response). Οι τρεις θεμελιώδεις ιδιότητες που χαρακτηρίζουν μια τέτοια συνάρτηση είναι [3],[8]:

- Ευρωστία (Robustness): η ντετερμινιστική αλληλεπίδραση των εφαρμοζόμενων διεγέρσεων και του χρησιμοποιούμενου φυσικού συστήματος, η οποία ουσιωδώς υποδηλώνει χρονικά σταθερές και επαναλήψιμες αποκρίσεις.

- Μη-προβλεψιμότητα (Unpredictability): η υψηλή πολυπλοκότητα της εν λόγω αλληλεπίδρασης, η οποία αποτρέπει οποιαδήποτε προσπάθεια πρόβλεψης των παραγόμενων αποκρίσεων.
- Μη-κλωνοποιησιμότητα (Unclonability): η μοναδικότητα της φυσικής δομής του χρησιμοποιούμενου συστήματος, η οποία καθιστά αδύνατη τη δημιουργία ενός ακριβούς αντιγράφου του, ακόμη και από τον ίδιο τον κατασκευαστή του.

Εν συντομία, οι υλοποιήσεις των PUFs διακρίνονται, ανάλογα με το είδος του φυσικού συστήματος που περιέχουν, σε ηλεκτρονικές και μη-ηλεκτρονικές [9]. Στις πρώτες περιλαμβάνονται ολοκληρωμένα κυκλώματα πυριτίου, όπως λογικές πύλες ή μνήμες, όπου αξιοποιούνται οι τυχαίες διαφοροποιήσεις στις προδιαγραφές λειτουργίας τους λόγω περιορισμένων κατασκευαστικών ανοχών. Εντούτοις, οι φυσικές διεργασίες που διέπουν τις αποκρίσεις τους χαρακτηρίζονται από σχετικά χαμηλή πολυπλοκότητα και καθιστούν την όλη υλοποίηση ευάλωτη σε κρυπταναλυτικές επιθέσεις, όπως machine-learning [9]-[13] και side-channel attacks [15]-[17].

Από την άλλη πλευρά στην δεύτερη κατηγορία, δεσπόζουσα θέση κατέχουν οι οπτικές υλοποιήσεις [18]-[20], οι οποίες κατά κύριο λόγο βασίζονται στην σκέδαση μιας δέσμης ακτινοβολίας laser από ένα οπτικό μέσο με πολυπληθείς και τυχαία κατανεμημένες ανομοιογένειες. Παραδείγματα τέτοιων μέσων αποτελούν τα λεπτά υμένια νανοσωματιδίων [21], οι τυχαία εγχαραγμένες επιφάνειες [22] και το κοινό χαρτί [23], η δομή των οποίων είναι πρακτικά αδύνατο να αναπαραχθεί, καθιστώντας την αντιγραφή του PUF ανέφικτη.

Κατά τη διάδοση σε τέτοια υλικά, μια δέσμη ακολουθεί ένα πλήθος οπτικών διαδρομών, με αποτέλεσμα τη μερική χωρική αποσυμφωνία της. Σκεδαζόμενα κύματα με την ίδια συχνότητα αλλά διαφορετικά πλάτη και φάσεις, οδηγούν σε πολύπλοκα φαινόμενα συμβολής, τα οποία καταγράφονται ως χωρικές αυξομειώσεις στην ένταση εξόδου και αποτυπώνονται ως μοναδικά κηλιδωτά μοτίβα (speckle patterns). Τα μοτίβα αυτά αντιστοιχούν στις ζητούμενες αποκρίσεις του συστήματος, οι οποίες δειγματοληπτούνται δημιουργώντας τα τελικά κρυπτογραφικά κλειδιά. Η πολυπλοκότητά τους εξαρτάται από τη διάμετρο και το μήκος κύματος της προσπίπτουσας δέσμης, τις διαστάσεις του υλικού καθώς και το μέγεθος των σκεδαστών, συνεπώς, οποιαδήποτε μεταβολή των παραμέτρων αυτών επιφέρει ισχυρή διαφοροποίηση, οδηγώντας σε ασυσχέτιστα μεταξύ τους κρυπτογραφικά κλειδιά. Αξίζει να σημειωθεί, ότι τα ωφέλιμα φαινόμενα σκέδασης μεγιστοποιούνται όταν οι ανομοιογένειες του υλικού είναι συγκρίσιμου μεγέθους με το μήκος κύματος της ακτινοβολίας. [24]

Εν γένει, οι PUFs μετρούν ήδη μια εικοσαετία ύπαρξης και διαφαίνεται ότι αποτελούν την καταλληλότερη μέθοδο παραγωγής κρυπτογραφικών κλειδιών. Εντούτοις, οι πρώτες απόπειρες αξιοποίησης τους, βασιζόμενες κυρίως σε ηλεκτρονικές υλοποιήσεις, δεν έχουν τύχει καθολικής αποδοχής και οι μέθοδοι παραμένουν πρακτικά αναξιοποίητες. Όσον αφορά τώρα τις φωτονικές PUFs, παρά τα πλεονεκτήματά τους, υπάρχουν ζητήματα που χρήζουν συστηματικής διερεύνησης για την επιτυχή τεχνολογική τους ωρίμανση. Από αυτά τα ζητήματα, τα κύρια συνοψίζονται ως εξής:

- Η αύξηση του αριθμού των δυνατών διεγέρσεων, σε επίπεδα συγκρίσιμα με τις σύγχρονες κρυπτογραφικές εφαρμογές. Στις μέχρι τώρα υλοποιήσεις το πλήθος των διεγέρσεων περιορίζεται σημαντικά από τη δυσκολία διαχείρισης της οπτικής δέσμης με χρήση ηλεκτρομηχανικών συστημάτων

με αποτέλεσμα οι οπτικές PUFs να καθίστανται ευάλωτες σε υπολογιστικές επιθέσεις εξάντλησης όλων των διεγέρσεων (exhaustion attacks) και να μην μπορούν να χρησιμοποιηθούν ως γεννήτριες κλειδιών παρά μόνο ως συστήματα αυθεντικοποίησης μοναδιαίας απόκρισης.

- Η αντικατάσταση των μηχανικών εξαρτημάτων, τα οποία είναι απαραίτητα για την προαναφερθείσα οδήγηση της δέσμης (όπως κάτοπτρα, translation stages και φακοί), αλλά αναπόφευκτα προκαλούν την αύξηση του μετρητικού θορύβου, υποβαθμίζοντας την επαναληψιμότητα των παραγόμενων αποκρίσεων.

1.2 Ερευνητικά Ερωτήματα / Υποθέσεις Εργασίας

Αντικείμενο της παρούσας διδακτορικής διατριβής είναι η συστηματική μελέτη τόσο σε θεωρητικό, όσο και πειραματικό επίπεδο, όλων των πιθανών παραμέτρων που αφορούν στη βέλτιστη υλοποίηση μιας φωτονικής PUF, ώστε να αποτελέσει πρότυπο για την σχεδίαση μιας φορητής συσκευής χαμηλού κόστους και μη-κλωνοποιήσιμης, η οποία θα παράγει πραγματικά τυχαία και ασυσχέτιστα κρυπτογραφικά κλειδιά. Σε αυτό το πλαίσιο λοιπόν, τα σχετικά ερευνητικά ερωτήματα διαμορφώνονται ως εξής:

- Επέκταση του πλήθους των εφαρμοζόμενων διεγέρσεων, ώστε να ικανοποιεί τις επιταγές των σύγχρονων δομών κρυπτασφάλισης.
- Βελτιστοποίηση της πειραματικής διάταξης, η οποία θα επιτρέπει την καταγραφή speckle patterns, με σημαντική καταστολή του θορύβου που υπεισέρχεται κατά την διεξαγωγή της μετρητικής διαδικασίας, συμπεριλαμβανομένης και της ανοχής στις περιβαλλοντικές συνθήκες.
- Διερεύνηση του καταλληλότερου οπτικού μέσου, το οποίο θα οδηγήσει στις βέλτιστες επιδόσεις καθόσον αφορά την ευρωστία, τη μη-κλωνοποιησιμότητα και τη μη-προβλεψιμότητα των παραγόμενων κλειδιών.
- Εντοπισμό ενδεχόμενων κενών ασφαλείας των υπό μελέτη υλοποιήσεων και εύρεση τρόπων αντιμετώπισής τους.

Η επιτυχής διερεύνηση των παραπάνω ερωτημάτων αναμένεται να οδηγήσει στην ανάπτυξη μιας νέας γενιάς υποσυστημάτων, τα οποία θα αποτελέσουν καινοτόμο εξέλιξη στον τομέα της κρυπτασφάλισης, ελαχιστοποιώντας το κόστος κατασκευής και μεγιστοποιώντας την παρεχόμενη ασφάλεια. Συγκεκριμένα, η προτεινόμενη φωτονική PUF θα μπορούσε να αποτελέσει δομικό στοιχείο των παρακάτω συσκευών:

- Γεννήτρια τυχαίων αριθμών (υπό την μορφή USB flash), συμβατή με ώριμα συστήματα ή/και πρωτόκολλα κρυπτασφάλειας, η οποία θα εξαλείψει την ανάγκη της ασφαλούς αποθήκευσης των παραγόμενων κρυπτογραφικών κλειδιών, αυξάνοντας το επίπεδο ασφάλειας και μειώνοντας το κόστος του συστήματος, επιτρέποντας τη χρήση τους σε ευρύ πεδίο εφαρμογών όπως: α) Κρυπτογράφηση με χρήση συμμετρικών και ασύμμετρων κλειδιών, χωρίς τα μειονεκτήματα των ψευδο-τυχαίων γεννητριών, τα οποία θα είναι κατάλληλα για διατραπεζικές συναλλαγές, ηλεκτρονικό εμπόριο, στρατιωτικές επικοινωνίες κλπ. β) Αυθεντικοποίηση χρηστών για τη φυσική πρόσβασή τους σε χώρους. γ) Μη αντιγράψιμες ψηφιακές υπογραφές δ) Ασφαλή αποθήκευση δεδομένων σε κοινόχρηστους πόρους ε) Αυθεντικοποίηση προϊόντων. στ) Κρυπτογράφηση για ασφαλή αποθήκευση και πρόσβαση στο νέφος. ζ) Αυθεντικοποίηση μεμονωμένων συσκευών τύπου Internet-of-Things (IoT).

- Γεννήτρια κρυπτογραφικών κλειδιών ως υποσύστημα έξυπνης κάρτας, η οποία, εφοδιασμένη με αλγορίθμους κρύπτο-αποκρυπτογράφησης θα μπορεί να καλύψει πλήρως τις ανάγκες ταυτοποίησης και εξουσιοδότησης του χρήστη, της απόκρυψης και ακεραιότητας δεδομένων, την ασφάλεια εξοπλισμού, λογισμικού και διαύλων επικοινωνίας.

1.3 Μεθοδολογία και Διάρθρωση Εργασίας

Η μεθοδολογική προσέγγιση που εφαρμόστηκε βάσει των διατυπωμένων στόχων και των ερευνητικών ερωτημάτων που τέθηκαν στην προηγούμενη ενότητα συνοψίζεται ως εξής:

Αρχικά διεξήχθη μια εκτενής βιβλιογραφική έρευνα πάνω στις υπάρχουσες υλοποιήσεις των οπτικών PUFs και τις φυσικές διεργασίες από τις οποίες αυτές διέπονται, ούτως ώστε να αποκτηθεί το απαραίτητο θεωρητικό υπόβαθρο για την ανάπτυξη ενός υπολογιστικού μοντέλου, μέσω του οποίου σχεδιάστηκαν όλες οι πειραματικές διατάξεις της παρούσας διατριβής. Ταυτόχρονα δοκιμάστηκαν σε πειραματικό επίπεδο ποικίλες πηγές σύμφωνης Η/Μ ακτινοβολίας για την παραγωγή των απαιτούμενων διεγέρσεων και διερευνήθηκαν εναλλακτικοί τρόποι οδήγησης της δέσμης για την ζητούμενη επέκταση του διαθέσιμου πλήθους τους. Σε κάθε περίπτωση ελέγχθηκαν διάφορα υποψήφια υλικά, από τα οποία προκρίθηκαν τα πλέον ενδεδειγμένα. Όσον αφορά τώρα τις αποκρίσεις των υπό μελέτη συστημάτων, η συλλογή και η ψηφιακή καταγραφή των παραγόμενων speckle patterns επιτεύχθηκε με κατάλληλες οπτικές και ηλεκτρονικές τεχνικές που επέτρεψαν τη βέλτιστη καταστολή του πειραματικού θορύβου, ενώ οι τελικές δυαδικές έξοδοι κάθε συστήματος προέκυψαν από την εφαρμογή διαφόρων μεθόδων επεξεργασίας δεδομένων σε αυτές. Στο σημείο αυτό θα πρέπει να σημειωθεί ότι με την χρήση τούτων των δυαδικών εξόδων ουσιαστικά διεξήχθη και η τελική μελέτη των στοχευόμενων χαρακτηριστικών απόδοσης, η οποία επέτρεψε την έγκυρη σύγκριση των μελετούμενων διατάξεων και οδήγησε στην εμπεριστατωμένη επιλογή της βέλτιστης υλοποίησης.

Τα χαρακτηριστικά απόδοσης κάθε συστήματος που έχουν μελετηθεί, λοιπόν, αφορούν: την ευρωστία, κάτω από την επίδραση ελεγχόμενων περιβαλλοντικών συνθήκων, την μη-κλωνοποιησιμότητα, μέσω εξόδων από πολλά οπτικά μέσα που προέρχονται από την ίδια κατασκευαστική διαδικασία και την μη-προβλεψιμότητα, εξετάζοντας την τυχαιότητα εξόδων που προκύπτουν από την εφαρμογή πολλών διεγέρσεων. Η μελέτη αυτή έλαβε χώρα μέσω ενός κατάλληλου υπολογιστικού περιβάλλοντος, το οποίο αναπτύχθηκε για την επεξεργασία και την ανάλυση των διαθέσιμων πειραματικών αποτελεσμάτων τόσο σε επίπεδο ψηφιακών στιγμιοτύπων όσο και σε επίπεδο δυαδικών εξόδων.

Αναλυτικότερα, στο κεφάλαιο 2 της παρούσας διατριβής παρουσιάζεται το αριθμητικό μοντέλο, το οποίο αναπτύχθηκε για την προσομοίωση των φυσικών διεργασιών που διέπουν τις υπό μελέτη οπτικές PUFs, συνοδευόμενο από το απαραίτητο θεωρητικό υπόβαθρό του. Συγκεκριμένα, το κεφάλαιο αυτό περιλαμβάνει μια περιεκτική σύνοψη της βαθμωτής θεωρίας για την περίθλαση, η οποία χρησιμοποιήθηκε για την προσομοίωση της αλληλεπίδρασης του φωτός με τα οπτικά στοιχεία των μελετούμενων υλοποιήσεων και μια σύντομη περίληψη της θεωρίας για την Η/Μ κυματοδήγηση, με την οποία μοντελοποιήθηκε η διάδοση μιας σύμφωνης δέσμης ακτινοβολίας σε μια πολύτροπη οπτική ίνα βηματικού δείκτη διάθλασης. Επίσης, αναφέρεται ο αλγόριθμος του θορύβου Perlin, μέσω του οποίου μοντελοποιήθηκαν οι θεωρούμενες ανομοιογενείς επιφάνειες της παρούσας εργασίας, ενώ παρατίθενται και οι θεμελιώδεις στατιστικές ιδιότητες των

speckle patterns που σχηματίζονται από την αλληλεπίδραση του φωτός με τούτες τις επιφάνειες.

Ακολούθως, στο κεφάλαιο 3 αρχικά παρουσιάζονται όλοι οι επιμέρους αλγόριθμοι της υπολογιστικής διαδικασίας που εφαρμόστηκε επί των ληφθέντων speckle patterns, ώστε να παραχθούν οι ζητούμενες δυαδικές έξοδοι από την εκάστοτε υλοποίηση. Κατόπιν, παρατίθενται όλες οι μέθοδοι ανάλυσης και ερμηνείας των πειραματικών αποτελεσμάτων, μέσω των οποίων κατέστη εφικτή η συγκριτική αξιολόγηση των υπό μελέτη συστημάτων. Ειδικότερα, το πρώτο σκέλος του κεφαλαίου 3 εστιάζει στο λογισμικό που αναπτύχθηκε για να διασφαλιστεί η εξαγωγή αναπαραγώγιμων και κρυπτογραφικά ασφαλών κλειδιών από κάθε μελετούμενη οπτική PUF, το οποίο ουσιαστικά αντιστοιχεί σε μια κατάλληλα τροποποιημένη υλοποίηση ενός ασαφούς εξαγωγέα. Στο πλαίσιο λοιπόν του ασαφούς αυτού εξαγωγέα εφαρμόζονται ποικίλες τεχνικές επεξεργασίας σήματος και συναρτήσεις κατακερματισμού εικόνας προκειμένου να μετατραπούν τα σημαντικότερα γεωμετρικά γνωρίσματα των ληφθέντων πειραματικών αποκρίσεων σε ένα σύνολο από αντιπροσωπευτικές δυαδικές ακολουθίες. Στο ίδιο πλαίσιο, εκτελείται επιπροσθέτως και ένας κώδικας ανίχνευσης και διόρθωσης λαθών, ώστε να αποκατασταθούν τα αναπόφευκτα σφάλματα που υπεισέρχονται στις ακολουθίες αυτές, λόγω του ανεπιθύμητου θορύβου παρατήρησης. Στο δεύτερο σκέλος του κεφαλαίου 3 από την άλλη πλευρά, παρατίθενται οι κυριότερες μετρικές που επιστρατεύθηκαν για την ποσοτικοποίηση της επίδοσης των υπό μελέτη συστημάτων, τόσο στο επίπεδο των πειραματικών εικόνων, μέσω της Ευκλείδειας απόστασης και του συντελεστή διασυσχέτισης Pearson, όσο και στο επίπεδο των δυαδικών κλειδιών, μέσω της απόστασης Hamming. Εν συνεχεία γίνεται μια σύντομη αναφορά στην στατιστική ανάλυση των παραγόμενων αποτελεσμάτων και στην ποιοτική τους ερμηνεία, ενώ τέλος παρατίθενται με συνοπτικό τρόπο όλοι οι διαγνωστικοί έλεγχοι του λογισμικού πακέτου NIST, οι οποίοι χρησιμοποιήθηκαν ούτως ώστε να διερευνηθεί η καταλληλότητα των υπό μελέτη συστημάτων ως γεννήτριες τυχαίων αριθμών.

Έπειτα, στα κεφάλαια 4, 5 και 6 εμπεριέχονται όλα τα πειραματικά αποτελέσματα, όπως αυτά προέκυψαν από τις τρεις διαφορετικές διατάξεις που κατασκευάστηκαν για τις ανάγκες της παρούσας διατριβής, οι οποίες σχεδιάστηκαν προκειμένου να δοκιμαστούν τρεις εναλλακτικές μέθοδοι παραγωγής διεγέρσεων και δύο υποψήφια υλικά· ένα γυάλινο πλακίδιο διάχυσης φωτός και μία πολύτροπη οπτική ίνα με βηματικό δείκτη διάθλασης και τυχαίες ατέλειες στις επιφάνειες εισόδου και εξόδου της. Συγκεκριμένα, στο κεφάλαιο 4 παρουσιάζεται η απόδοση των δύο προαναφερθέντων υλικών, όπως αυτή προκύπτει από τη διάταξη που κατασκευάστηκε για να αξιολογηθεί ως τεχνική παραγωγής διεγέρσεων η μεταβολή του μήκους κύματος μιας δέσμης ακτινοβολίας, η οποία προέρχεται από ένα συντονιζόμενο διοδικό laser που εκπέμπει στο εγγύς υπέρυθρο. Έπειτα, το κεφάλαιο 5 επικεντρώνεται στην εφαρμογή διεγέρσεων που αντιστοιχούν σε ένα σύνολο δυαδικών μοτίβων, τα οποία τροποποιούν τα σημεία πρόσπτωσης του φωτός επί του εκάστοτε ανομοιογενούς μέσου μέσω μίας οθόνης LCD, η οποία παρεμβάλλεται στην οπτική διαδρομή μιας δέσμης που παράγεται από ένα laser HeNe στο φάσμα του ορατού. Ακολούθως, το κεφάλαιο 6 πραγματεύεται μια βελτιωμένη παραλλαγή της πειραματικής διάταξης με την οθόνη LCD, στην οποία όμως η διαμόρφωση της προσπίπτουσας δέσμης και η μεταβολή των σημείων πρόσπτωσης επί του εκάστοτε δείγματος επιτυγχάνεται μέσω μιας ηλεκτρο-οπτικής συσκευής DMD.

Τέλος, στα τελευταία δύο κεφάλαια της εν λόγω διατριβής συνοψίζονται τα σημαντικότερα συμπεράσματα, όπως αυτά προέκυψαν από την θεωρητική και

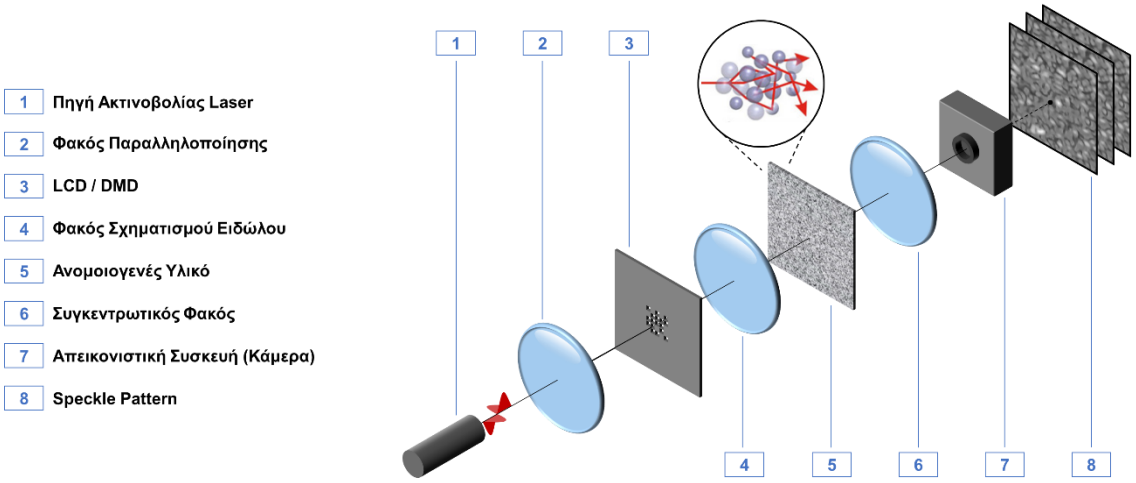
πειραματική διερεύνηση των επιλεγμένων υλοποιήσεων, καθώς και πιθανές κατευθύνσεις για άλλες μελλοντικές μελέτες.

2. ΘΕΩΡΗΤΙΚΗ ΠΕΡΙΓΡΑΦΗ PUFS - ΜΟΝΤΕΛΟΠΟΙΗΣΗ

Όπως έχει γίνει ήδη φανερό από την εισαγωγική ενότητα, η συνεχής ενασχόληση της επιστημονικής κοινότητας με τις οπτικές μη - κλωνοποιήσιμες φυσικές συναρτήσεις έχει οδηγήσει σε ένα ευρύ φάσμα από προτεινόμενες υλοποιήσεις, το οποίο εμπλουτίζεται διαρκώς με καινούριες και καινοτόμες ιδέες. Εντούτοις, οι περισσότερες από αυτές τις ιδέες, ως παρεπόμενα βασικής έρευνας, συνήθως δεν ευδοκιμούν σε επίπεδο εφαρμογής, καθώς η ολοκληρωμένη τεχνολογική τους ανάπτυξη απαιτεί εξειδικευμένο και ογκώδη εξοπλισμό υψηλού κόστους.

Στην πραγματικότητα λοιπόν, οι πιο εξεζητημένες από τις προτεινόμενες οπτικές PUF, παρά το μεγάλο επιστημονικό τους ενδιαφέρον, έχουν παραμείνει στάσιμες σε ένα πρώιμο στάδιο εργαστηριακού πρωτολείου, το οποίο δεν αναμένεται να ξεπεραστεί στο εγγύς μέλλον. Αντίθετα, οι φαινομενικά απλούστερες προσεγγίσεις, που κατά κανόνα αποτελούν παραλλαγές της αρχετυπικής PUF όπως αυτή εισήχθη από τον Pappu το 2001 [3],[21], έχουν γίνει ήδη αντικείμενο συστηματικότερης μελέτης, με τις πρώτες αντίστοιχες συσκευές τους πλέον να δοκιμάζονται υπό ρεαλιστικές συνθήκες λειτουργίας και σε πραγματικά συστήματα ασφαλείας.

Εν προκειμένω, στο σχήμα που ακολουθεί επιδεικνύεται ένα αντιπροσωπευτικό δείγμα μιας τυπικής οπτικής PUF, η οποία βασίζεται στο φαινόμενο της πολλαπλής σκέδασης του φωτός, όπως αυτή του Pappu. Το εν λόγω διάγραμμα ουσιαστικά αποτελεί το αμάλγαμα των πειραματικών διατάξεων που κατασκευάστηκαν στο πλαίσιο της παρούσας μελέτης, από το οποίο όμως έχουν παραληφθεί κάποια οπτικά στοιχεία που επιστρατεύθηκαν για την οδήγηση της δέσμης και τον έλεγχο της έντασης αυτής.



Σχήμα 2.1: Αντιπροσωπευτική υλοποίηση μιας τυπικής οπτικής PUF που βασίζεται στο φαινόμενο της πολλαπλής σκέδασης.

Επιγραμματικά, η πειραματική διαδικασία που αναπαριστάται στο παραπάνω σχήμα συνοψίζεται ακολούθως: αρχικά, μια δέσμη σύμφωνου φωτός που προέρχεται από μια πηγή ακτινοβολίας laser 1, διέρχεται από έναν επιπεδόκυρτο φακό παραλληλοποίησης 2 και προσπίπτει ως ένα επίπεδο κύμα σε μια οθόνη υγρών κρυστάλλων (Liquid Crystal Display - LCD) 3, στην οποία προβάλλεται με διαδοχικό τρόπο μια αλληλουχία δυαδικών εικόνων. Κάθε μία από αυτές τις εικόνες ενεργοποιεί έναν διαφορετικό συνδυασμό εικονοστοιχείων, ο οποίος με την σειρά του τροποποιεί το μέτωπο του προσπίπτοντος κύματος, σχηματίζοντας ένα μοναδικό οπτικό μοτίβο. Το είδωλο του σχηματιζόμενου μοτίβου έπειτα

απεικονίζεται μέσω ενός αμφίκυρτου φακού [4] στην επιφάνεια ενός ανομοιογενούς υλικού μέσου [5], με το φως που διαδίδεται εντός του να υπόκειται στο φαινόμενο της πολλαπλής σκέδασης. Αποτέλεσμα του φαινομένου αυτού αποτελεί ένα πολύπλοκο πρότυπο συμβολής που ονομάζεται speckle pattern, το οποίο συλλέγεται μέσω ενός συγκεντρωτικού φακού [6] σε μία κάμερα [7], με την οποία καταγράφεται και η τελική του μορφή [8].

Επομένως, υπό το γενικό πλαίσιο ορισμού μιας PUF, κάθε διέγερση της εικονιζόμενης διάταξης αντιστοιχεί στις ακριβείς συνθήκες ακτινοβόλησης του ανομοιογενούς μέσου, με την εφαρμογή της σε αυτό να οδηγεί στην παραγωγή ενός speckle που αποτελεί την ζητούμενη απόκριση του συστήματος. Οι συνθήκες αυτές μάλιστα αφορούν έναν ικανό αριθμό παραμέτρων, οι οποίες είναι καίριας σημασίας για την συνολική απόδοση του συστήματος, καθώς η επιλογή τους σε σχέση με το μέγεθος των ανομοιογενειών και το πάχος του υλικού επηρεάζουν άμεσα την πολυπλοκότητα των εξαγόμενων αποκρίσεων [24],[25]. Το μήκος κύματος και η γωνία πρόσπτωσης της δέσμης πάνω στο υλικό μέσο, η διαμόρφωση που εφαρμόζεται σε αυτή από το προβαλλόμενο μοτίβο επί της LCD και η χρησιμοποιούμενη μεγέθυνση του απεικονιζόμενου ειδώλου αποτελούν ένα ενδεικτικό δείγμα αυτών των παραμέτρων.

Στις παραγράφους λοιπόν του παρόντος κεφαλαίου παρουσιάζεται ένα υπολογιστικό μοντέλο που αναπτύχθηκε με σημείο αναφοράς την διάταξη του σχήματος 2.1, στην έκδοση 3.9.11 της Python. Το συγκεκριμένο κεφάλαιο ουσιαστικά διαρθώνεται σε τρεις κύριες θεματικές υποενότητες, οι οποίες περιέχουν το απαραίτητο θεωρητικό υπόβαθρο των φυσικών διεργασιών που διέπουν μια οπτική PUF και μερικά αντιπροσωπευτικά αποτελέσματα προσομοιώσεων που υποβοηθούν την κατανόηση και τον σχεδιασμό ενός τέτοιου συστήματος.

Ειδικότερα, η πρώτη υποενότητα του κεφαλαίου αυτού περιέχει μια περιεκτική σύνοψη της βαθμωτής θεωρίας για την περίθλαση, με την οποία περιγράφεται η διάδοση του φωτός σε ένα διηλεκτρικό μέσο, παρουσία οπτικών εμποδίων. Η συγκεκριμένη θεωρία χρησιμοποιήθηκε για την προσομοίωση της αλληλεπίδρασης μιας ιδανικής δέσμης laser με τα διάφορα οπτικά στοιχεία που απαρτίζουν την εικονιζόμενη πειραματική διάταξη, όπως φακούς, συστήματα διαμόρφωσης πλάτους (LCD/DMD), διαφράγματα και ίριδες.

Η δεύτερη υποενότητα από την άλλη πλευρά, επικεντρώνεται στη μοντελοποίηση επιφανειών με τυχαίες ανομοιογένειες και την προσομοίωση της σκέδασης του φωτός από αυτές. Ουσιαστικά στην ενότητα αυτή παρατίθενται κάποια βασικά στοιχεία από την κλασσική θεωρία για το speckle pattern και αναφέρονται οι θεμελιώδεις στατιστικές ιδιότητες από τις οποίες αυτό χαρακτηρίζεται.

Τέλος, η τρίτη υποενότητα περιλαμβάνει μια σύντομη περίληψη της H/M θεωρίας για την διάδοση του φωτός σε κυματοδηγούς κυλινδρικής συμμετρίας, εστιάζοντας κυρίως στην μοντελοποίηση πολύτροπων οπτικών ινών με βηματικό δείκτη διάθλασης.

2.1 Βαθμωτή Θεωρία Περίθλασης

Ο όρος περίθλαση αναφέρεται σε ένα αμιγώς κυματικό φαινόμενο, το οποίο λαμβάνει χώρα όταν κατά την διάδοση ενός H/M πεδίου παρεμβληθεί μία δομή που επιβάλλει την χωρική ανακατανομή της εγκάρσιας έντασής του. Πρακτικά, πρόκειται για οποιαδήποτε εκτροπή του φωτός από την πορεία διάδοσής του, όπως αυτή διέπεται από τους νόμους της γεωμετρικής οπτικής, η οποία δεν μπορεί να αποδοθεί στα φαινόμενα της ανάκλασης και της διάθλασης [26].

Εν συντομία, η φυσική ερμηνεία της περίθλασης απορρέει από την αρχή των Huygens και Fresnel, η οποία διατυπώνεται ως εξής: όλα τα σημεία ενός μετώπου κύματος δρουν ως μια δευτερογενής πηγή σφαιρικών κυμάτων ίδιας συχνότητας με την αρχική, όπου η επαλληλία τους αποτελεί το πλάτος του καινούριου πεδίου, όπως αυτό διαμορφώνεται μετά από κάποιο χρονικό διάστημα διάδοσης. Η αρχή αυτή λοιπόν, σε συνδυασμό με την Η/Μ θεωρία του Maxwell, αποτελεί την βάση για την θεωρητική και μαθηματική θεμελίωση του εν λόγω φαινομένου.

Ειδικότερα, όπως αποδεικνύεται από τις εξισώσεις του Maxwell για ένα επίπεδο μονοχρωματικό κύμα που διαδίδεται εντός ενός γραμμικού, ομογενούς, ισότροπου και μη μαγνητικού διηλεκτρικού υλικού χωρίς διασπορά, όλες οι συνιστώσες του Η/Μ πεδίου συμπεριφέρονται με πανομοιότυπο τρόπο και μπορούν να περιγραφούν από μία κοινή και βαθμωτή κυματική εξίσωση:

$$\frac{1}{c^2}\frac{\partial^2}{\partial t^2}u(r,t)-\nabla^2 u(r,t)=0 \tag{2.1}$$

όπου c η ταχύτητα του φωτός στο διηλεκτρικό μέσο διάδοσης και u(r,t) οποιαδήποτε συνιστώσα του πεδίου, με $U(r) = U_0(r)\exp(j\varphi)$ το μιγαδικό της πλάτος.

$$u(r,t)=U_0(r)\cos\left[\omega t+\varphi(r)\right]=\mathrm{Re}\left\{U(r)\exp\left[-j\omega t\right]\right\} \tag{2.2}$$

Επιπρόσθετα, από τον συνδυασμό των δύο παραπάνω σχέσεων προκύπτει και η χρονοανεξάρτητη εξίσωση του Helmholtz, όπου $k = 2\pi/\lambda$ ο λεγόμενος κυματάριθμος,

$$\left(\nabla^2+k\right)U=0 \tag{2.3}$$

η λύση της οποίας συνιστά, τόσο τον κεντρικό πυρήνα της υπό μελέτη βαθμωτής θεωρίας για την περίθλαση, όσο και την μαθηματική αφετηρία του αριθμητικού μοντέλου που θα παρουσιαστεί στην συνέχεια.

Εν προκειμένω, το βαθμωτό μιγαδικό πλάτος U(r) που ικανοποιεί την εξίσωση του Helmholtz δίνεται από το ολοκλήρωμα Rayleigh - Sommerfeld:

$$U(P_2)=\iint_{\Sigma}U(P_1)\frac{\exp(jkr)}{j\lambda r}\cos\theta\,d\xi d\eta \tag{2.4}$$

Στο άνωθεν ολοκλήρωμα τα $P_1 = (\xi,\eta)$ και $P_2 = (x,y)$ αντιπροσωπεύουν τα μελετούμενα σημεία υπολογισμού, τα οποία βρίσκονται σε δύο παράλληλα επίπεδα παρατήρησης με απόσταση z και διαφορετικό σύστημα συντεταγμένων, ενώ το r συμβολίζει την απόσταση που χωρίζει τα δύο αυτά σημεία, για την οποία ισχύει

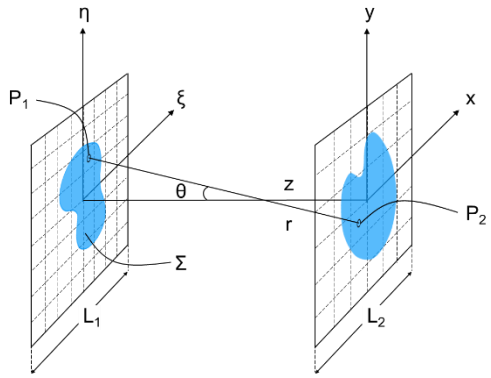
$$r=\sqrt{(x-\xi)^2+(y-\eta)^2+z^2} \tag{2.5}$$

και $\cos\theta = z/r$. Τέλος, το Σ αντιστοιχεί στην συνολική επιφάνεια του αρχικού U.

Θα πρέπει να υπογραμμισθεί ότι η δοθείσα ολοκληρωτική λύση οδηγεί σε αρκούντως ικανοποιητικά αποτελέσματα μόνο υπό από τις ακόλουθες δύο προϋποθέσεις: όταν η διατομή της επιφάνειας Σ είναι συγκρίσιμη με το μήκος κύματος λ της διαδιδόμενης ακτινοβολίας και όταν η απόσταση z μεταξύ των επιπέδων παρατήρησης είναι αρκετές τάξεις μεγέθους μεγαλύτερη από αυτό. Στην αντίθετη περίπτωση, οι διανυσματικές συνιστώσες του Η/Μ πεδίου παραμένουν συζευγμένες μέσω των εξισώσεων του Maxwell και το φως δεν μπορεί να εκληφθεί εξαρχής ως ένα βαθμωτό μέγεθος, αφού τα φαινόμενα σύζευξης στις οριακές

συνθήκες που αντιπροσωπεύουν την αλληλεπίδραση του φωτός με την ύλη δεν μπορούν να θεωρηθούν αμελητέα.

Συνοψίζοντας, το ολοκλήρωμα Rayleigh - Sommerfeld της σχέσης (2.4) αντιστοιχεί στην αναλυτική λύση της εξίσωσης του Helmholtz για ένα βαθμωτό H/M πεδίο, αποτελώντας μια εναλλακτική έκφραση της αρχής των Huygens και Fresnel: το πεδίο σε κάθε σημείο $P_2(x,y)$ επί ενός επιπέδου παρατήρησης προσδιορίζεται ως το άθροισμα των συνεισφορών από ένα σύνολο σφαιρικών κυμάτων, τα οποία πηγάζουν από κάθε σημείο $P_1(\xi,\eta)$ της αρχικής επιφάνειάς του Σ.



Σχήμα 2.2: Η γεωμετρία του ολοκληρώματος Rayleigh - Sommerfeld για διάδοση ακτινοβολίας μεταξύ δύο παράλληλων επιπέδων παρατήρησης.

2.1.1 Περίθλαση Φωτός από Διάφραγμα

Γενικά, η περίθλαση της οπτικής ακτινοβολίας αποτελεί ένα κοινό κυματικό φαινόμενο, το οποίο εκφράζεται στην φύση με μυριάδες διαφορετικούς τρόπους [1]. Ένας από αυτούς είναι και η διάχυση που υφίσταται μια δέσμη φωτός, αφού διέλθει από μία μικρή οπή.

Έστω λοιπόν ένα επίπεδο κύμα μονοχρωματικής ακτινοβολίας που διέρχεται από ένα διάφραγμα με ακανόνιστη διατομή, όπως αυτό του σχήματος 2.2, και διαδίδεται για μια απόσταση z στην οποία έχει τοποθετηθεί ένα αδιαφανές πέτασμα παρατήρησης. Η εγκάρσια κατανομή της έντασης που προβάλλεται στο πέτασμα αυτό είναι γνωστή ως το πρότυπο περίθλασης του πεδίου.

Το πρότυπο περίθλασης ενός πεδίου υπολογίζεται από το μέτρο της προαναφερθείσας λύσης κατά Sommerfeld ενώ η μορφή του εξαρτάται από τρεις βασικές παραμέτρους: τη μέγιστη ακτίνα d του περιθλώντος ανοίγματος, το μήκος κύματος λ της διαδιδόμενης ακτινοβολίας και την απόσταση z του πετάσματος παρατήρησης από το άνοιγμα. Βάσει μάλιστα της τελευταίας, κάθε φαινόμενο περίθλασης μπορεί να διακριθεί σε τρεις κύριες περιοχές: την περιοχή της γεωμετρικής σκιάς, την περιοχή του εγγύς πεδίου (περίθλαση Fresnel) και την περιοχή του μακρινού πεδίου (περίθλαση Fraunhofer) [27],[28]. Στην περιοχή της γεωμετρικής σκιάς, η οποία βρίσκεται αμέσως μετά το χρησιμοποιούμενο διάφραγμα, η διαδιδόμενη δέσμη ακτινοβολίας δεν προλαβαίνει να διευρυνθεί σύμφωνα με την αρχή των Huygens - Fresnel και το αντίστοιχο πρότυπο περίθλασης ουσιαστικά αποτελεί την ευθεία προβολή του σχήματος από το

[1] Η παρατήρηση περιθλαστικών φαινομένων από έναν μέσο παρατηρητή και υπό κανονικές συνθήκες είναι αρκετά σπάνια, καθώς στην πλειοψηφία των περιπτώσεων η χρησιμοποιούμενη πηγή ακτινοβολίας είναι πολυχρωματική, η διατομή του πεδίου σχετικά μεγάλη και η οπτική εκδήλωση ανεπαρκής.

άνοιγμα του διαφράγματος. Από την άλλη πλευρά, στην περιοχή του εγγύς πεδίου, η οποία εντοπίζεται για αποστάσεις:

$$z^3 >> \left\{ \frac{\pi}{4\lambda} \left[(x-\xi)^2 + (y-\eta)^2 \right]^2 \right\}_{max} \tag{2.6}$$

η εγκάρσια κατανομή της έντασης αρχίζει να διευρύνεται, εμφανίζοντας ένα κεντρικό μέγιστο που θυμίζει το σχήμα του διαφράγματος, το οποίο περιβάλλεται από αχνούς κροσσούς συμβολής. Τέλος, στην περιοχή του μακρινού πεδίου για αποστάσεις

$$z >> \left[\frac{k\left(\xi^2 + \eta^2\right)}{2} \right]_{max} \tag{2.7}$$

όπου τα διαδιδόμενα κύματα μπορούν να θεωρηθούν επίπεδα, η μορφή του προτύπου περίθλασης, όπως μπορεί να αποδειχτεί, συμπίπτει με τον μετασχηματισμό Fourier του περιθλώντος ανοίγματος, παραμένει σταθερή και το μόνο που αλλάζει είναι το μέγεθος της. Στο σημείο αυτό αξίζει να αναφερθεί, ότι για τα πεδία που παρουσιάζουν μικρή χωρική μεταβολή έντασης, το όριο μεταξύ των περιοχών Fresnel και Fraunhofer μπορεί επίσης να προσδιοριστεί μέσω του αριθμού Fresnel:

$$N_F = \frac{d^2}{\lambda z} \tag{2.8}$$

τιμές του οποίου μεγαλύτερες από την μονάδα υποδηλώνουν περίθλαση στην περιοχή του μακρινού πεδίου.

Επί του πρακτέου τώρα, ο υπολογισμός της αναλυτικής λύσης κατά Sommerfeld μπορεί να αποτελέσει μια ιδιαίτερα χρονοβόρα διαδικασία με αρκετά υψηλό υπολογιστικό κόστος. Εντούτοις, το κόστος αυτό δύναται να μειωθεί αισθητά κάνοντας χρήση του θεωρήματος Fourier. Εκτελώντας λοιπόν μια σειρά από κατάλληλες αντικαταστάσεις στη σχέση (2.4), η προαναφερθείσα λύση λαμβάνει την ακόλουθη μορφή [28]:

$$U(P_2) = \iint_{\Sigma} U(P_1)\, h(x-\xi, y-\eta)\, d\xi d\eta \tag{2.9}$$

η οποία συνιστά ένα ολοκλήρωμα συνέλιξης, όπου η h(x,y) αντιστοιχεί στην κρουστική απόκριση (impulse response) της διάδοσης.

$$h(x,y) = \frac{z \exp(jkr)}{j\lambda r^2} \tag{2.10}$$

Συνεπώς, βάσει του θεωρήματος Fourier η εν λόγω λύση μπορεί να εκφραστεί από την ισοδύναμη εξίσωση:

$$U(P_2) = \Im^{-1}\left\{ \Im\left[U(P_1)\right] \Im\left[h(P_1, P_2)\right] \right\} \tag{2.11}$$

ή εναλλακτικά, θεωρώντας ένα κοινό σύστημα συντεταγμένων και για τα δύο επίπεδα παρατήρησης από την:

$$U_2(x,y) = \Im^{-1}\left\{ \Im\left[U_1(x,y)\right] H(f_x, f_y) \right\} \tag{2.12}$$

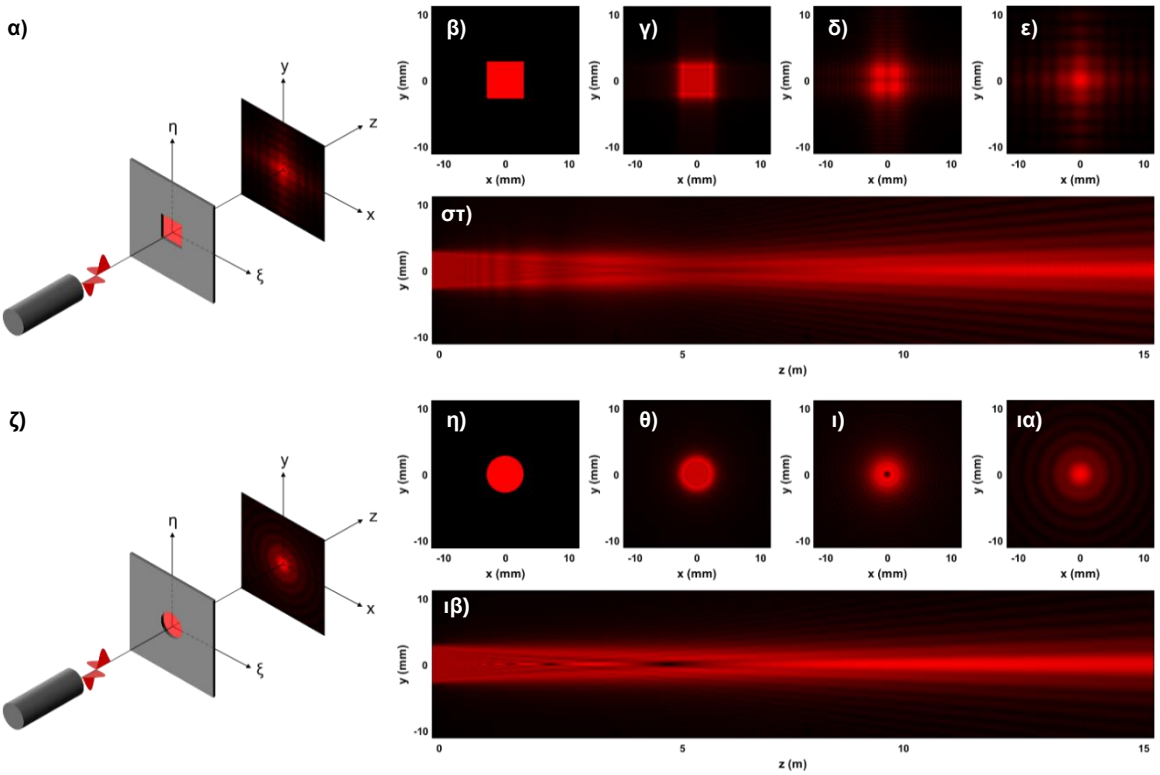
Στην άνωθεν σχέση, οι παράμετροι f_x, f_y αντιπροσωπεύουν τις μεταβλητές της χωρικής συχνότητας για κάθε διάσταση, για τις οποίες ισχύει:

$$\sqrt{f_x^2 + f_y^2} \le \frac{1}{\lambda} \tag{2.13}$$

με $f_x \in [-1/(2dx),+1/(2dx)]$ και $df_x = 1/L_x$, όπου L_x είναι το οριζόντιο μήκος των επιπέδων παρατήρησης. Ομοίως, η χωρική συχνότητα για τον κάθετο άξονα των y δίνεται από τις σχέσεις $f_y \in [-1/(2dy),+1/(2dy)]$ και $df_y = 1/L_y$ αντιστοίχως. Τέλος, η $H(f_x,f_y)$ αποτελεί την συνάρτηση μεταφοράς (transfer function) της διάδοσης, η οποία γράφεται ακολούθως:

$$H\left(f_x, f_y\right) = \exp\left[jkz\sqrt{1-\left(\lambda f_x\right)^2 - \left(\lambda f_y\right)^2} \right] \tag{2.14}$$

Θα πρέπει να σημειωθεί ότι η σωστή επιλογή των τιμών για τις πραγματικές διαστάσεις των επιπέδων παρατήρησης, L_x και L_y, όπως και για τα διαφορικά διακριτοποίησής τους, dx και dy, είναι υψίστης σημασίας, ώστε ο υπολογισμός των παραπάνω σχέσεων να είναι ορθός. Επομένως, προκειμένου να αποφευχθούν υπολογιστικά λάθη, τα οποία οφείλονται κυρίως σε ελλιπή δειγματοληψία, θεωρείται σκόπιμο να εφαρμόζονται οι ακόλουθοι εμπειρικοί κανόνες: οι διαστάσεις των πινάκων υπολογισμού ιδανικά πρέπει να ορίζονται ως δυνάμεις του δύο, τα μήκη των επιπέδων να τίθενται το λιγότερο διπλάσια από το μέγιστο εύρος του τελικού πεδίου που προβάλλεται στο πέτασμα παρατήρησης και τα αντίστοιχα διαφορικά τους να είναι αρκετά μικρότερα από το πηλίκο λz/L [28].



Σχήμα 2.3: α) Διάφραγμα με τετραγωνική διατομή και πλευρά 5mm, που ακτινοβολείται από ένα επίπεδο μονοχρωματικό κύμα στα 635nm. Τα πρότυπα περίθλασης στο εγκάρσιο επίπεδο xy, όπως αυτά υπολογίστηκαν για αποστάσεις ίσες με **β)** z = 1m, **γ)** z = 5m, **δ)** z = 10m και **ε**) z = 15m, μαζί με **ς)** την αντίστοιχη κατανομή της έντασης στο διαμήκες επίπεδο yz. **ζ-ιβ)** Τα αντίστοιχα αποτελέσματα για ένα διάφραγμα κυκλικής διατομής με διάμετρο 5mm

Υπό αυτό το πλαίσιο, στα διαγράμματα του σχήματος 2.3 παρουσιάζεται ένα ενδεικτικό δείγμα από αποτελέσματα προσομοιώσεων, όπως αυτά προέκυψαν για ένα επίπεδο μονοχρωματικό κύμα στα 635nm, το οποίο διέρχεται από δύο διαφορετικά διαφράγματα με ανόμοιο σχήμα αλλά παρεμφερές μέγεθος. Για την εξαγωγή των αποτελεσμάτων αυτών χρησιμοποιήθηκε η σχέση (2.12), η οποία

επελέγη για λόγους ευχρηστίας και ακρίβειας. Το εγκάρσιο επίπεδο παρατήρησης xy σε κάθε περίπτωση ορίστηκε ως ένας πίνακας $2^{13}\times2^{13}$ στοιχείων, που αντιπροσωπεύει ένα τετραγωνικό πέτασμα πλάτους 40mm, από το οποίο παρουσιάζεται μόνο το κεντρικό του τμήμα.

Αναλυτικότερα, όπως φαίνεται από τις αντίστοιχες εικόνες, οι εγκάρσιες κατανομές της έντασης που προκύπτουν για αποστάσεις z = 1m και z = 5m αποτελούν χαρακτηριστικά παραδείγματα από πρότυπα περίθλασης στην περιοχή του εγγύς πεδίου, ενώ αντίθετα όλες οι κατανομές για z = 15m συμπίπτουν με τον μετασχηματισμό Fourier των αρχικών εντάσεων, όπως αυτές προσδιορίζονται για z = 0m, συνιστώντας τα τυπικά πρότυπα περίθλασης εκάστου πεδίου στην περιοχή Fraunhofer.

Εν κατακλείδι, λαμβάνοντας υπόψιν ότι για ένα διάφραγμα με d~2.5mm, το όριο μεταξύ των δύο προαναφερθείσων περιοχών εντοπίζεται κατά προσέγγιση σε απόσταση 9.8m, εξάγεται το συμπέρασμα πως οι παρούσες προσομοιώσεις οδηγούν σε αποτελέσματα που ανταποκρίνονται στην πραγματικότητα και συνάδουν σε ικανοποιητικό βαθμό με την βαθμωτή θεωρία για την περίθλαση, όπως αυτή παρουσιάστηκε στις προηγούμενες παραγράφους.

2.1.2 Περίθλαση Φωτός με Φακό

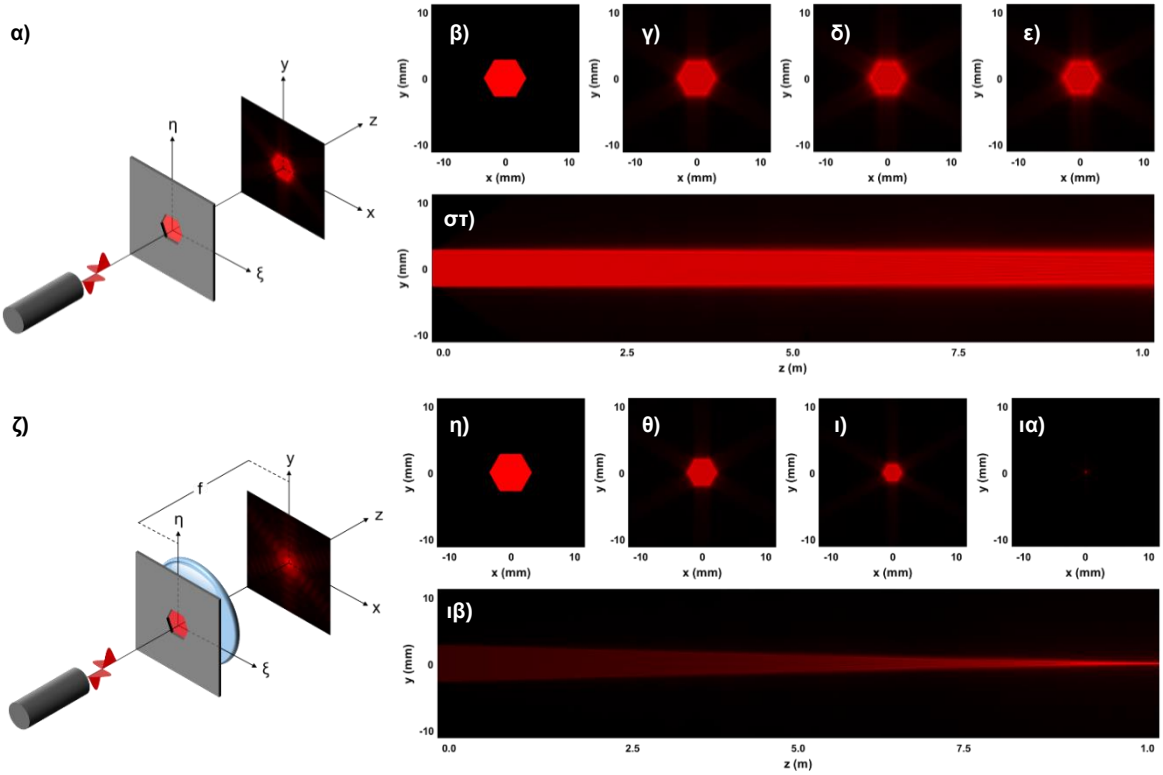
Από την παραπάνω ενότητα γίνεται εύκολα αντιληπτό ότι η παρατήρηση περιθλαστικών φαινομένων στην περιοχή Fraunhofer απαιτεί μεγάλες αποστάσεις διάδοσης, οι οποίες σε πρακτικό επίπεδο είναι αρκετά δύσκολο να επιτευχθούν. Ωστόσο, σύμφωνα με τον αριθμό του Fresnel, ελαττώνοντας το εύρος d του χρησιμοποιούμενου διαφράγματος, η καταγραφή προτύπων περίθλασης, όπως αυτά διαμορφώνονται στην περιοχή μακρινού πεδίου, καθίσταται εφικτή και σε μικρότερα μήκη z. Καθώς όμως η μείωση της διατομής του πεδίου δεν αποτελεί μια ρεαλιστική λύση για την πλειοψηφία των περιπτώσεων, τα ζητούμενα πρότυπα περίθλασης συνήθως λαμβάνονται με την βοήθεια φακών.

Ως γνωστόν, ένας φακός είναι ένα ομογενές οπτικό μέσο με πάχος w_f, δείκτη διάθλασης n_f και δύο διοπτρικές επιφάνειες διαφορετικών καμπυλοτήτων, R_1 και R_2 αντιστοίχως, οι οποίες εκτρέπουν μια προσπίπτουσα ακτίνα φωτός σύμφωνα με τον νόμο του Snell.

Όπως ορίζει λοιπόν η γεωμετρική οπτική, η κατεύθυνση κάθε ακτίνας που εξέρχεται από έναν φακό εξαρτάται, τόσο από την αρχική γωνία πρόσπτωσής της σε αυτόν, όσο και από τις προαναφερθείσες καμπυλότητες των επιφανειών του. Ανάλογα μάλιστα με τις τιμές των καμπυλοτήτων και την επίδραση τους στην πορεία του φωτός, οι φακοί διακρίνονται σε δύο βασικές κατηγορίες, τους συγκλίνοντες και τους αποκλίνοντες. Οι πρώτοι συγκεντρώνουν μια δέσμη παράλληλων ακτινών σε μια απόσταση f, η οποία ονομάζεται εστιακή απόσταση του φακού και δίνεται από τον παρακάτω τύπο

$$\frac{1}{f}=\left(n_f-1\right)\left(\frac{1}{R_1}-\frac{1}{R_2}\right) \tag{2.15}$$

ενώ οι δεύτεροι αντίστοιχα την αποσυγκεντρώνουν. Να σημειωθεί ότι η άνωθεν εξίσωση αναφέρεται στην εστιακή απόσταση λεπτών, συγκλίνοντων ή και αποκλίνοντων φακών, το πάχος των οποίων w_f έχει θεωρηθεί αμελητέο σε σχέση με τις ακτίνες καμπυλοτήτων τους R_1 και R_2 [27].



Σχήμα 2.4: α) Διάφραγμα εξαγωνικής διατομής με πλευρά ~2.88mm, το οποίο ακτινοβολείται από ένα επίπεδο μονοχρωματικό κύμα στα 635nm. Τα πρότυπα περίθλασης στο εγκάρσιο επίπεδο xy, όπως αυτά υπολογίστηκαν για αποστάσεις ίσες με **β)** z = 0m, **γ)** z = 2.5m, **δ)** z = 5.0m και **ε)** z = 1m, μαζί με **ς)** την αντίστοιχη κατανομή της έντασης στο διαμήκες επίπεδο yz. **ζ-ιβ)** Τα αποτελέσματα για το ίδιο διάφραγμα, στο οποίο έχει τοποθετηθεί εφαπτομενικά ένας συγκεντρωτικός φακός εστιακής απόστασης f = 1m.

Υπό κυματική σκοπιά τώρα, η επίδραση ενός φακού σε ένα κύμα οπτικής ακτινοβολίας ουσιαστικά ισοδυναμεί με την εισαγωγή μιας καθυστέρησης φάσης, η οποία οφείλεται στην διαφορά των οπτικών δρόμων που ακολουθούν οι διαδιδόμενες ακτίνες εντός του. Η καθυστέρηση αυτή εκφράζεται μαθηματικά από την συνάρτηση διαπερατότητας [26]:

$$t_f = \exp\left[-j\frac{k}{2f}\left(x^2+y^2\right)\right] \tag{2.16}$$

η οποία αντιπροσωπεύει ένα σφαιρικό μέτωπο κύματος, όπως αυτό διαμορφώνεται για μια απόσταση f από την πηγή του. Συνεπώς, το πεδίο στην έξοδο του φακού ισούται με

$$U_{out} = U_{in} \cdot t_f \tag{2.17}$$

όπου η συνάρτηση t_f μετασχηματίζει το προσπίπτον μέτωπο κύματος από επίπεδο σε σφαιρικό, μεταφράζοντας την τοποθεσία κάθε κάθετης ακτίνας στο επίπεδο εισόδου σε μια αντίστοιχη γωνία διάδοσης στο επίπεδο εξόδου. Ομοίως ισχύει και το αντίστροφο, όπου για τους ίδιους λόγους, τα σφαιρικά κύματα που προέρχονται από μια σημειακή πηγή ακτινοβολίας μετατρέπονται από έναν φακό σε επίπεδα, με τις προσπίπτουσες γωνίες στο επίπεδο εισόδου να μεταφράζονται σε συντεταγμένες θέσεων στο επίπεδο εξόδου. Κατά συνέπεια, κάθε φακός αποτελεί έναν αμφίδρομο μετασχηματισμό φάσης, η εφαρμογή του οποίου αντιστοιχίζει όλες τις γωνίες των ακτινών μιας φωτεινής δέσμης σε συγκεκριμένες χωρικές συντεταγμένες στο επίπεδο και αντιστρόφως. Όπως μάλιστα μπορεί να αποδειχθεί αντικαθιστώντας την σχέση (2.17) στην ολοκληρωτική λύση του Sommerfeld, αυτός ο μετασχηματισμός φάσης για z = f, όπου f η εστιακή απόσταση του φακού,

οδηγεί στον μετασχηματισμό του πεδίου κατά Fourier, το μέτρο του οποίου είναι το πρότυπο περίθλασης στην περιοχή Fraunhofer [26].

Στα διαγράμματα του σχήματος 2.4 παρουσιάζονται οι διαφορές που ανακύπτουν στα πρότυπα περίθλασης ενός διαφράγματος, όταν αυτά καταγράφονται εν απουσία, ή εν παρουσία, ενός λεπτού συγκεντρωτικού φακού με f = 1m. Το παρόν διάφραγμα έχει εξαγωνική διατομή με πλευρά ~2.88mm και ακτινοβολείται από ένα επίπεδο κύμα στα 635nm. Ο φακός τοποθετείται εφαπτομενικά στην επιφάνεια εξόδου του, με το εγκάρσιο επίπεδο παρατήρησης να ορίζεται και σε αυτήν την περίπτωση ως ένας πίνακας $2^{13}\times2^{13}$ στοιχείων που αντιπροσωπεύει ένα τετραγωνικό πέτασμα πλάτους 40mm.

Όπως φαίνεται λοιπόν και από τα αντίστοιχα γραφήματα, τα πρότυπα περίθλασης που προκύπτουν από την ελεύθερη διάδοση του πεδίου, χωρίς τον προαναφερθέντα φακό, παραμένουν εντός της περιοχής του Fresnel για z < 1m. Αντίθετα, στην προσομοίωση με τον φακό παρατηρείται μια ταχεία μετάβαση από το εγγύς στο μακρινό πεδίο, όπου στο εστιακό επίπεδό του εμφανίζεται ο μετασχηματισμός Fourier του αρχικού εξαγώνου. Επομένως, τα εν λόγω αποτελέσματα βρίσκονται σε πλήρη συμφωνία με την αντίστοιχη θεωρία.

2.1.3 Σχηματισμός και Μεγέθυνση Ειδώλου

Είναι προφανές, ότι ο συνδυασμός της ολοκληρωτικής λύσης κατά Sommerfeld, όπως αυτή δίνεται από την εξίσωση (2.4) ή τις ισοδύναμες εκφράσεις (2.11) και (2.12), μαζί με την συνάρτηση διαπερατότητας των φακών (2.16), καθιστά εφικτή την μοντελοποίηση μιας πληθώρας οπτικών συστημάτων, με απλούστερο αυτό της απεικόνισης ειδώλων.

Συνοπτικά, το είδωλο ενός αντικειμένου που απέχει κατά ένα μήκος z_1 από έναν λεπτό συγκεντρωτικό φακό με εστιακή απόσταση f, λαμβάνεται σε ένα πέτασμα παρατήρησης, τοποθετημένο από τον εν λόγω φακό σε μια απόσταση z_2, η οποία πρέπει να ικανοποιεί τον τύπο του Gauss:

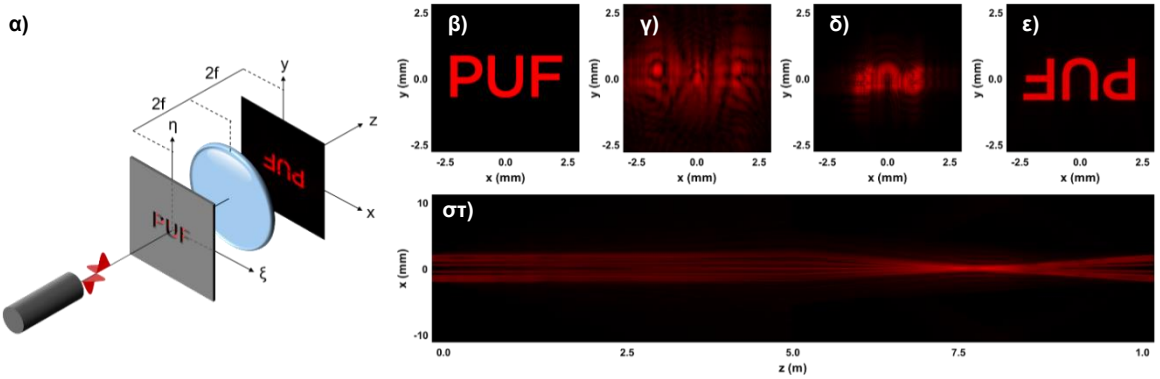
$$\frac{1}{z_1}+\frac{1}{z_2}=\frac{1}{f} \tag{2.18}$$

Εάν $z_1 > f$, τότε το είδωλο αυτό θα είναι πραγματικό και ανεστραμμένο, με την εγκάρσια μεγέθυνση του να δίνεται από την παρακάτω σχέση:

$$M=-\frac{z_2}{z_1} \tag{2.19}$$

Συνεπώς, σύμφωνα με την γεωμετρική οπτική, η σωστή απεικόνιση ενός ειδώλου που έχει πανομοιότυπες διαστάσεις με αυτές του αρχικού αντικειμένου, πραγματοποιείται για $z_1 = z_2 = 2f$ [27], με τα αποτελέσματα του σχήματος 2.5 να έχουν παραχθεί αντιστοίχως, για έναν φακό εστιακής απόστασης 25cm.

Σε αυτό το σημείο πρέπει να υπογραμμισθεί, ότι σε όλες τις άνωθεν προσομοιώσεις δεν έχει ληφθεί καθόλου υπόψιν η κόρη εξόδου των διαφόρων απεικονιστικών διατάξεων, η οποία αντιστοιχεί στο άνοιγμα του τελευταίου οπτικού στοιχείου που περιθλά το φως πριν από την τελική καταγραφή του.



Σχήμα 2.5: α) Διάταξη για την απεικόνιση ειδώλου με μοναδιαία μεγέθυνση, μέσω συγκεντρωτικού φακού με εστιακή απόσταση f = 25cm. Τα πρότυπα περίθλασης που υπολογίστηκαν για αποστάσεις ίσες με **β)** z = 50cm, **γ)** z = 90cm και **δ)** 100cm μαζί με την **στ)** αντίστοιχη κατανομή έντασης επί του επιπέδου xz.

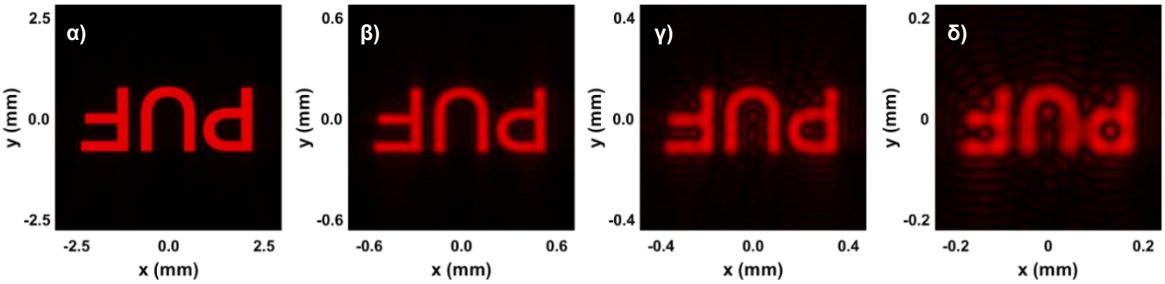
Προκειμένου λοιπόν να συμπεριληφθεί η επίδραση της κόρης εξόδου στην διάταξη του σχήματος 2.5, αρκεί να τροποποιηθεί η συνάρτηση διαπερατότητας του φακού με έναν επιπλέον όρο P(x,y)

$$t_f = \exp\left[-j\frac{k}{2f}\left(x^2+y^2\right)\right]P(x,y) \tag{2.20}$$

ο οποίος στην παρούσα περίπτωση αντιπροσωπεύει ένα άνοιγμα κυκλικής διατομής, όπου R η αντίστοιχη ακτίνα του [28]

$$P(x,y)=\begin{cases}1\ ,\ x^2+y^2\le R^2\\ 0\ ,\ x^2+y^2>R^2\end{cases} \tag{2.21}$$

Εν προκειμένω, στις εικόνες που ακολουθούν παρουσιάζονται τα καινούρια είδωλα που προκύπτουν από την παραπάνω διάταξη, θέτοντας την προαναφερθείσα ακτίνα ίση με R = 5mm και μεταβάλλοντας τις διαστάσεις του αρχικού αντικειμένου.



Σχήμα 2.6:Τα είδωλα που προέκυψαν από την διάταξη 2.4α για ένα σταθερό άνοιγμα φακού με R = 5mm, ελαττώνοντας το μέγεθος του αντικειμένου**. α)** Είδωλο για το αρχικό μέγεθος του αντικειμένου και είδωλα, όπου ο λόγος των διαστάσεων εκάστου αντικειμένου σε σχέση με το αρχικό είναι **β)** 1:4 **γ)** 1:6 και **δ)** 1:8.

Όπως φαίνεται λοιπόν από τις αντίστοιχες εικόνες, το είδωλο που παρατηρείται για το αντικείμενο με τις μέγιστες χρησιμοποιούμενες διαστάσεις αποτελεί ένα ανεστραμμένο και ακριβές αντίγραφό του, όπως αυτό προβλέπεται από την θεωρία της γεωμετρικής οπτικής. Καθώς όμως το μέγεθος του αντικειμένου αρχίζει να μειώνεται, ελαττώνεται και η ευκρίνεια των ληφθείσων εικόνων: οι ακμές των ειδώλων γίνονται όλο και πιο ασαφείς ενώ παρατηρείται και η προοδευτική εμφάνιση ενός είδους κυματικών παραμορφώσεων που οφείλονται στην περίθλαση της ακτινοβολίας από το άνοιγμα του φακού.

Με άλλα λόγια, η περίθλαση του φωτός από την κόρη εξόδου ελαττώνει την διακριτική ικανότητα του συστήματος. Ο όρος διακριτική ικανότητα αναφέρεται στην δυνατότητα του εκάστοτε απεικονιστικού συστήματος να διαχωρίζει τις μικρές

λεπτομέρειες ενός αντικειμένου που βρίσκονται σε κοντινή γωνιακή απόσταση και καθορίζεται από το κριτήριο του Rayleigh, βάσει του οποίου ερμηνεύονται τα παραπάνω αποτελέσματα ακολούθως.

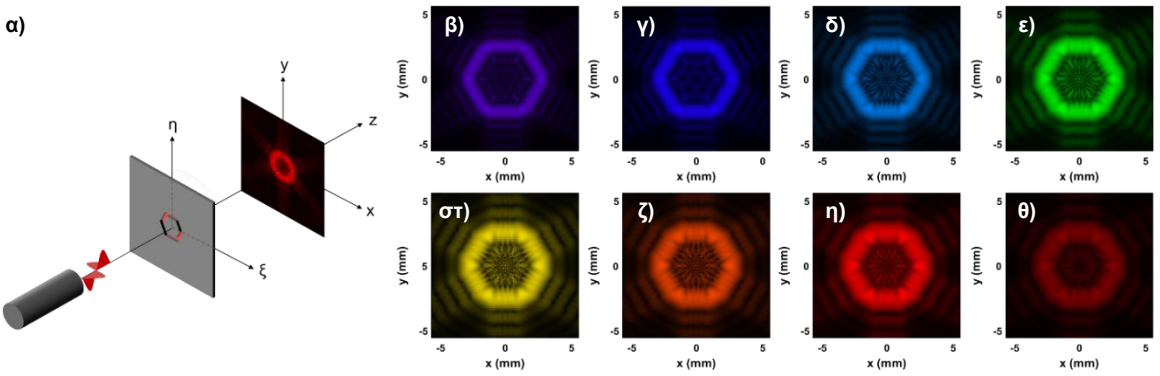
Όπως μπορεί να αποδειχθεί, η εικόνα ενός αντικειμένου, όπως αυτή διαμορφώνεται στο επίπεδο παρατήρησης ενός ιδανικού συστήματος απεικόνισης [2], είναι το αποτέλεσμα της συνέλιξης μεταξύ 1) του μετασχηματισμού Fourier επί του ανοίγματος P(x,y) και 2) του ειδώλου που αναμένεται βάσει των αρχών της γεωμετρικής οπτικής [26]. Επίσης είναι προφανές ότι ο μετασχηματισμός Fourier του παρόντος ανοίγματος P(x,y) συμπίπτει με το πρότυπο περίθλασης από μια στρογγυλή οπή στην περιοχή του Fraunhofer (σχήμα 2.3.ια), το οποίο παρουσιάζει μια κεντρική φωτεινή κηλίδα που αποκαλείται δίσκος Airy. Η ακτίνα ρ του δίσκου Airy δίνεται από την σχέση [27]:

$$\rho = 1.22\frac{\lambda f}{2R} \qquad (2.22)$$

η οποία είναι μια εναλλακτική μορφή του προαναφερθέντος κριτηρίου. Σύμφωνα λοιπόν με την παραπάνω εξίσωση, η ακτίνα ρ είναι αντιστρόφως ανάλογη του R, γεγονός που υποδηλώνει ότι η ικανότητα εστίασης ενός φακού αυξάνει όσο το εύρος ανοίγματος αυτού ελαττώνεται. Ταυτόχρονα όμως, το συνολικό πρότυπο περίθλασης διευρύνεται, καθώς οι κροσσοί συμβολής απομακρύνονται από τον εν λόγω δίσκο, με το άνοιγμα P(x,y) να αποκλείει την περαιτέρω διάδοσή τους, ουσιασικά δρώντας ως χαμηλοπερατό φίλτρο που αποκόπτει τις υψηλές συχνότητες και μειώνει την οξύτητα της εικόνας.

2.1.4 Περίθλαση με Διαφορετικά Μήκη Κύματος

Επιστρέφοντας στην εξίσωση (2.8), η αντιστρόφως ανάλογη εξάρτηση που εμφανίζει ο αριθμός Fresnel από το μήκος κύματος της διαδιδόμενης ακτινοβολίας συνεπάγεται ότι όταν η τιμή του λ αυξάνεται και μετακινείται προς το ερυθρό, η εκδήλωση των διαφόρων περιθλαστικών φαινομένων καθίσταται εντονότερη, με το όριο των περιοχών Fresnel και Fraunhofer να μετατοπίζεται σε μεγαλύτερες αποστάσεις z.



Σχήμα 2.7: α) Διάφραγμα με διατομή εξαγωνικού πλαισίου, εξωτερικής πλευράς 2.88mm και εύρους 0.5mm, το οποίο ακτινοβολείται από ένα μονοχρωματικό κύμα στα **β)** 420nm, **γ)** 460nm, **δ)** 480nm, **ε)** 532nm, **στ)** 573nm, **ζ)** 600nm, **η)** 635nm και **θ)** 665nm. Οι εικόνες περίθλασης που προέκυψαν σε κάθε περίπτωση αντιστοιχούν για μια απόσταση διάδοσης ίση με z = 80cm.

[2] Στα ιδανικά συστήματα απεικόνισης (diffraction-limited systems) δεν λαμβάνονται υπόψιν τα σφάλματα από μεγάλες γωνίες πρόσπτωσης (paraxial approximation) και ατέλειες φακών (aberrations)

Από τις εικόνες λοιπόν του σχήματος 2.7 παρατηρείται ότι τα πρότυπα περίθλασης που παράγονται από το χρησιμοποιούμενο μοντέλο για ένα διάφραγμα με σταθερή διατομή, πράγματι εμφανίζουν εντονότερους κροσσούς συμβολής και βρίσκονται πιο κοντά στην περιοχή μακρινού πεδίου όσο το μήκος κύματος της ακτινοβολίας αυξάνει.

Αξίζει να αναφερθεί ότι στα πλαίσια του παρόντος μοντέλου, η ψηφιακή αναπαράσταση της χρωματικής πληροφορίας που εμπεριέχεται σε κάθε μήκος κύματος του ορατού φάσματος πραγματοποιήθηκε με χρήση των χώρων CIE XYZ και sRGB, η σύντομη περιγραφή των οποίων παρατίθεται στις επόμενες υποενότητες.

2.1.4.1 Χρωματικός Χώρος XYZ

Ο χρωματικός χώρος CIE XYZ εισήχθη από τη Διεθνή Επιτροπή Φωτισμού (Commission Internationale de l'Eclairage - CIE) το 1931 και έκτοτε αποτελεί ένα καθιερωμένο σύστημα αναφοράς, με το οποίο καθίσταται εφικτή η μαθηματική περιγραφή και ταξινόμηση κάθε πιθανού χρώματος. Περιλαμβάνει τρεις κύριες συνιστώσες, η μίξη των οποίων επιτρέπει την ποσοτικοποίηση οποιουδήποτε μήκους κύματος λ στο ορατό, λαμβάνοντας υπόψιν την φασματική απόκριση του ανθρώπινου οφθαλμού, καταγεγραμμένη υπό ορισμένες συνθήκες φωτισμού και γωνίες παρατήρησης.

Συγκεκριμένα, το κύριο χρώμα οποιουδήποτε αντικειμένου, όπως αυτό γίνεται αντιληπτό από τους φωτοϋποδοχείς ενός ανθρώπινου οφθαλμού, αντιστοιχεί σε ένα σύνολο τριών παραμέτρων που προκύπτουν από τις ακόλουθες σχέσεις [29]:

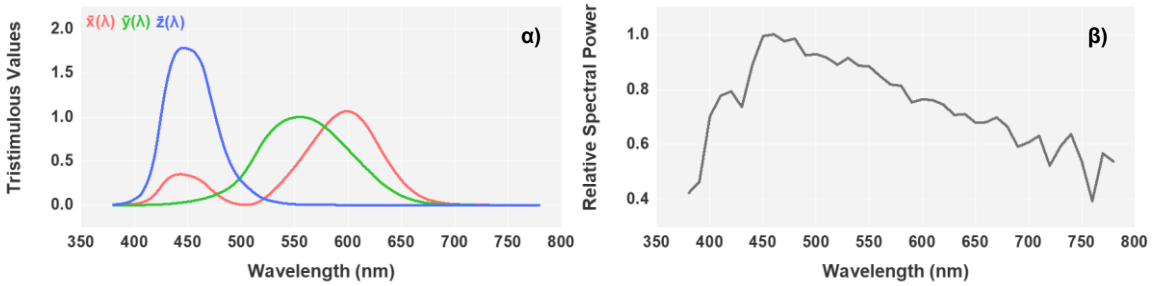
$$X = k\sum_{\lambda} S(\lambda)R(\lambda)\bar{x}(\lambda) \tag{2.23}$$

$$Y = k\sum_{\lambda} S(\lambda)R(\lambda)\bar{y}(\lambda) \tag{2.24}$$

$$Z = k\sum_{\lambda} S(\lambda)R(\lambda)\bar{z}(\lambda) \tag{2.25}$$

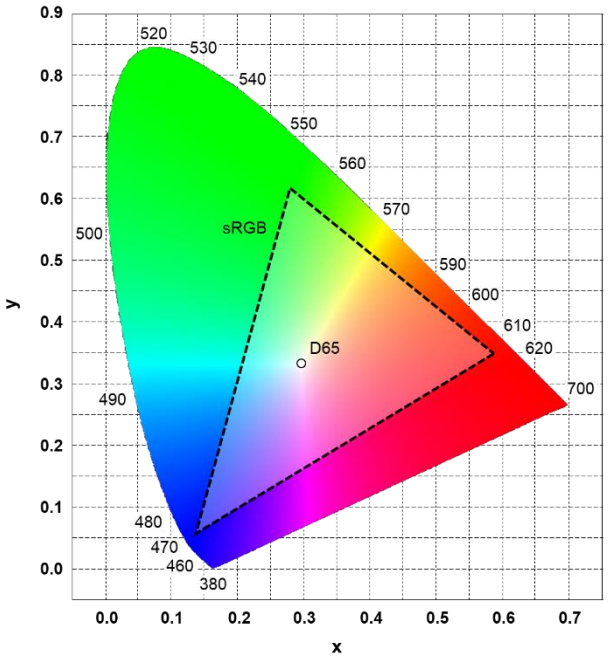
όπου S(λ) είναι η φασματική κατανομή της χρησιμοποιούμενης πηγής φωτισμού και R(λ) η ανακλαστικότητα του παρατηρούμενου αντικειμένου. Οι συντελεστές βάρους $\bar{x}$, $\bar{y}$ και $\bar{z}$ (Color Matching Functions - CMF) ουσιαστικά αντιπροσωπεύουν τις αναλογίες των τριών βασικών χρωμάτων (κόκκινο, πράσινο και μπλε) που πρέπει να αναμιχθούν, ώστε να γίνει αντιληπτό ένα δεδομένο μήκος κύματος σύμφωνα με τη μέση ανθρώπινη φυσιολογία υπό συγκεκριμένη γωνία παρατήρησης, ενώ το k αποτελεί μια σταθερά βαθμονόμησης, η οποία δίνεται από την εξίσωση:

$$k = \frac{100}{\sum_{\lambda} S(\lambda)\bar{x}(\lambda)} \tag{2.26}$$



Σχήμα 2.8: α) Οι κατανομές των color matching functions $\bar{x}(\lambda)$, $\bar{y}(\lambda)$ και $\bar{z}(\lambda)$ όπως αυτές καταγράφηκαν για μία γωνία παρατήρησης 2°. **β)** Η φασματική κατανομή της πρότυπης πηγής φωτισμού D65.

Στο σχήμα 2.8α παρουσιάζονται οι κατανομές των CMF για γωνία παρατήρησης ίση με 2^o, ενώ στο σχήμα 2.8β επιδεικνύεται το φάσμα εκπομπής που προέρχεται από την πρότυπη πηγή φωτισμού D65, η οποία αντιστοιχεί σε ηλιακό φως ημέρας [30].



Σχήμα 2.9: Το διάγραμμα χρωματικότητας CIE xyY, στην περίμετρο του οποίου σημειώνονται όλα τα χρώματα του φάσματος από τα 380 έως τα 700 nm.

Στο σημείο αυτό θα πρέπει να σημειωθεί, ότι σε πρακτικό επίπεδο, αντί των προαναφερθέντων συνιστωσών XYZ συνήθως χρησιμοποιούνται οι κανονικοποιημένες εκδοχές τους x = X/(X+Y+Z), y = Y/(X+Y+Z) και z = Z/(X+Y+Z) = 1-x-y, οι οποίες αντιστοιχούν στις λεγόμενες συντεταγμένες χρωματικότητας. Οι συντεταγμένες χρωματικότητας ουσιαστικά απαρτίζουν ένα ισοδύναμο χρωματικό μοντέλο που ονομάζεται CIE xyY, το δισδιάστατο γράφημα του οποίου (σχήμα 2.9) είναι ένα από τα πιο διαδεδομένα εργαλεία για την αντιπαραβολή του χρωματικού εύρους διαφορετικών χρωματικών χώρων.

2.1.4.2 Χρωματικός Χώρος Standard RGB (sRGB)

Συνοπτικά, το χρωματικό μοντέλο sRGB εισήχθη το 1996 από τις εταιρείες Microsoft και HP για την υποστήριξη οθονών CRT και αποτελεί ένα περιορισμένο υποσύνολο των χρωματικών χώρων XYZ και xyY, όπως φαίνεται και από το διάγραμμα χρωματικότητας του σχήματος 2.9. Οι τιμές των τριών συνιστωσών του, R′, G′ και B′, προσδιορίζονται σε δύο βήματα [31]. Αρχικά εκτελείται ο γραμμικός μετασχηματισμός:

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 3.2410 & -1.5374 & -0.4986 \\ -0.9692 & 1.8760 & 0.0416 \\ 0.0556 & -0.2040 & 1.0570 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \quad (2.27)$$

στις ευρεθείσες τριχρωματικές παραμέτρους του χρωματικού χώρου XYZ, εκ των οποίων αποκόπτονται τα αρνητικά αποτελέσματα, και στη συνέχεια εφαρμόζεται μια μη γραμμική συνάρτηση, που είναι γνωστή ως διόρθωση γάμμα, η οποία συμπιέζει την χρωματική παλέτα του μοντέλου ακολούθως:

Για R,G,B ≤ 0.00304

$$\begin{bmatrix} R' \\ G' \\ B' \end{bmatrix} = 12.92 \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.28}$$

Για R,G,B > 0.00304

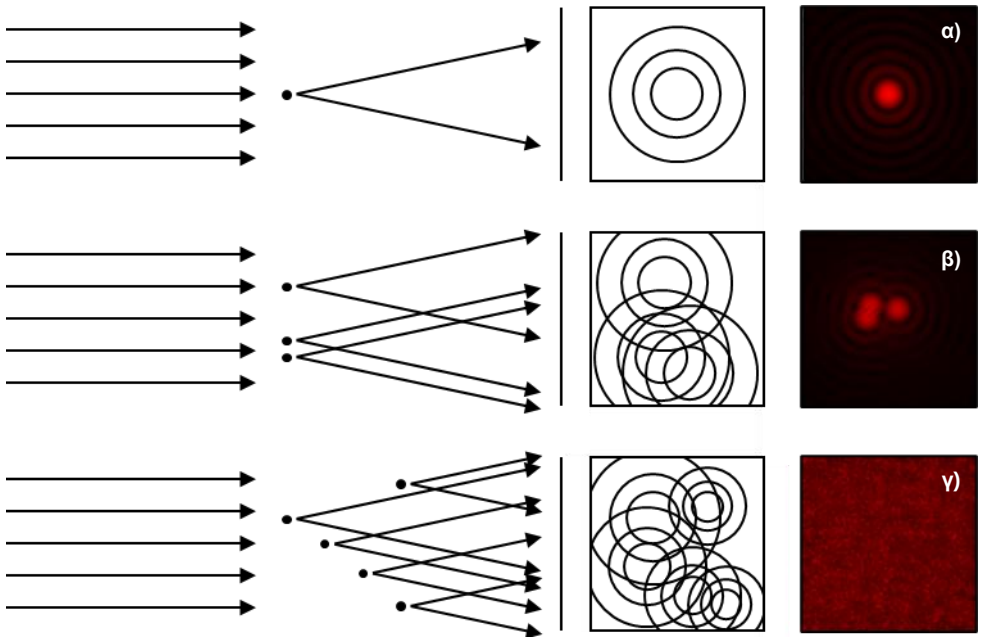
$$\begin{bmatrix} R' \\ G' \\ B' \end{bmatrix} = 1.055 \begin{bmatrix} R \\ G \\ B \end{bmatrix}^{\frac{1}{2.4}} - 0.055 \tag{2.29}$$

2.2 Κλασσική Θεωρία Speckle Pattern

Ανατρέχοντας στη θεωρία της προηγούμενης υποενότητας, όπως έχει ήδη ειπωθεί, το πρότυπο περίθλασης Fraunhofer από ένα διάφραγμα με κυκλική διατομή (σχήμα 2.3ια) παρουσιάζει μια κεντρική φωτεινή περιοχή που ονομάζεται δίσκος Airy. Για ένα απλό απεικονιστικό σύστημα ειδώλου, η ακτίνα ρ του δίσκου Airy δίνεται από την εξίσωση (2.22), η οποία απουσία φακών μπορεί να επαναδιατυπωθεί ακολούθως:

$$\rho = 1.22\frac{\lambda z}{2R} \Rightarrow \sin\theta = \frac{1.22\lambda}{2R} \tag{2.30}$$

όπου z η τεθείσα απόσταση του επιπέδου παρατήρησης στο μακρινό πεδίο, R η ακτίνα του χρησιμοποιούμενου κυκλικού διαφράγματος και θ η γωνία στην οποία εμφανίζεται ο πρώτος σκοτεινός δακτύλιος του σχηματιζόμενου προτύπου. Το δεξί σκέλος της (2.30) αποτελεί και το προαναφερθέν κριτήριο του Rayleigh, το οποίο ουσιαστικά καθορίζει τη γωνιακή διακριτική ικανότητα του συστήματος, θέτοντας την οριακή συνθήκη υπό την οποία δύο πρότυπα περίθλασης παραμένουν ακόμη ευκρινή [27].



Σχήμα 2.10: Πρότυπα περίθλασης, όπως αυτά σχηματίζονται στην περιοχή του Fraunhofer, **α)** από μία πηγή σφαιρικών κυμάτων, **β)** τρεις πηγές σφαιρικών κυμάτων που ισαπέχουν από το πέτασμα παρατήρησης, εκ των οποίων οι δύο είναι οριακά διακριτές και **γ)** ~2500 περίπου σημειακές πηγές με τυχαίες αποστάσεις από το εν λόγω πέτασμα.

Σύμφωνα λοιπόν με το κριτήριο του Rayleigh, τα πρότυπα περίθλασης που προέρχονται από δυο πηγές σφαιρικών κυμάτων μπορούν να διαχωριστούν οριακά, όταν η μεταξύ τους γωνιακή απόσταση είναι το λιγότερο θ, όταν δηλαδή το

κεντρικό μέγιστο του ενός επικαλύπτει το πρώτο ελάχιστο του άλλου. Στην περίπτωση που το κριτήριο αυτό παραβιάζεται, τα δύο πρότυπα δεν είναι πλέον διακριτά, το πλάτος του πεδίου στην περιοχή του Fraunhofer προκύπτει από το άθροισμα των πλατών εκάστης πηγής και το πλήθος των πηγών ακτινοβολίας καθίσταται απροσδιόριστο.

Υπό αυτό το πλαίσιο, στο σχήμα 2.10γ παρουσιάζεται το πρότυπο περίθλασης που σχηματίζεται από ένα σύνολο παρακείμενων πηγών ακτινοβολίας, με τυχαία κατανομή θέσεων ως προς το αρχικό επίπεδο παρατήρησης και ανεπαρκή τη μέση γωνιακή τους απόσταση. Το εν λόγω πρότυπο ουσιαστικά αντιστοιχεί σε μια πολύπλοκη κατανομή αυξομειώσεων στην ένταση του παρατηρούμενου Η/Μ πεδίου, οι οποίες οφείλονται στις τυχαίες ενισχυτικές και καταστρεπτικές συμβολές των επιμέρους συνιστωσών εκάστης πηγής. Με άλλα λόγια, το κοκκώδες αποτέλεσμα του παρακάτω σχήματος προκύπτει από την επαλληλία ενός μεγάλου πλήθους κυμάτων, τα οποία, λόγω των διαφορετικών αποστάσεων που διανύουν, συμβάλλουν στο επίπεδο παρατήρησης με μια μικρή διαφορά στην φάση και το πλάτος τους.

Εν γένει, οποιαδήποτε χωρική κατανομή έντασης που παρουσιάζει την χαρακτηριστική κοκκώδη όψη του άνωθεν σχήματος είθισται να ονομάζεται speckle pattern. Επομένως, η μεθοδολογία των πολλαπλών οπών, όπως αυτή περιγράφηκε στην προηγούμενη παράγραφο και χρησιμοποιήθηκε για την εξαγωγή του εικονιζόμενου αποτελέσματος, αποτελεί μία από τις απλούστερες δυνατές προσεγγίσεις για την παραγωγή παρόμοιων εικόνων. Δεδομένου όμως του μεγάλου πλήθους από διαφορετικές συνθήκες, υπό τις οποίες προξενούνται τέτοια περίπλοκα φαινόμενα, οι αριθμητικές μέθοδοι που δύναται να εφαρμοστούν για την προσομοίωση ενός τυπικού speckle pattern είναι ποικίλες.

Ενδεικτικά, οι συνηθέστερες φυσικές διεργασίες που οδηγούν στον σχηματισμό ενός speckle είναι:

- η απεικόνιση του ειδώλου μιας ανάγλυφης επιφάνειας με ανωμαλίες που δεν είναι διακριτές από το χρησιμοποιούμενο οπτικό σύστημα
- η διάδοση φωτός σε ένα διαταραγμένο οπτικό μέσο (turbulent medium)
- η σκέδαση ακτινοβολίας από ένα μέσο με τυχαίες διακυμάνσεις στον μιγαδικό δείκτη διάθλασής του
- η διάχυση μιας δέσμης σύμφωνου φωτός από μια ανάγλυφη επιφάνεια με μεγάλη τραχύτητα
- και η συμβολή των ρυθμών διάδοσης μιας πολύτροπης οπτικής ίνας.

Από τις διεργασίες αυτές, το παρόν κεφάλαιο επικεντρώνεται στις δύο τελευταίες με την τρέχουσα ενότητα κυρίως να εστιάζεται στην αλληλεπίδραση μιας γραμμικά πολωμένης μονοχρωματικής δέσμης laser με μια τραχιά επιφάνεια.

Στο σημείο αυτό αξίζει να επισημανθεί ότι οι διεργασίες που οδηγούν στον σχηματισμό speckle patterns είναι κατά κανόνα στατιστικές και τα μορφολογικά χαρακτηριστικά των παραγόμενων εικόνων συνήθως υπακούουν σε συγκεκριμένες κατανομές, εφόσον τα στατιστικά γνωρίσματα της πηγής και του χρησιμοποιούμενου υλικού μέσου πληρούν ορισμένους περιορισμούς. Συνεπώς, η θεωρία που επιτρέπει την μαθηματικοποιημένη περιγραφή ενός speckle pattern δύναται να εφαρμοστεί σε οποιαδήποτε διαδικασία σχηματισμού του, με την ακριβή μοντελοποίηση του υποκείμενου φαινομένου να μην θεωρείται πάντοτε αναγκαία [32].

Έστω λοιπόν μια σχετικά σύμφωνη δέσμη γραμμικά πολωμένου και μονοχρωματικού φωτός που προσπίπτει σε μια επιφάνεια γεμάτη προεξοχές, με τυχαία ύψη, τα οποία ακολουθούν μια τυπική κανονική κατανομή και διαφέρουν κατά μέσο όρο περισσότερο από το μήκος κύματος της χρησιμοποιούμενης ακτινοβολίας. Σύμφωνα με την αρχή των Huygens και Fresnel, το μέτωπο κύματος που διαμορφώνεται από την αλληλεπίδραση της δέσμης με την ανάγλυφη υφή της εν λόγω επιφάνειας, συνίσταται από ένα σύνολο N δευτερογενών σημειακών πηγών, τα σφαιρικά κύματα των οποίων συμβάλλουν με μια τυχαία διαφορά φάσης και πλάτους σε ένα πέτασμα παρατήρησης, τοποθετημένο στην περιοχή του Fraunhofer. Ως εκ τούτου, το μιγαδικό πλάτος του πεδίου U(x,y,z) στο πέτασμα αυτό ισούται με το άθροισμα των συνεισφορών κάθε πηγής:

$$U(x,y,z)=\sum_{k=1}^{N}\frac{1}{\sqrt{N}}\,\alpha_k(x,y,z)=\frac{1}{\sqrt{N}}\sum_{k=1}^{N}|\alpha_k|e^{i\varphi_k} \qquad (2.31)$$

όπου α_k το πλάτος και φ_k η φάση του τυχαίου φάσορα που προκύπτει από την k-οστή πηγή αντιστοίχως. Θεωρώντας ότι

- οι δευτερογενείς πηγές αντιπροσωπεύουν τα κέντρα σκέδασης της επιφάνειας
- τα κέντρα σκέδασης είναι ομοιογενώς κατανεμημένα και με τυχαίο τρόπο σε αυτήν
- τα πλάτη α_k αποτελούν ένα σύνολο στατιστικά ανεξάρτητων μεταβλητών
- οι φάσεις φ_k είναι ομοιογενώς κατανεμημένες στο διάστημα [-π,+π] και είναι στατιστικά ανεξάρτητες τόσο μεταξύ τους όσο και σε σχέση με τα πλάτη α_k
- η επιφάνεια δεν μεταβάλλει την πόλωση του προσπίπτοντος φωτός

τότε η εξίσωση (2.31) αντιστοιχεί σε μια στοχαστική διαδικασία, η οποία συμπίπτει με το διαδεδομένο πρόβλημα του τυχαίου περιπάτου στο μιγαδικό επίπεδο. Όταν μάλιστα το πλήθος των σκεδαστών N προσεγγίζει το άπειρο, η άνωθεν εξίσωση αντιστοιχεί σε ένα κανονικοποιημένο άθροισμα από ανεξάρτητες τυχαίες μεταβλητές, το οποίο τείνει σε μια κυκλική γκαουσιανή στοχαστική διεργασία.

Όπως λοιπόν μπορεί να αποδειχθεί, βάσει των ανωτέρω παραδοχών και σύμφωνα με το κεντρικό οριακό θεώρημα (Central Limit Theorem), το πραγματικό Res[U(x,y,z)] και το φανταστικό μέρος Im[U(x,y,z)] του παραπάνω αθροίσματος είναι δύο σύνολα από στατιστικώς ανεξάρτητες τυχαίες μεταβλητές που ακολουθούν μια κανονική κατανομή με μηδενική μέση τιμή και πανομοιότυπη διακύμανση. Η κατανομή της από κοινού πιθανότητας των δύο αυτών μεγεθών είναι επίσης κανονική, επομένως και το μέτρο του μιγαδικού πλάτους |U(x,y,z)| υπακούει στη κατανομή Rayleigh. Επιπρόσθετα, η ένταση $I = |U(x,y,z)|^2$ του H/M πεδίου ακολουθεί μια αρνητική εκθετική κατανομή (negative exponential distribution), η μέση τιμή της οποίας <I> ισούται με την αντίστοιχη τυπική της απόκλιση $\sigma = [<(I-<I>)>]^{1/2}$ [33][34]

$$p\left(|U(x,y,z)|^2\right)=p(I)=\frac{1}{\langle I\rangle}\exp\left(-\frac{I}{\langle I\rangle}\right) \qquad (2.32)$$

Σε αυτό το σημείο κρίνεται δέον να εισαχθεί το μέγεθος της φωτοαντίθεσης C (contrast), το οποίο υπολογίζεται από τον λόγο της προαναφερθείσας τυπικής απόκλισης σ προς την μέση ένταση <I> και ιδανικά ισούται με την μονάδα, αφού οι δύο χρησιμοποιούμενες ποσότητες έχουν την ίδια τιμή. Ειδικότερα, η C είναι αντιστρόφως ανάλογη του λόγου σήματος προς θόρυβο (signal to noise ratio -

SNR), με οποιαδήποτε απόκλιση της από την αναμενόμενη τιμή 1 να υποδηλώνει την υποβάθμιση της ποιότητας του υπό μελέτη speckle από την παρουσία μετρητικού θορύβου [35]

$$\mathrm{SNR} = \frac{1}{C} = \frac{\langle I \rangle}{\sigma} \tag{2.33}$$

Συνεπώς, η συνάρτηση πυκνότητας πιθανότητας (Probability Density Function - PDF) p(I) και η φωτοαντίθεση C ενός speckle pattern επιτρέπουν την στατιστική περιγραφή των διακυμάνσεων στην παρατηρούμενη φωτεινότητά του. Από την άλλη πλευρά, το φάσμα ισχύος Wiener (Power Spectral Density - PSD) και η συνάρτηση αυτοσυσχέτισης (Autocorrelation Function - ACF) αυτού παρέχουν πληροφορίες για τον ρυθμό με τον οποίο εναλλάσονται οι εν λόγω διακυμάνσεις στο επίπεδο παρατήρησης· με άλλα λόγια επιτρέπουν τον υπολογισμό των διαστάσεων των κόκκων του [33]–[35].

Συγκεκριμένα, η συσχέτιση μεταξύ δύο εντάσεων I_1 και I_2 για ένα ζεύγος σημείων (x_1,y_1) και (x_2,y_2) στο επίπεδο ενός speckle, προσδιορίζεται μέσω της από κοινού πιθανότητας τους $p(I_1,I_2)$, η κατανομή της οποίας, όπως ισχύει για οποιαδήποτε PDF μιας κυκλικής γκαουσιανής τυχαίας διεργασίας [34], καθορίζεται με απόλυτο τρόπο από τη συνάρτηση αυτοσυσχετίσεως τους:

$$\mathrm{ACF}(\Delta x, \Delta y) = \langle I_1 I_2 \rangle = \langle I(x_1, y_1) I(x_2, y_2) \rangle \tag{2.34}$$

όπου $\Delta x = x_2 - x_1$ και $\Delta y = y_2 - y_1$. Συνήθως, η συνάρτηση αυτοσυσχετίσεως υπολογίζεται μέσω του θεωρήματος Wiener - Khinchin, το οποίο διατυπώνεται ακολούθως:

$$\mathrm{ACF}(x,y) = \langle I(x,y) I(0,0) \rangle = \Im^{-1}\{\mathrm{PSD}[I(x,y)]\} \tag{2.35}$$

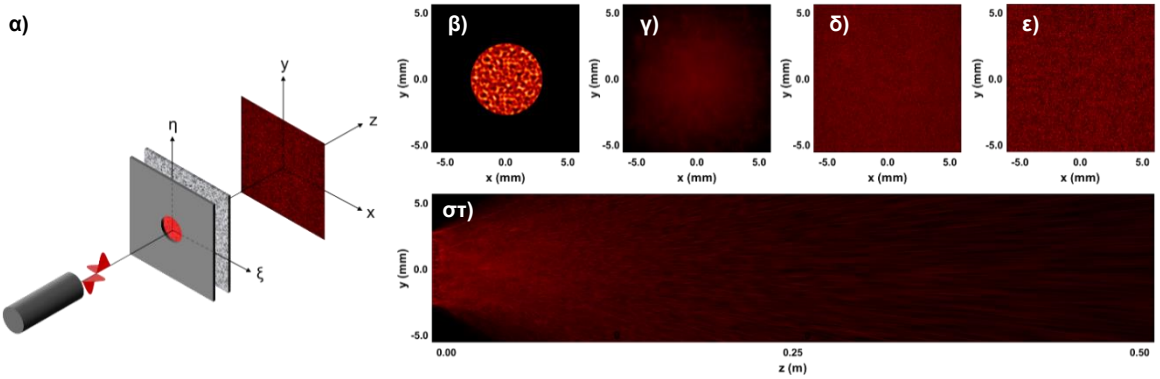
με PSD[I(x,y)] το προαναφερθέν φάσμα ισχύος Wiener του υπό μελέτη speckle pattern:

$$\mathrm{PSD}[I(x,y)] = \left|\Im[I(x,y)]\right|^2 \tag{2.36}$$

Το εύρος της συνάρτησης αυτής ισοδυναμεί και με το ελάχιστο μέγεθος των κηλίδων από τις οποίες απαρτίζεται το υπό μελέτη speckle.

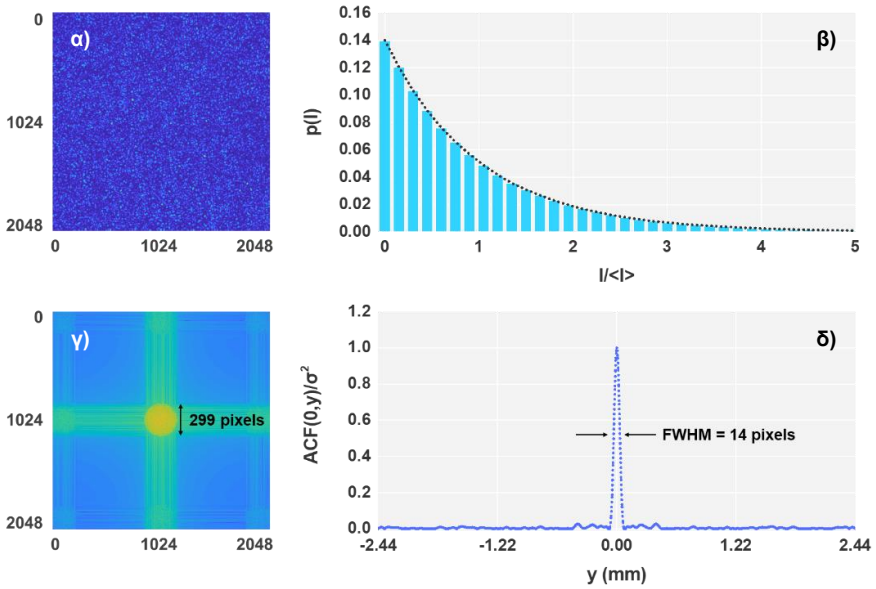
Αξίζει επιπλέον να αναφερθεί ότι στη περίπτωση της ελεύθερης διάδοσης ενός speckle, το πλάτος της φωτιζόμενης επιφάνειας αποτελεί το τελευταίο περιθλόν άνοιγμα της διάταξης και επομένως επιδρά ως κόρη εξόδου του χρησιμοποιούμενου συστήματος, καθορίζοντας την γωνιακή διακριτική ικανότητά του. Σύμφωνα λοιπόν με το κριτήριο του Rayleigh το μέγεθος των κηλίδων ενός speckle είναι αντιστρόφως ανάλογο της διατομής που ακτινοβολείται και μάλιστα δύναται να υπολογιστεί εκ των προτέρων από την ακτίνα του δίσκου Airy.

Υπό αυτό το πλαίσιο, στις εικόνες του σχήματος 2.11 παρουσιάζονται τα αποτελέσματα των προσομοιώσεων που προέκυψαν από την αλληλεπίδραση μιας μονοχρωματικής και γραμμικά πολωμένης δέσμης, με μήκος κύματος στα 635nm και διαμέτρο στα 5mm, με μια επιφάνεια μεγάλης τραχύτητας, οι τυχαίες προεξοχές της οποίας έχουν μέγιστο ύψος 15μm και εύρος 117μm. Το εγκάρσιο επίπεδο παρατήρησης xy, και σε αυτή την περίπτωση, ορίστηκε ως ένας πίνακας 8192×8192 στοιχείων που αντιστοιχεί σε ένα τετραγωνικό πέτασμα πλάτους 40mm, από το οποίο επιδεικνύεται μόνο μια κεντρική περιοχή διαστάσεων 10mm.



Σχήμα 2.11: α) Διάταξη για δημιουργία speckle pattern στην περιοχή Fraunhofer: Ένα επίπεδο κύμα στα 635nm διέρχεται από ένα κυκλικό διάφραγμα διαμέτρου 5mm, στο οποίο έχει τοποθετηθεί εφαπτομενικά μια επιφάνεια μεγάλης τραχύτητας. **β)** Το heatmap της επιφάνειας, οι προεξοχές της οποίας ακολουθούν μια κανονική κατανομή, έχουν μέγιστο ύψος 15μm και μέσο εύρος ~117μm. Τα speckle patterns στο εγκάρσιο επίπεδο xy, όπως αυτά υπολογίστηκαν για αποστάσεις ίσες με **γ)** z = 5cm, **δ)** z = 25cm και **ε)** z = 50cm, μαζί με **στ)** την αντίστοιχη κατανομή της έντασης στο διαμήκες επίπεδο yz.

Ακολούθως, στο σχήμα 2.12 επιδεικνύεται η συνάρτηση πυκνότητας πιθανότητας p(I) για την ένταση της εικόνας 2.11ε, συνοδευόμενη από το προκύπτον φάσμα ισχύος και την αντίστοιχη συνάρτηση αυτοσυσχετίσεως της, όπως αυτή εξήχθη κατά μήκος του άξονα y.



Σχήμα 2.12: α) Το speckle pattern που σχηματίζεται από μια επιφάνεια πλάτους 5mm σε απόσταση 50cm, μαζί με **β)** την συνάρτηση πυκνότητα πιθανότητας της έντασης, **γ)** το φάσμα ισχύος Wiener και **δ)** την συνάρτηση αυτοσυσχετίσεως ως προς τον άξονα y.

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι η παρεμβολή οποιουδήποτε φακού στον οπτικό δρόμο ενός speckle δεν επιφέρει καμία ουσιαστική διαφοροποίηση στα τελικά στατιστικά χαρακτηριστικά του [33][34]. Επομένως, η άνωθεν μαθηματική προσέγγιση μπορεί να εφαρμοστεί αυτούσια σε όλα τα γραμμικά πολωμένα speckle patterns που προέρχονται από μια μονοχρωματική πηγή σύμφωνης ακτινοβολίας και προσπίπτουν σε ένα αδιαφανές πέτασμα παρατήρησης εντός της περιοχής του Fraunhofer. Ωστόσο, για την ρεαλιστική μοντελοποίηση της υπό μελέτη PUF, όπως αυτή παρουσιάζεται στο σχηματικό διάγραμμα της εικόνας 2.1, η επανεξέταση των εν λόγω χαρακτηριστικών καθίσταται απαραίτητη, προκειμένου να συμπεριληφθεί η επίδραση της απεικονιστικής συσκευής που χρησιμοποιείται για την καταγραφή των ζητούμενων στιγμιοτύπων.

Εν συντομία, η τελική ένταση I_0 ενός speckle pattern, όπως αυτό καταγράφεται από μια απεικονιστική συσκευή πεπερασμένων διαστάσεων με m πανομοιότυπα εικονοστοιχεία, προκύπτει από τον μέσο όρο των εντάσεων που καλύπτουν την περιοχή εκάστου pixel. Η PDF της τελικής αυτής έντασης υπακούει στη κατανομή Γάμμα:

$$p(I_0) = \left[\frac{M}{\langle I \rangle}\right]^M \frac{I_0^{M-1}}{\Gamma(M)} \exp\left[-M\frac{I_0}{\langle I \rangle}\right] \tag{2.37}$$

όπου η παράμετρος M σχετίζεται με τον αριθμό των κηλίδων που χωράνε στη συνολική επιφάνεια του χρησιμοποιούμενου αισθητήρα. Ειδικότερα, η παράμετρος M ορίζεται στο διάστημα [1,∞] και υπολογίζεται προσεγγιστικά από την παρακάτω σχέση:

$$M \approx 1 + \frac{S_m}{S_c} \tag{2.38}$$

με τη μεταβλητή S_c να συμβολίζει την ελάχιστη επιφάνεια που καταλαμβάνουν οι κόκκοι του προβαλόμενου speckle στο επίπεδο του εν λόγω αισθητήρα και τη μεταβλητή S_m να αντιστοιχεί στην ενεργή επιφάνεια των διαθέσιμων εικονοστοιχείων του. Βάσει μάλιστα της παραμέτρου αυτής μπορεί κάλλιστα να υπολογιστεί και η μετρούμενη φωτοαντίθεση C του ληφθέντος πλέον speckle, η οποία επαναδιατυπώνεται ακολούθως:

$$C = \frac{\sigma_0}{\langle I_0 \rangle} = \frac{1}{\sqrt{M}} \tag{2.39}$$

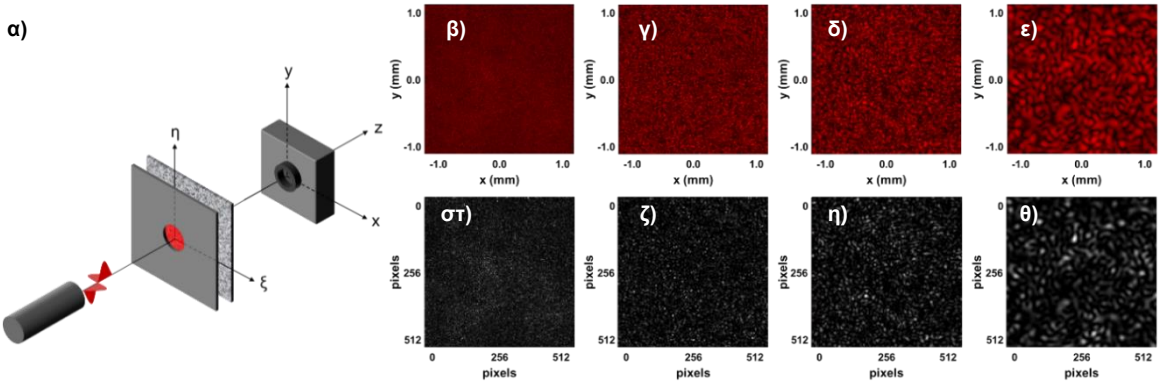
Σύμφωνα λοιπόν με τα παραπάνω, τα τελικά στατιστικά χαρακτηριστικά ενός speckle που καταγράφεται από μια συσκευή απεικόνισης εικόνων, είναι άμεσα εξαρτημένα από τις πεπερασμένες διαστάσεις του χρησιμοποιούμενου αισθητήρα και του πλήθους των εικονοστοιχείων από τα οποία αυτός απαρτίζεται.

Συγκεκριμένα, εάν η επιφάνεια των εικονοστοιχείων είναι σημαντικά μεγαλύτερη από την επιφάνεια των κόκκων του speckle και ισχύει η ανισότητα $S_m << S_c$, τότε η παραμέτρος M αποκτά την οριακή τιμή της μονάδας. Σε αυτή την περίπτωση, η συνάρτηση πυκνότητας πιθανότητας της έντασης $p(I_0)$ τείνει προς την εκθετικά μειούμενη κατανομή του πραγματικού speckle, με την φωτοαντίθεσή του, C, να ισούται με 1. Αντιθέτως, για την περίπτωση $S_c << S_m$, όπου το μέγεθος των κηλίδων είναι αρκετά μικρότερο από την επιφάνεια των pixels, η τιμή της M απειρίζεται, η PDF $p(I_0)$ της μετρούμενης έντασης απομακρύνεται από την ιδανική συμπεριφορά μιας negative exponential κατανομής τείνοντας προς την κανονική και το αντίστοιχο contrast μηδενίζεται.

Με άλλα λόγια, η καταγραφή ενός speckle pattern με στατιστικές ιδιότητες, οι οποίες προσεγγίζουν τις αντίστοιχες πραγματικές, λαμβάνει χώρα όταν η επιφάνεια του χρησιμοποιούμενου αισθητήρα είναι αρκετά μικρότερη από το εμβαδόν που καταλαμβάνουν οι κηλίδες στο επίπεδο απεικόνισης, όταν δηλαδή το πλήθος των διαθέσιμων εικονοστοιχείων m είναι τουλάχιστον ίσο ή μικρότερο από τον αριθμό των προβαλλόμενων κόκκων. [33]

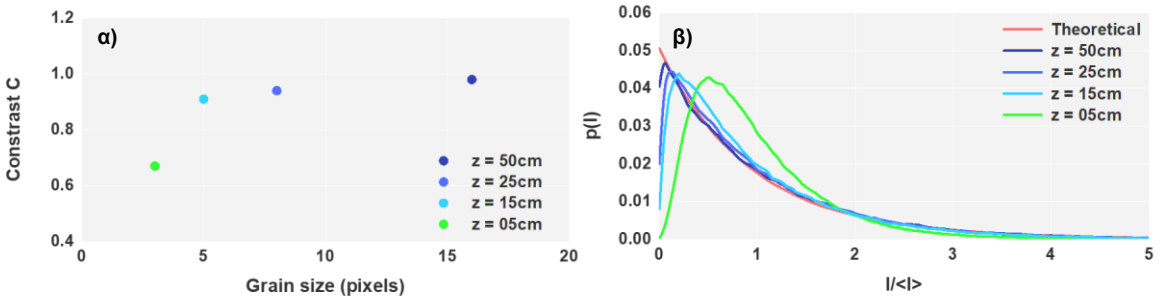
Υπό αυτό το πλαίσιο, τα υπολογιστικά αποτελέσματα του σχήματος 2.13 αντιστοιχούν σε ένα σύνολο από ιδανικά speckle patterns, τα οποία παράχθηκαν χρησιμοποιώντας την διάταξη του σχήματος 2.11. Το εγκάρσιο επίπεδο παρατήρησης ορίστηκε ομοίως ως ένας πίνακας $2^{13}\times2^{13}$ στοιχείων, ο οποίος αντιστοιχεί σε ένα τετραγωνικό πέτασμα πλάτους 40mm. Στο ίδιο σχήμα

συμπεριλαμβάνονται και οι ψηφιακές εικόνες που προέκυψαν από την αντικατάσταση του πετάσματος αυτού με μια συσκευή απεικόνισης, η επίδραση της οποίας μοντελοποιήθηκε με την διαδοχική εφαρμογή ενός αλγόριθμου παρεμβολής κοντινότερων γειτόνων (nearest neighbor interpolation) και ενός Gaussian φίλτρου, διαστάσεων 3 pixels και διακύμανσης 0.5. Η απεικονιστική αυτή συσκευή ουσιαστικά αντιστοιχεί σε έναν αισθητήρα κάμερας με συνολικό εύρος 2mm, χρωματικό βάθος 8 bits και ανάλυση 512×512 pixels.



Σχήμα 2.13: α) Διάταξη για καταγραφή speckle pattern στην περιοχή Fraunhofer: Ένα επίπεδο κύμα στα 635nm διέρχεται από ένα κυκλικό διάφραγμα διαμέτρου 5mm, στο οποίο έχει τοποθετηθεί εφαπτομενικά μια επιφάνεια μεγάλης τραχύτητας. Τα πραγματικά speckles που σχηματίζονται πάνω σε ένα πέτασμα παρατήρησης, για **β)** z = 5cm, **γ)** z = 15cm, **δ)** z = 25cm και **ε)** z = 50cm. **στ-θ)** Οι αντίστοιχες εικόνες που προκύπτουν εάν το πέτασμα παρατήρησης αντικατασταθεί από μια κάμερα ανάλυσης 512×512 τετραγωνικών pixels με πλάτος 4μm.

Ακολούθως, στα διαγράμματα του σχήματος 2.14 παρουσιάζεται η φωτοαντίθεση των ψηφιακών αυτών εικόνων, ως συνάρτηση του μεγέθους των κόκκων τους, μαζί με τις αντίστοιχες συναρτήσεις πυκνότητας πιθανότητας της καταγραφόμενης έντασής τους. Όπως λοιπόν μπορεί να παρατηρηθεί από τα διαγράμματα αυτά, όταν η απόσταση της κάμερας από την ανάγλυφη επιφάνεια της χρησιμοποιούμενης διάταξης ελαττώνεται, το μέγεθος των κηλίδων μειώνεται, η τιμή της φωτοαντίθεσης C φθίνει και η PDF της μετρούμενης έντασης αποκλίνει όλο και περισσότερο από την εκθετικά μειούμενη κατανομή του πραγματικού speckle, αποκτώντας μια πιο gaussian μορφολογία.



Σχήμα 2.14: α) Η φωτοαντίθεση των καταγραφόμενων speckle patterns συναρτήσει του μεγέθους των κόκκων τους. **β)** Οι συναρτήσεις πυκνότητας πιθανότητας για την μετρούμενη ένταση αυτών.

Ολοκληρώνοντας την παρούσα ενότητα, κρίνεται αναγκαίο να επισημανθεί ότι η άνωθεν μαθηματική θεωρία περιγράφει επιτυχώς μόνο τις στατιστικές ιδιότητες των speckles που προκύπτουν από την αλληλεπίδραση μιας τέλεια πολωμένης δέσμης σύμφωνου και μονοχρωματικού φωτός με ένα οπτικό μέσο μεγάλης τραχύτητας, το οποίο διατηρεί αναλλοίωτη την πόλωση του προσπίπτοντος Η/Μ πεδίου. Ως εκ τούτου, οποιαδήποτε διαφοροποίηση στα χαρακτηριστικά της πηγής ή του μέσου επιβάλλει την επανεξέταση των ιδιοτήτων αυτών, καθιστώντας αναγκαία την προσαρμογή της εν λόγω θεωρίας. Ενδεικτικά αναφέρεται ότι η συνάρτηση

πυκνότητας πιθανότητας της έντασης ενός speckle, το οποίο προέρχεται από ένα πεδίο με βαθμό πόλωσης P, επαναδιατυπώνεται ακολούθως:

$$p(I) = \frac{1}{P\langle I\rangle}\left\{\exp\left[-\frac{2}{(1+P)}\frac{I}{\langle I\rangle}\right] - \exp\left[-\frac{2}{(1-P)}\frac{I}{\langle I\rangle}\right]\right\} \quad (2.40)$$

με την ένταση του παρατηρούμενου προτύπου να προκύπτει εν τέλει υπολογιστικά από την εξίσωση:

$$I = \frac{1}{2}(1+P)I_1 + \frac{1}{2}(1-P)I_2 \quad (2.41)$$

όπου I_1, I_2 οι εντάσεις δύο ανεξάρτητα κατασκευασμένων speckles [32]. Θα πρέπει να σημειωθεί ότι ο βαθμός πόλωσης P ενός H/M πεδίου ορίζεται ως ο λόγος εντάσεως της πολωμένης συνιστώσας αυτού ως προς την συνολική έντασή του, ο οποίος σύμφωνα με τις παραμέτρους Stokes λαμβάνει τιμές στο διάστημα [0,1] [36]. Συγκεκριμένα, η τιμή P = 1 χαρακτηρίζει ένα πεδίο με μία από τις 3 γνωστές και διπλά εκφυλισμένες καταστάσεις πόλωσης ή έναν γραμμικό συνδυασμό τους, όπως αυτοί αναπαρίστανται ως σημεία στην επιφάνεια της σφαίρας Poincare [3]. Στην περίπτωση αυτή, η PDF της έντασης του speckle pattern συμπίπτει με την εκθετικά μειούμενη κατανομή των προηγούμενων παραγράφων και η μέγιστη θεωρητική τιμή της φωτοαντίθεσης του C, ισούται με 1. Αντίθετα, για την τιμή P = 0, η οποία αντιστοιχεί σε ένα πλήρως απόλωτο πεδίο που δεν δύναται να μετατραπεί σε ένα γραμμικά πολωμένο ισοδύναμο χωρίς απώλεια ενέργειας, η συνάρτηση πυκνότητας πιθανότητας p(I) του speckle χαρακτηρίζεται από μια πιο Gaussian μορφολογία και η μέγιστη θεωρητική τιμή της φωτοαντίθεσής του ισούται με $1/\sqrt{2}$ [35].

2.2.1 Μοντελοποίηση Ανάγλυφων Επιφανειών

Επανεξετάζοντας τις παραδοχές της προηγούμενης υποενότητας γίνεται εμφανές ότι η απλούστερη μέθοδος που μπορεί να εφαρμοστεί για τον σχηματισμό speckle patterns με τα προαναφερθέντα στατιστικά χαρακτηριστικά, είναι η διαμόρφωση του H/M πεδίου με μια μάσκα ψευδοτυχαίων φάσεων, οι οποίες είναι ομοιογενώς κατανεμημένες στο διάστημα [-π,+π]. Ως εκ τούτου, ο βαθμωτός πολλαπλασιασμός του μιγαδικού πλάτους U(x,y,z), με έναν όρο της μορφής exp[-jφ(x,y)], όπου $\varphi(x,y) \in (-\pi,+\pi)$, είναι αρκετός για την πρωταρχική προσομοίωση της επίδρασης που ασκεί μια επιφάνεια μεγάλης τραχύτητας στο μέτωπο κύματος μιας σύμφωνης μονοχρωματικής δέσμης. Εντούτοις, η μέθοδος αυτή δεν επιδέχεται την εισαγωγή οποιασδήποτε επιπρόσθετης παραμέτρου, καθιστώντας τον χειρισμό του συγκεκριμένου μοντέλου αρκετά δύσκολο. Συνεπώς, για την προσομοίωση του εν λόγω φαινομένου επιλέχθηκε να χρησιμοποιηθεί μια εναλλακτική και πιο ευέλικτη προσέγγιση, η οποία λαμβάνει υπόψιν τα μορφολογικά γνωρίσματα των θεωρούμενων επιφανειών, επιτρέποντας την ελεγχόμενη τροποποίηση των συνθηκών υπό τις οποίες παράγονται τα ζητούμενα speckles. Στο πλαίσιο της παρούσας διατριβής λοιπόν, η μοντελοποίηση όλων των ανάγλυφων επιφανειών πραγματοποιήθηκε μέσω του αλγόριθμου Perlin, ο οποίος

[3] Η κατάσταση πόλωσης ενός κύματος καθορίζεται από τον λόγο των πλατών και τη διαφορά φάσης που παρουσιάζουν οι δύο κάθετες συνιστώσες του. Μπορεί να προσδιοριστεί από τις παραμέτρους Stokes, οι οποίες περιγράφουν πλήρως την συνολική ένταση, την ελλειπτικότητα, το αζιμούθιο και την φορά της περιστροφής του πεδίου. Οι παράμετροι αυτοί αποτελούν και τους όρους των ομόνυμων διανυσμάτων Stokes, τα οποία απεικονίζονται γραφικά με χρήση της λεγόμενης σφαίρας Poincare.

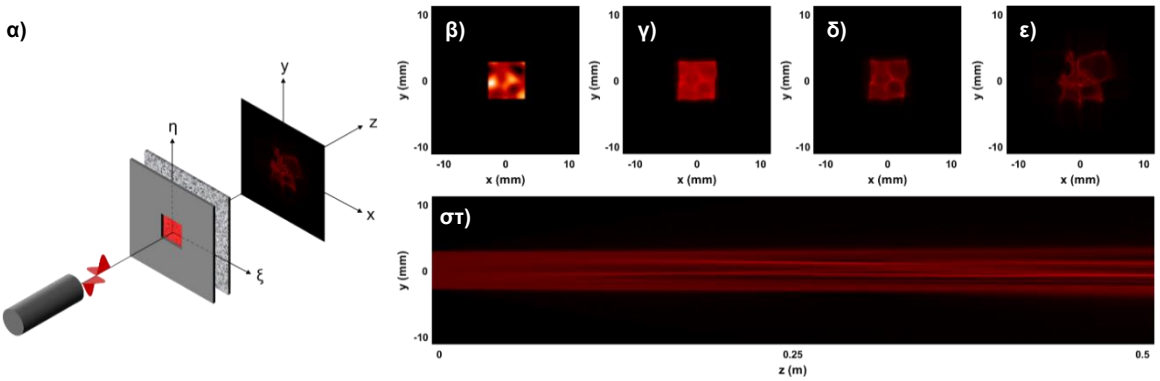
αναπτύχθηκε για τις ανάγκες της ταινίας Tron από τον Ken Perlin το 1982. Ουσιαστικά πρόκειται για μια συνάρτηση παραγωγής θορύβου, η αναδρομική εκτέλεση της οποίας οδηγεί σε ρεαλιστικές υφές με ομοιόμορφες κλιμακώσεις πανομοιότυπου μεγέθους [37] [38].

Ειδικότερα, η λειτουργία του εν λόγω αλγορίθμου συνοψίζεται ακολούθως: αρχικά κατασκευάζεται ένας πίνακας τυχαίων αριθμών που κατατέμνεται σε ένα ομοιόμορφο πλέγμα τετραγώνων, το μέγεθος των οποίων καθορίζεται βάσει μιας προεπιλεγμένης χωρικής συχνότητας. Οι γωνίες των τετραγώνων αυτών εν συνεχεία αντιστοιχίζονται σε ένα επιπλέον τυχαίο διάνυσμα, το οποίο αντιπροσωπεύει μια κατευθύνουσα παράγωγο που υποδεικνύει την διεύθυνση και την φορά με την οποία το πλάτος του παραγόμενου θορύβου θα αυξάνεται. Έπειτα κάθε στοιχείο του αρχικού πίνακα αντικαθίσταται από τον σταθμισμένο μέσο όρο τεσσάρων εσωτερικών γινομένων, τα οποία προσδιορίζονται μεταξύ των παραγώγων που περιβάλλουν το εκάστοτε σημείο με τις αποστάσεις των αντιστοίχων γωνιών από αυτό. Ύστερα, ο προκύπτων πίνακας εξομαλύνεται περαιτέρω μέσω μιας μεθόδου παρεμβολής, οδηγώντας σε μια συνεχή συνάρτηση θορύβου με περιοδικές διακυμάνσεις πλατών.

Συνήθως, η άνωθεν περιγραφείσα διαδικασία επαναλαμβάνεται για ένα πεπερασμένο αριθμό διαφορετικών συχνοτήτων, με τους εξαγόμενους πίνακες να προστίθενται ανά στοιχείο, παράγοντας την ζητούμενη τελική υφή. Η υφή αυτή αποτελεί και την εγκάρσια κατατομή των υψών Δℓ της χρησιμοποιούμενης ανώμαλης επιφάνειας, η οποία με την σειρά της μετατρέπεται σε μια δισδιάστατη συνάρτηση διαφορών στη φάση του Η/Μ πεδίου μέσω του ακόλουθου τύπου:

$$t = \exp\left[-j\Delta\varphi(x,y)\right] = \exp\left[-j2\pi\frac{\Delta\ell(x,y)}{\lambda}\right] \qquad (2.42)$$

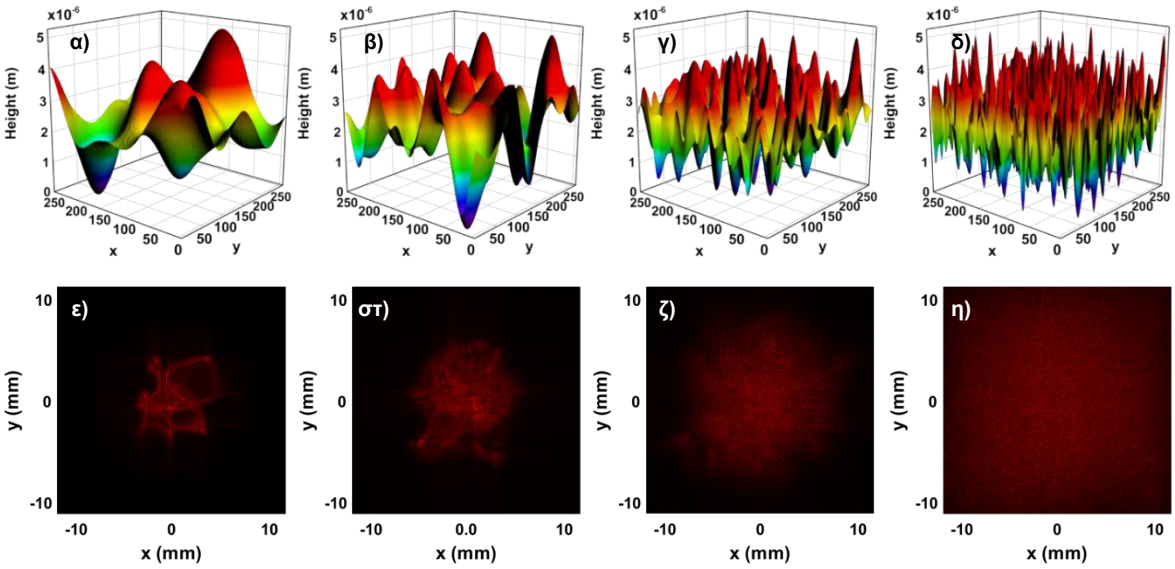
Εν προκειμένω, στις εικόνες του σχήματος 2.15 παρουσιάζεται ένα αντιπροσωπευτικό σύνολο από αποτελέσματα προσομοιώσεων, όπως αυτά προέκυψαν για μια ανάγλυφη επιφάνεια χαμηλής τραχύτητας, η οποία μοντελοποιήθηκε μέσω του αλγορίθμου Perlin, με μία μόνο εφαρμογή της προαναφερθείσας συνάρτησης και τιμή χωρικής συχνότητας ίση με 2.5.



Σχήμα 2.15: α) Διάταξη για καταγραφή speckle pattern στην περιοχή Fraunhofer: Ένα επίπεδο κύμα στα 635nm διέρχεται από ένα τετραγωνικό διάφραγμα πλάτους 5mm, στο οποίο έχει τοποθετηθεί εφαπτομενικά μια επιφάνεια χαμηλής τραχύτητας. **β)** Το heatmap της ανάγλυφης επιφάνειας που κατασκευάστηκε μέσω του αλγόριθμου Perlin για τιμή συχνότητας ίση με 2.5. Η ένταση του πεδίου στο επίπεδο xy, όπως αυτή διαμορφώνεται επί ενός πετάσματος παρατήρησης, τοποθετημένο σε αποστάσεις **γ)** z = 5cm, **δ)** z = 25cm και **ε)** z =50cm.**ς)** Η αντίστοιχη κατανομή της έντασης στο διαμήκες επίπεδο yz.

Όπως είναι λοιπόν πρόδηλο από την άνωθεν περιγραφή, η σημαντικότερη παράμετρος του αλγορίθμου Perlin είναι η συχνότητα (frequency) της εφαρμοζόμενης συνάρτησης, η οποία αντιπροσωπεύει τον αριθμό των κύκλων ανά

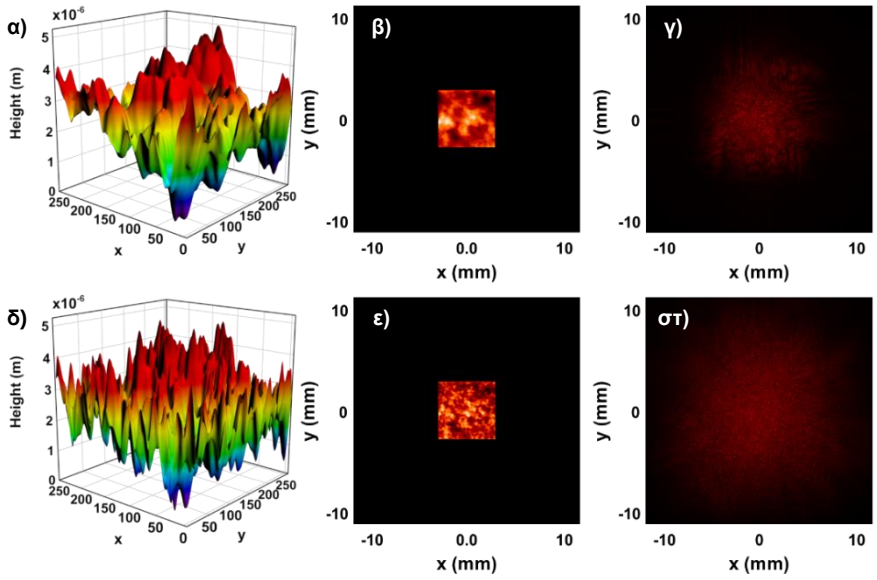
μονάδα επιφάνειας και καθορίζει τον ρυθμό με τον οποίο εναλλάσσονται τα πλάτη του εξαγόμενου θορύβου. Συνεπώς, οι υψηλότερες τιμές συχνοτήτων δημιουργούν υφές με πιο απότομες διακυμάνσεις υψών, η τραχύτητα των οποίων οδηγούν στον σχηματισμό των ζητούμενων speckle patterns (σχήμα 2.16).



Σχήμα 2.16: Κατατομή ανάγλυφων επιφανειών που κατασκευάστηκαν μέσω του αλγόριθμου Perlin, με χρήση μίας μόνο οκτάβας και αντίστοιχες τιμές συχνοτήτων **α)** f = 2.5, **β)** f = 5, **γ)** 10 και **δ)** f = 20. **ε-η)** Η ένταση του πεδίου για κάθε μία από τις εικονιζόμενες επιφάνειες, όπως αυτή διαμορφώνεται σε ένα πέτασμα παρατήρησης, τοποθετημένο σε απόσταση 50cm.

Η δεύτερη σημαντική παράμετρος του αλγορίθμου Perlin από την άλλη πλευρά, είναι η λεγόμενη οκτάβα (octave), η οποία ουσιαστικά αποτελεί τον αριθμό των επαναλήψεων που εφαρμόζεται η συνάρτηση θορύβου, ισοδυναμώντας με το πλήθος των προστιθέμενων επιπέδων από το οποίο συντίθεται το τελικό αποτέλεσμα. Η αύξηση αυτής της παραμέτρου συνεπάγεται την προσθήκη επιπλέον λεπτομερειών στην επιφάνεια της ελάχιστης χρησιμοποιούμενης συχνότητας και επομένως οδηγεί σε πιο περίπλοκες και ρεαλιστικές υφές. Στο σημείο αυτό θα πρέπει να επισημανθεί ότι το μέγεθος αυτών των επιπρόσθετων λεπτομερειών διέπεται από δύο συμπληρωματικές μεταβλητές, την κενότητα (lacunarity) και την ανθεκτικότητα (persistence). Η κενότητα είναι ο ρυθμός με τον οποίο αυξάνεται η συχνότητα της συνάρτησης θορύβου ανά οκτάβα, ενώ η ανθεκτικότητα είναι ο ρυθμός με τον οποίο μειώνεται το αντίστοιχο πλάτος αυτής. Στο σχήμα που ακολουθεί παρουσιάζονται δύο σχετικά παραδείγματα επιφανειών, τα οποία έχουν προέλθει από την πρόσθεση των υφών του σχήματος 2.16 για δύο διαφορετικές τιμές ανθεκτικότητας, μαζί με τα αντίστοιχα speckle patterns αυτών, όπως προκύπτουν σε απόσταση 50cm, χρησιμοποιώντας την διάταξη του σχήματος 2.15.

Ολοκληρώνοντας την υποενότητα για την μοντελοποίηση των ανάγλυφων επιφανειών θα πρέπει επίσης να αναφερθεί ότι η προσθήκη επιπλέον οκτάβων κατά την εφαρμογή του αλγορίθμου Perlin συνεπάγεται την επαύξηση του υπολογιστικού χρόνου που απαιτείται για την εξαγωγή των χρησιμοποιούμενων υφών. Για τον λόγο αυτόν, προτιμήθηκε η χρήση μίας μόνο οκτάβας με υψηλή συχνότητα θορύβου, η οποία, όπως αποδεικνύεται, θεωρείται επαρκής για την παραγωγή των speckle patterns με τα ζητούμενα στατιστικά χαρακτηριστικά.



Σχήμα 2.17: α) Κατατομή επιφάνειας όπως αυτή προέκυψε από τον αλγόριθμο του Perlin για 4 οκτάβες με αρχική συχνότητα 2.5, lacunarity 2 και persistence 1/2. **β-γ)** Το heatmap της επιφάνειας αυτής μαζί με το speckle pattern της σε απόσταση z = 50cm **δ-ς)** Τα αντίστοιχα αποτελέσματα για persistence ίσο με 9/10.

2.3 Θεωρία Διάδοσης Φωτός σε Ίνες με Βηματικό Δείκτη Διάθλασης

Ο όρος οπτική ίνα αναφέρεται σε έναν διηλεκτρικό κυματοδηγό κυλινδρικής συμμετρίας, ο οποίος αποτελείται από δυο ομοαξονικές περιοχές με ακτίνες a και b > a αντιστοίχως. Η κεντρική περιοχή του, η οποία ονομάζεται πυρήνας (core), συνήθως χαρακτηρίζεται από έναν σταθερό δείκτη διάθλασης, που ισούται με n_1, και σε αυτήν πραγματοποιείται η ζητούμενη κυματοδήγηση της προσπίπτουσας ηλεκτρομαγνητικής ακτινοβολίας. Από την άλλη πλευρά, η περιβάλλουσα περιοχή του κυματοδηγού, ο λεγόμενος μανδύας του (cladding), έχει δείκτη διάθλασης $n_2 < n_1$, η τιμή του οποίου επιλέγεται καταλλήλως ώστε να διασφαλίζεται ο χωρικός περιορισμός της διάδοσης εντός του πυρήνα.

Υπό την σκοπιά της γεωμετρικής οπτικής, η αρχή λειτουργίας μιας τυπικής οπτικής ίνας βασίζεται στο φαινόμενο της ολικής εσωτερικής ανάκλασης (total internal reflection) που υπόκειται μια ακτίνα φωτός, όταν προσπέσει στην διεπαφή των δύο πραναφερθεισών περιοχών. Η σχηματική αναπαράσταση της διεργασίας αυτής επιδεικνύεται στην εικόνα 2.18α, για την οποία όμως έχει θεωρηθεί, χάριν ευκολίας, ένας παρεμφερής επίπεδος κυματοδηγός με συμμετρική κατανομή δεικτών διάθλασης ως προς τον άξονα διάδοσης του φωτός.

Όπως φαίνεται λοιπόν από το παρακάτω σχήμα, το φαινόμενο της ολικής εσωτερικής ανακλάσεως λαμβάνει χώρα όταν η ελάχιστη γωνία πρόσπτωσης της ακτίνας στην εν λόγω διεπαφή ισούται με $\theta_c = \sin^{-1}(n_2/n_1)$ και όταν η αντίστοιχη γωνία εισόδου της στον πυρήνα του κυματοδηγού είναι $n_2\sin(\pi/2 - \theta_1) \geq n_1$. Συνεπώς, το κριτήριο που πρέπει να ικανοποιείται για την εκδήλωση αυτού του φαινομένου, σύμφωνα με τον νόμο του Snell, είναι:

$$\theta_0 \leq \sin^{-1}\left(\sqrt{n_2^2 - n_1^2}\right) \equiv \theta_{max} \qquad (2.43)$$

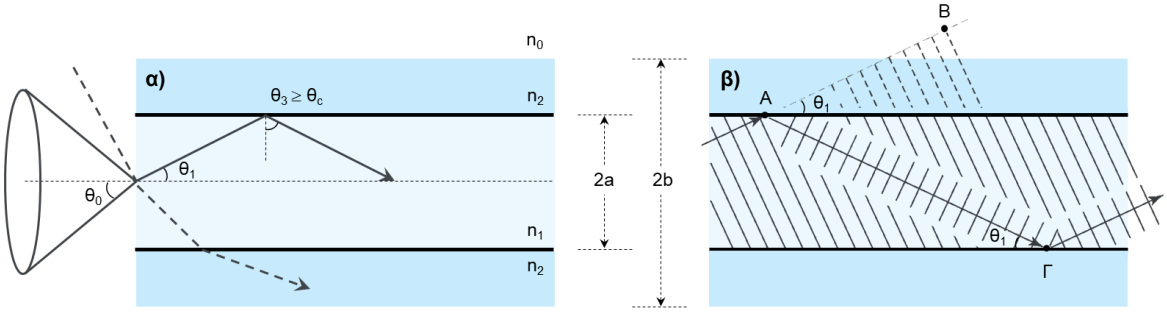
Εν γένει, η διαφορά μεταξύ των δύο δεικτών διάθλασης n_1 και n_2 ορίζεται μικρότερη του 1%. Επομένως, η εξίσωση (2.43) μπορεί να επαδιατυπωθεί προσεγγιστικά ακολούθως

$$\theta_{max} \cong \sqrt{n_2^2 - n_1^2} \qquad (2.44)$$

όπου θ_{max} η μέγιστη δυνατή γωνία πρόσπτωσης της ακτίνας στην επιφάνεια εισόδου του κυματοδηγού. Αυτή μάλιστα αντιστοιχεί και στο αποκαλούμενο αριθμητικό άνοιγμά του (numerical aperture NA), το οποίο, λαμβάνοντας υπόψιν την σχετική διαφορά των δύο δεικτών διάθλασης,

$$\Delta = \frac{n_2^2 - n_1^2}{2n_1^2} \cong \frac{n_2 - n_1}{n_1} \qquad (2.45)$$

μπορεί να εκφραστεί ισοδυνάμως από την σχέση $NA \approx n_1(2\Delta)^{1/2}$.



Σχήμα 2.18: α) Γεωμετρική αναπαράσταση της ολικής εσωτερικής ανάκλασης που υφίσταται μια ακτίνα ακτινοβολίας, όταν προσπίπτει στα τοιχώματα του πυρήνα ενός επίπεδου κυματοδηγού με συμμετρική κατανομή δείκτη διάθλασης. **β)** Τα μέτωπα κύματος αυτής της ακτίνας, όπως αυτά σχηματίζονται εντός του προαναφερθέντος πυρήνα, μαζί με την νοητή διάδοσή της, απουσία της παρεμβαλλόμενης διεπαφής.

Εν ολίγοις, οι ακτίνες που προσπίπτουν στον πυρήνα ενός κυματοδηγού, υπό $\theta_0 \leq \theta_{max}$, υφίστανται διαδοχικές ολικές εσωτερικές ανακλάσεις από τα τοιχώματα αυτού, με την διάδοση της Η/Μ ακτινοβολίας να περιορίζεται εντός του και το κυματοδηγούμενο φως να ακολουθεί ένα πλήθος οπτικών διαδρομών, οι οποίες καθορίζονται από τις αρχικές γωνίες πρόσπτωσης θ_0 και τις αντίστοιχες γωνίες εισόδου τους θ_1. Ωστόσο, οι γωνίες αυτές στην πραγματικότητα δεν αντιστοιχούν σε μια συνεχή συνάρτηση τιμών, αλλά αποτελούν ένα κβαντισμένο μέγεθος, το οποίο διέπεται τόσο από το εύρος και το Δ του χρησιμοποιούμενου κυματοδηγού, όσο και από το μήκος κύματος του προσπίπτοντος πεδίου.

Ειδικότερα, οι διαδρομές που υποστηρίζονται από έναν κυματοδηγό με πυρήνα εύρους 2α, κατά την διάδοση μιας δέσμης ακτινοβολίας με μήκος κύματος λ, είναι αυτές που τα μέτωπα κύματός τους μετά από δύο διαδοχικές ανακλάσεις συμβάλλουν ενισχυτικά με τα αντίστοιχα αρχικά. Αυτό συμβαίνει όμως, μόνο όταν η διαφορά φάσης Δφ μεταξύ των συγκεκριμένων μετώπων είναι ακέραιο πολλαπλάσιο της ποσότητας 2π.

Σε αυτό το πλαίσιο, επιστρατεύοντας το προαναφερθέν παράδειγμα του επίπεδου και συμμετρικού κυματοδηγού, στην εικόνα 2.18β παρουσιάζονται τα μέτωπα κύματος μιας ακτίνας που υφίσταται δυο διαδοχικές εσωτερικές ολικές ανακλάσεις στα σημεία Α και Γ αντιστοίχως. Στην ίδια εικόνα αναπαρίσταται και η νοητή διάδοσή της από το σημείο Α στο Β, όπως αυτή θα προέκυπτε απουσία της παρεμβαλλόμενης διεπαφής. Σύμφωνα λοιπόν με τα παραπάνω, η οπτική διαδρομή του εν λόγω σχήματος είναι παρατηρήσιμη μόνο όταν η Δφ των μετώπων στα σημεία Β και Γ ικανοποιεί την ακόλουθη συνθήκη:

$$\Delta\varphi = \left(k\,\overline{A\Gamma} + 2\Phi \right) - k\,\overline{AB} = 2\pi m \qquad (2.46)$$

όπου $k = 2\pi n_1/\lambda$ ο κυματάριθμος της ακτινοβολίας στο εσωτερικό του πυρήνα και Φ η μετατόπιση Goos - Hänchen, η οποία ουσιαστικά αποτελεί την φάση που συσσωρεύεται από κάθε ανάκλαση [39]

$$\Phi = -2\tan^{-1}\sqrt{\frac{2\Delta}{\sin^2\theta_1}-1} \tag{2.47}$$

Συνεπώς, αντικαθιστώντας στην εξίσωση (2.46) τις αποστάσεις ΑΓ = 2α/sinθ$_1$ και ΑΒ = 2αcos(2θ$_1$)/sinθ$_1$, αποδεικνύεται ότι οι διακριτές γωνίες εισόδου θ$_{1,m}$ στον πυρήνα ενός κυματοδηγού μπορούν εν τέλει να υπολογιστούν από την σχέση:

$$\tan\left[\frac{2\pi n_1}{\lambda}\alpha\sin\theta_{1,m}-\frac{m\pi}{2}\right]=\sqrt{\frac{2\Delta}{\sin^2\theta_{1,m}}-1} \tag{2.48}$$

με τις κατανομές των πεδίων που αντιστοιχούν σε κάθε μία από αυτές να αποτελούν τους λεγόμενους ρυθμούς (ή τρόπους) διαδόσεώς του. Οι ρυθμοί διάδοσης με την σειρά τους προσδιορίζονται μέσω της προαναφερθείσας εξίσωσης του Helmholtz (σχέση 2.3) στη διανυσματική της μορφή και των τεσσάρων εξισώσεων του Maxwell, εφαρμόζοντας τις κατάλληλες συνοριακές συνθήκες, όπως αυτές επιβάλλονται από την εκάστοτε κυματοδηγική δομή.

Θεωρώντας λοιπόν μια οπτική ίνα με βηματική κατανομή δείκτη διάθλασης n(r), όπου n_0 ο δείκτης διάθλασης του κενού:

$$`n(r)=\begin{cases} n_1 \ , & 0<r<a \\ n_2 \ , & a<r<b \\ n_0 \ , & r>b \end{cases} \tag{2.49}$$

και εκφράζοντας το ηλεκτρικό πεδίο σε κυλινδρικές συντεταγμένες, $\vec{E} = E_r\hat{r}+E_\varphi\hat{\varphi}+E_z\hat{z}$, η αντίστοιχη εξίσωση του Helmholtz στην διανυσματική της μορφή δίνεται από την σχέση:

$$\left[\left(\nabla^2+k^2\right)E_r-\frac{2\partial E_\varphi}{r^2\partial\varphi}-\frac{E_r}{r^2}\right]\hat{r}+\left[\left(\nabla^2+k^2\right)E_\varphi-\frac{2\partial E_r}{r^2\partial\varphi}-\frac{E_\varphi}{r^2}\right]\hat{\varphi}+\left(\nabla^2+k^2\right)E_z\hat{z}=0 \tag{2.50}$$

Καθώς οι E_φ και E_r παραμένουν πεπλεγμένες, αρχικά αναζητούνται οι λύσεις της χρονο-ανεξάρτητης κυματικής εξίσωσης για την διαμήκη συνιστώσα E_z:

$$\nabla^2E_z+k^2E_z \Rightarrow \left[\frac{\partial^2}{\partial r^2}+\frac{1}{r}\frac{\partial}{\partial r}+\frac{1}{r^2}\frac{\partial^2}{\partial\varphi^2}+\frac{\partial^2}{\partial z^2}+k^2\right]E_Z=0 \tag{2.51}$$

οι οποίες, σύμφωνα με τη μέθοδο των χωριζομένων μεταβλητών, γράφονται $E_z(r,\varphi,z) = R(r)\Phi(\varphi)Z(z)$.

Θεωρώντας λοιπόν κατά σύμβαση ότι $Z(z) = e^{-j(\beta z-\omega t)}$, λόγω της διάδοσης άνευ απωλειών προς το +z, και $\Phi(\varphi) = \Phi(\varphi+2\pi\ell) = e^{j\ell\varphi}$ με $\ell = 0,\pm1,\pm2,\pm3\ldots$, λόγω της κυλινδρικής συμμετρίας που επιβάλλει τη διατήρηση του πεδίου για στροφές γωνίας 2π, προκύπτει η διαφορική εξίσωση Bessel:

$$\left[\frac{\partial^2}{\partial r^2}+\frac{1}{r}\frac{\partial}{\partial r}+\left(k^2-\beta^2-\frac{\ell^2}{r^2}\right)\right]R(r)=0 \tag{2.52}$$

η γενική λύση της οποίας είναι:

$$R(r)=\begin{cases} AJ_\ell(hr)+BY_\ell(hr) & \text{για} \quad h^2=k^2-\beta^2>0 \\ CK_\ell(qr)+DI_\ell(qr) & \text{για} \quad -q^2=k^2-\beta^2<0 \end{cases} \tag{2.53}$$

Οι παράμετροι h,q στην παραπάνω εξίσωση αποτελούν τις εγκάρσιες συνιστώσες των $k_1 = n_1k_0$ και $k_2 = n_2k_0$ στις περιοχές του πυρήνα και του μανδύα αντιστοίχως, για τις οποίες ισχύει $h^2,q^2 > 0$ και $h,q \in \mathbb{R}$, ούτως ώστε να πληρείται η απαραίτητη συνθήκη της κυματοδήγησης $k^2 - \beta^2 > 0 \Rightarrow n_2k_0 < \beta < n_1k_0$, Από την άλλη πλευρά, οι $J_\ell(hr)$ και $Y_\ell(hr)$ συμβολίζουν τις συναρτήσεις Bessel $1^{ου}$ και $2^{ου}$ είδους με τάξη ℓ, οι $I_\ell(qr)$ και $K_\ell(qr)$ τις τροποιημένες συναρτήσεις Bessel $1^{ου}$ και $2^{ου}$ είδους ιδίας τάξης, ενώ οι παράμετροι A, B,C,D αποτελούν τους αντίστοιχους συντελεστές κανονικοποίησής τους. Εξ αυτών, οι B και D τίθενται ίσοι με το μηδέν προκειμένου η ακτινοβολία στο εσωτερικό του μανδύα να έχει την μορφή διαφεύγοντος κύματος (evanescent wave) με εκθετικά αποσβεννύμενο πλάτος και το πεδίο να παραμένει πεπερασμένο στη διεπαφή των δύο περιοχών. [40]

Συνεπώς, η ακριβής λύση της χρονοανεξάρτητης κυματικής εξίσωσης για τη διαμήκη συνιστώσα E_z ενός H/M πεδίου, το οποίο διαδίδεται σε έναν διηλεκτρικό κυματοδηγό με κυλινδρική συμμετρία και βηματικό δείκτη διάθλασης, δίνεται εν τέλει από την σχέση:

$$E_z(r,\varphi,z) = R(r)\Phi(\varphi)Z(z) = \begin{cases} AJ_\ell(hr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r \le a \\ CK_\ell(qr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r > a \end{cases} \qquad (2.54)$$

υποδηλώνοντας μια ημιτονοειδή συμπεριφορά της συνιστώσας εντός του πυρήνα και μια εκθετικά μειούμενη συμπεριφορά στη περιοχή του μανδύα.

Με όμοιο τρόπο, υπολογίζεται και η διαμήκης συνιστώσα H_z του μαγνητικού πεδίου H, καθιστώντας εφικτό τον προσδιορισμό των υπόλοιπων συνιστωσών E_r, E_φ, H_r, H_φ, μέσω των 4 εξισώσεων του Maxwell. Επιπρόσθετα, από τις συνοριακές συνθήκες στην διεπαφή των δύο περιοχών (r = a), υπολογίζονται οι συντελεστές A, C, ενώ παράλληλα εξάγεται και η λεγόμενη χαρακτηριστική εξίσωση του κυματοδηγού. Η εξίσωση αυτή ουσιαστικά συνδέει τη σταθερά διάδοσης β με τα δομικά χαρακτηριστικά της υπό μελέτη οπτικής ίνας και συνήθως επιλύεται γραφικά, οδηγώντας σε έναν συγκεκριμένο αριθμό ιδιοτιμών $\beta_{\ell m}$, όπου κάθε μια εξ αυτών αντιστοιχεί σε έναν δεδομένο ρυθμό διάδοσης. Θα πρέπει όμως να υπογραμμισθεί ότι καθώς οι ακτινικοί όροι της σχέσης (2.54) δεν παρουσιάζουν οποιαδήποτε εξάρτηση από τους αντίστοιχους αζιμουθιακούς, για κάθε ζεύγος τιμών $\pm\ell$ όταν $\ell \ge 1$ προκύπτει μια διπλή ιδιοτιμή $\beta_{\ell m}$, η οποία υποδηλώνει την ύπαρξη δύο εκφυλισμένων ιδιοκαταστάσεων με κοινή ακτινική κατανομή [4].

Σε αυτό το πλαίσιο λοιπόν, οι ρυθμοί διάδοσης ενός κυλινδρικού κυματοδηγού μπορούν εν γένει να διαχωριστούν σε τέσσερεις βασικές κατηγορίες, οι οποίες καθορίζονται από τις τιμές που λαμβάνουν οι διαμήκεις συνιστώσες του ηλεκτρικού E και του μαγνητικού H πεδίου. Αυτές είναι:

- οι εγκάρσιοι ηλεκτρικοί ρυθμοί (Transverse Electric Modes - TE), με $E_z = 0$ και $H_z \neq 0$.
- οι εγκάρσιοι μαγνητικοί ρυθμοί (Transverse Magnetic Modes - TM) με $E_z \neq 0$ και $H_z = 0$

[4] Καθώς ο όρος $\exp(j\ell\varphi)$ μπορεί να αντικατασταθεί από 2 πιθανές ημιτονοειδείς συναρτήσεις, την $\cos(|\ell|\varphi)$ και την $\sin(|\ell|\varphi)$, κάθε ρυθμός διάδοσης με $\ell \neq 0$ αντιστοιχίζεται σε 2 κατανομές πεδίου στο εγκάρσιο επίπεδο που διαδίδονται με πανομοιότυπη ταχύτητα, δηλαδή έχουν κοινή σταθερά διάδοσης $\beta_{\ell m}$. Πρακτικά, η παράμετρος ℓ υποδηλώνει πόσους λοβούς παρουσιάζει αυτή η κατανομή ενώ η παράμετρος m πόσους δακτυλίους.

- οι υβριδικοί ηλεκτρικοί ρυθμοί (Hybrid Electric Modes - HE) με $E_z \neq 0$, $H_z \neq 0$ και κυριάρχη την H_z
- οι υβριδικοί μαγνητικοί ρυθμοί (Hybrid Magnetic Modes - EH), όπου $E_z \neq 0$, $H_z \neq 0$ και κυριάρχη την E_z

Ειδικότερα, οι δύο πρώτες κατηγορίες αντιστοιχούν στις λύσεις της εξίσωσης (2.54), για τις οποίες η ακτινική παράμετρος ℓ ισούται με το μηδέν. Ουσιαστικά, οι ρυθμοί TE_{0m} και TM_{0m} αποτελούν τις αποκαλούμενες μεσημβρινές ακτίνες διάδοσης (meridional rays) του κυματοδηγού, οι οποίες διαδίδονται σε επίπεδα που τέμνουν πάντοτε τον άξονα συμμετρίας του. Βάσει αυτών μάλιστα αναπτύχθηκε και η γεωμετρική ερμηνεία των προηγούμενων παραγράφων. Αντιθέτως, οι υβριδικοί ρυθμοί $HE_{\ell m}$ και $EH_{\ell m}$, οι οποίοι χαρακτηρίζονται από ακτινική παράμετρο ℓ διάφορη του μηδενός, αντιστοιχούν στις λεγόμενες «στρεβλές» ακτίνες του κυματοδηγού (skewed rays), οι οποίες ακολουθούν ελικοειδείς τροχιές εντός του πυρήνα και δεν τέμνουν ποτέ τον άξονα διάδοσής του z.

Όπως γίνεται φανερό, ο ακριβής υπολογισμός των ρυθμών διάδοσης ενός κυλινδρικού κυματοδηγού αποτελεί μια ιδιαίτερα χρονοβόρα διαδικασία, η οποία απαιτεί εκτεταμένες και πολύπλοκες μαθηματικές πράξεις, αφού όλες οι διανυσματικές συνιστώσες του H/M πεδίου είναι μη μηδενικές και συζευγμένες. Η εν λόγω διαδικασία όμως δύναται να απλοποιηθεί αρκετά, λαμβάνοντας υπόψιν το γεγονός ότι η διαφορά των δύο δεικτών διάθλασης n_1 και n_2 σε μια τυπική οπτική ίνα είναι συνήθως μικρότερη του 1%. Συγκεκριμένα, υπό την θεώρηση $n_1 \approx n_2$ και βάσει της αναφερθείσας συνθήκης για την κυματοδήγηση, προκύπτει ότι $h,q << \beta$ με $\beta \approx n_1 k_0 \approx n_2 k_0$. Συνεπώς, οι εφαπτομενικές συνιστώσες του ηλεκτρικού και του μαγνητικού πεδίου στη διεπαφή πυρήνα - μανδύα συμπεριφέρονται με πανομοιότυπο τρόπο, ενώ οι αντίστοιχες διαμήκεις συνιστώσες τους μπορούν να εκληφθούν ως σχεδόν αμελητέες. Με άλλα λόγια, η κυματοδηγούμενη ακτινοβολία σε μια οπτική ίνα με $\Delta << 1$ δύναται να προσδιοριστεί προσεγγιστικά ως ένα εγκάρσιο και γραμμικά πολωμένο πεδίο, το οποίο μάλιστα μπορεί να εκφραστεί και σε καρτεσιανές συντεταγμένες.

Εν προκειμένω, έστω $\vec{E} = E_x(r,\varphi)\,\hat{x} + E_y(r,\varphi)\,\hat{y} + E_z(r,\varphi)\,\hat{z}$ και $\vec{H} = H_x(r,\varphi)\,\hat{x} + H_y(r,\varphi)\,\hat{y} + H_z(r,\varphi)\,\hat{z}$ η γενική μορφή των ζητούμενων λύσεων, όπως αυτές καθορίζονται από τις παραπάνω παραδοχές, οι οποίες αντιστοιχούν σε ένα γραμμικά πολωμένο ηλεκτρομαγνητικό πεδίο που ικανοποιεί την διανυσματική εξίσωση του Helmholtz σε καρτεσιανές συντεταγμένες. Από την χρονοανεξάρτητη κυματική εξίσωση και τις τέσσερεις εξισώσεις του Maxwell λοιπόν μπορεί να αποδειχθεί ότι όταν το θεωρούμενο αυτό πεδίο είναι πολωμένο ως προς y, οι συνιστώσες του δίνονται από τις παρακάτω εξισώσεις, εκ των οποίων μόνο 4 είναι μη μηδενικές, με κυριάρχες τις E_y και H_x.

$$E_x(r,\varphi,z) = \begin{cases} 0 & \text{για } r \le a \\ 0 & \text{για } r > a \end{cases} \tag{2.55}$$

$$E_y(r,\varphi,z) = \begin{cases} AJ_\ell(hr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r \le a \\ CK_\ell(qr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r > a \end{cases} \tag{2.56}$$

$$E_z(r,\varphi,z)=\begin{cases}\frac{A}{2}\frac{h}{\beta}\left[J_{\ell+1}(hr)e^{j(\ell+1)\varphi}+J_{\ell-1}(hr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r\le a\\ \frac{C}{2}\frac{q}{\beta}\left[K_{\ell+1}(qr)e^{j(\ell+1)\varphi}-K_{\ell-1}(qr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.57)$$

$$H_x(r,\varphi,z)=\begin{cases}\frac{-\beta}{\omega\mu}AJ_\ell(hr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r\le a\\ \frac{-\beta}{\omega\mu}CK_\ell(qr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.58)$$

$$H_y(r,\varphi,z)\approx\begin{cases}0 & \text{για } r\le a\\ 0 & \text{για } r>a\end{cases} \quad (2.59)$$

$$H_z(r,\varphi,z)=\begin{cases}\frac{-ih}{\omega\mu}\frac{A}{2}\left[J_{\ell+1}(hr)e^{j(\ell+1)\varphi}-J_{\ell-1}(hr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r\le a\\ \frac{-ih}{\omega\mu}\frac{C}{2}\left[K_{\ell+1}(qr)e^{j(\ell+1)\varphi}+K_{\ell-1}(qr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.60)$$

Ομοίως, για διεύθυνση πόλωσης πεδίου ως προς τον άξονα των x, οι ίδιες συνιστώσες επαναδιατυπώνονται ακολούθως, με κυρίαρχες τις E_x και H_y αντιστοίχως.

$$E_x(r,\varphi,z)=\begin{cases}AJ_\ell(hr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r\le a\\ CK_\ell(qr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.61)$$

$$E_y(r,\varphi,z)=\begin{cases}0 & \text{για } r\le a\\ 0 & \text{για } r>a\end{cases} \quad (2.62)$$

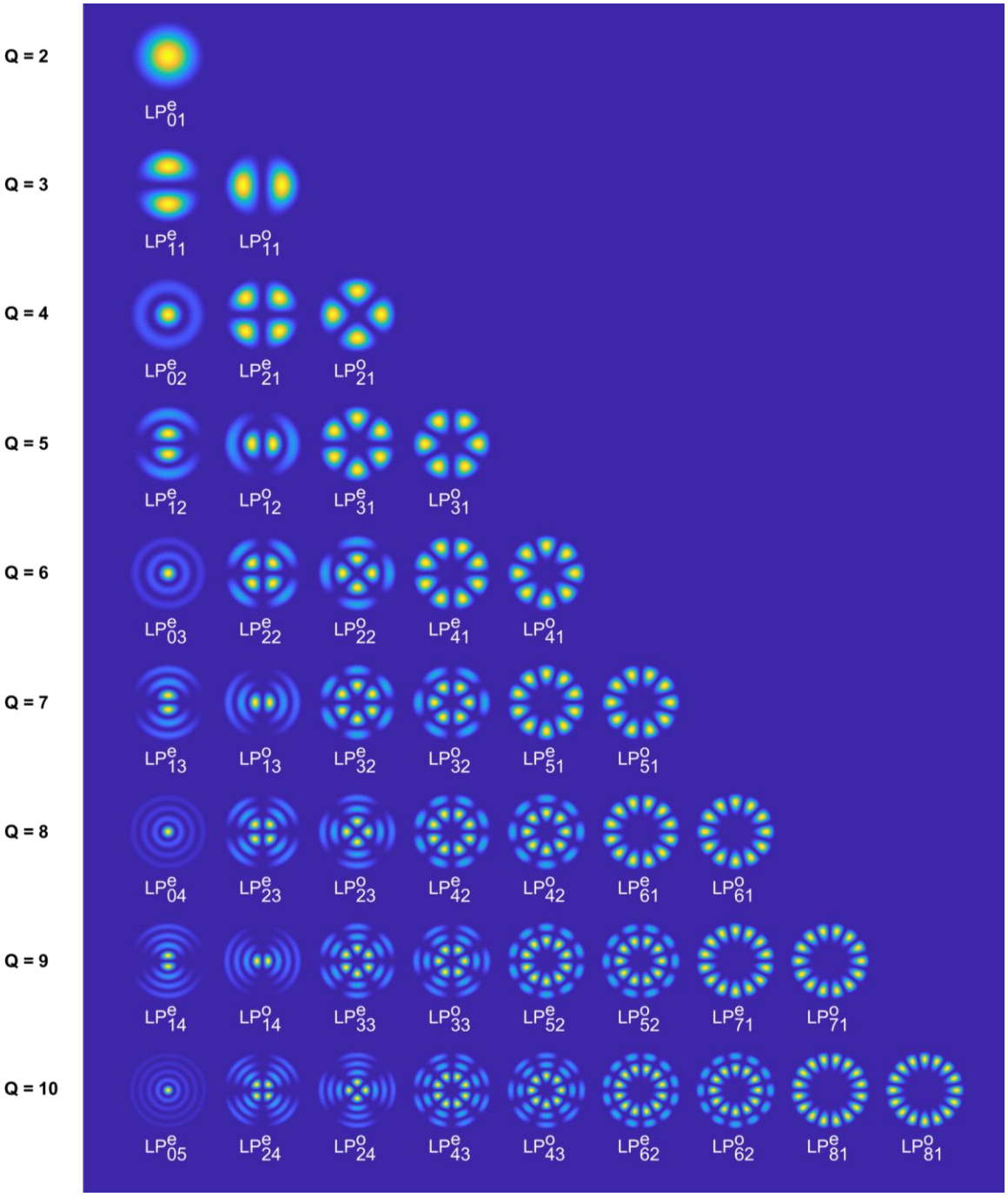
$$E_z(r,\varphi,z)=\begin{cases}\frac{A}{2}\frac{ih}{\beta}\left[J_{\ell+1}(hr)e^{j(\ell+1)\varphi}-J_{\ell-1}(hr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r\le a\\ \frac{C}{2}\frac{iq}{\beta}\left[K_{\ell+1}(qr)e^{j(\ell+1)\varphi}+K_{\ell-1}(qr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.63)$$

$$H_x(r,\varphi,z)\approx\begin{cases}0 & \text{για } r\le a\\ 0 & \text{για } r>a\end{cases} \quad (2.64)$$

$$H_y(r,\varphi,z)=\begin{cases}\frac{\beta}{\omega\mu}AJ_\ell(hr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r\le a\\ \frac{\beta}{\omega\mu}CK_\ell(qr)e^{j\ell\varphi}e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.65)$$

$$H_z(r,\varphi,z)=\begin{cases}\frac{A}{2}\frac{h}{\omega\mu}\left[J_{\ell+1}(hr)e^{j(\ell+1)\varphi}+J_{\ell-1}(hr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r\le a\\ \frac{C}{2}\frac{q}{\omega\mu}\left[K_{\ell+1}(qr)e^{j(\ell+1)\varphi}-K_{\ell-1}(qr)e^{j(\ell-1)\varphi}\right]e^{-j\beta z} & \text{για } r>a\end{cases} \quad (2.66)$$

Συνεπώς, το H/M πεδίο σε έναν κυλινδρικό κυματοδηγό με Δ << 1 έχει πανομοιότυπη χωρική κατανομή και ίδια ταχύτητα διαδόσεως ανεξαρτήτως της θεωρούμενης πόλωσής του, υποδηλώνοντας τον τετραπλό εκφυλισμό της ακτινικής κατανομής για κάθε $\ell \neq 0$. Εν γένει, οι προσεγγιστικές λύσεις του πεδίου, όπως αυτές παρουσιάζονται στις άνωθεν εξισώσεις, ονομάζονται γραμμικά πολωμένοι ρυθμοί του κυματοδηγού (linear polarized modes $LP_{\ell m}$) και ουσιαστικά αντιστοιχούν σε μια γραμμική επαλληλία των πραγματικών λύσεων $HE_{\ell+1,m}$ και $EH_{\ell-1,m}$, οι οποίες έχουν διαφορετικές τιμές ακτινικής παραμέτρου ℓ αλλά μια παρεμφερή σταθερά διάδοσης β [40]. Με άλλα λόγια, οι πραγματικές λύσεις του H/M πεδίου που διαδίδονται με παρεμφερή ταχύτητα φάσης εντός ενός κυλινδρικού κυματοδηγού με Δ << 1, ομαδοποιούνται σε ένα ενιαίο σύνολο που συμπεριφέρεται ως ένα γραμμικά πολωμένο H/M πεδίο, το οποίο χαρακτηρίζεται από μια κοινή αζιμουθιακή παράμετρο m.



Σχήμα 2.19: Η κατανομή έντασης του εγκάρσιου ηλεκτρικού πεδίου, όπως αυτή υπολογίστηκε για τους γραμμικά πολωμένους ρυθμούς διάδοσης $LP_{\ell m}$ των 9 πρώτων ανηγμένων δεικτών Q.

Επί του πρακτέου τώρα, για τις προσομοιώσεις της παρούσας διδακτορικής διατριβής, αρχικά χρησιμοποιήθηκε ένα προϋπάρχον αριθμητικό μοντέλο [41], μέσω του οποίου υπολογίστηκαν οι παράμετροι h, q και β οποιουδήποτε ρυθμού διάδοσης $LP_{\ell m}$ που μπορεί να διεγερθεί κατά την πρόσπτωση μίας σύμφωνης μονοχρωματικής δέσμης με μήκος κύματος στα 650nm σε μία πολυμερική οπτική ίνα (Polymer Optical Fiber - POF), με a = 980μm, $n_1 = 1.4893$ και $n_2 = 1.40286$. Εν συνεχεία, πραγματοποιήθηκε η επιλογή των ρυθμών $LP_{\ell m}$ που πρέπει να διεγερθούν σύμφωνα με το αριθμητικό άνοιγμα της χρησιμοποιούμενης δέσμης, προσδιορίζοντας τις γωνίες εσωτερικής ανακλάσεως θ_3 από τις γωνίες θ_0 του κώνου πρόσπτωσης αυτής και μετατρέποντάς τες σε ένα σύνολο αζιμουθιακών και ακτινικών παραμέτρων (ℓ,m) μέσω του ακόλουθου ανηγμένου δείκτη Q [42]:

$$Q = 2\frac{an_1 \sin\theta_3}{\lambda} = \ell + 2m \tag{2.67}$$

Κατόπιν υπολογίστηκε η εγκάρσια κατανομή του ηλεκτρικού πεδίου για κάθε επιλεγμένο ρυθμό $LP_{\ell m}$, μέσω των σχέσεων (2.56) ή (2.61), συμπεριλαμβάνοντας και την επίδραση της φάσης που συσσωρεύεται λόγω διάδοσης. Να σημειωθεί ότι φαινόμενα σύζευξης και απωλειών δεν λήφθηκαν καθόλου υπόψιν στο παρόν μοντέλο. Έπειτα εφαρμόστηκε ο μετασχηματισμός φάσης της (2.42) σε κάθε κατανομή πεδίου, έχοντας θεωρήσει ότι η επιφάνεια εξόδου της χρησιμοποιούμενης οπτικής ίνας χαρακτηρίζεται από τυχαίες ανομοιογένειες. Ύστερα πραγματοποιήθηκε η ελεύθερη διάδοση κάθε προκύπτουσας κατανομής μέσω της εξίσωσης (2.12), με το αλγεβρικό άθροισμα αυτών να αποτελεί το τελικό ηλεκτρικό πεδίο που προσπίπτει στην επιφάνεια εισόδου της θεωρούμενης απεικονιστικής συσκευής, το οποίο εν τέλει καταγράφεται και από αυτήν.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι ο όρος $e^{-j\beta z}$ των σχέσεων (2.56) και (2.61) αντικατοπτρίζει την φάση που συσσωρεύεται κατά την διάδοση κάθε ρυθμού $LP_{\ell m}$ εντός της χρησιμοποιούμενης οπτικής ίνας. Στην πράξη όμως, ο όρος αυτός αντικαταστάθηκε από έναν αντίστοιχο όρο e^{φ}, ο εκθέτης του οποίου αντιστοιχεί σε μια τυχαία μεταβλητή $\varphi \in [0,2\pi]$, με τιμές που ακολουθούν μια κανονική κατανομή. Η εν λόγω αντικατάσταση, η οποία ουσιαστικά αντιπροσωπεύει την μοναδική πηγή θορύβου που ενσωματώθηκε στο αριθμητικό μοντέλο της παρούσας εργασίας, πραγματοποιήθηκε ούτως ώστε να ληφθεί υπόψιν η θορυβική επίδραση των μεταβολών που προκαλούνται από ακουστικά ή θερμικά φαινόμενα επί του μήκους της ίνας [43].Εντούτοις κρίνεται απαραίτητο να υπογραμμιστεί ότι οποιοδήποτε είδος θορύβου, όπως αυτό υπεισέρχεται στην εκάστοτε πειραματική διαδικασία, διαδραματίζει καίριο ρόλο για την εύρυθμη και ορθή λειτουργία μιας οπτικής PUF, καθώς αλλοιώνει τα γεωμετρικά γνωρίσματα των καταγραφόμενων speckles της, οδηγώντας αναπόφευκτα στην υποβάθμιση της επαναληψιμότητας των παραγόμενων αποκρίσεών της. Σε αυτό το πλαίσιο λοιπόν, μερικές ενδεικτικές πηγές θορύβου που επηρεάζουν αποδεδειγμένα την επίδοση μιας οπτικής PUF ως προς την ιδιότητα του robustness της, είναι:

- οι μεταβολές επί της θερμοκρασίας, της υγρασίας αλλά και του φωτισμού του περιβάλλοντος χώρου, όπως αυτές λαμβάνουν χώρα κατά την διάρκεια της εκάστοτε μετρητικής διαδικασίας
- η μηχανική αστάθεια και οι ανεπιθύμητες μετατοπίσεις των οπτικών στοιχείων που απαρτίζουν το εκάστοτε σύστημα
- ο θόρυβος πλάτους και ο θόρυβος φάσης του χρησιμοποιούμενου laser [44]
- και ο θόρυβος της χρησιμοποιούμενης απεικονιστικής συσκευής, η οποία στην πλειοψηφία των περιπτώσεων αντιστοιχεί σε μια κάμερα CMOS [45]

3. ΜΕΘΟΔΟΙ ΕΠΕΞΕΡΓΑΣΙΑΣ ΚΑΙ ΑΝΑΛΥΣΗΣ ΔΕΔΟΜΕΝΩΝ

3.1 Επεξεργασία Δεδομένων

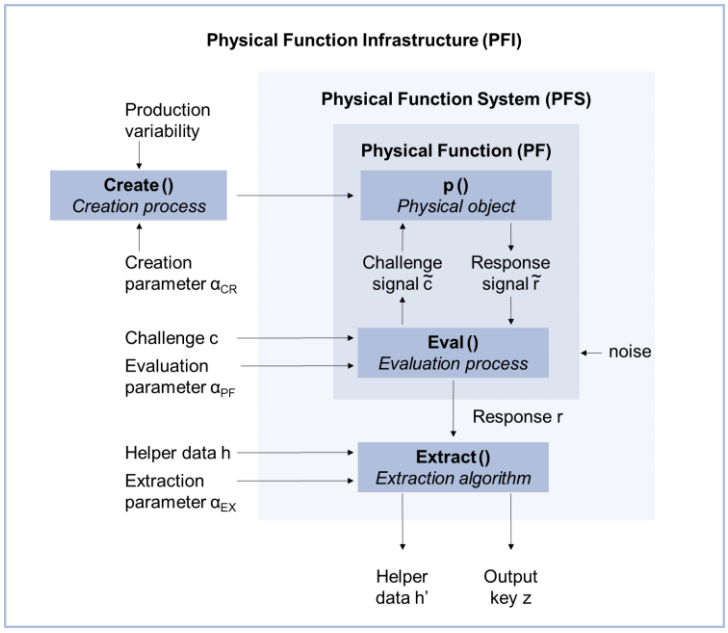
Όπως ήδη έχει αναφερθεί στις προηγούμενες ενότητες, η λειτουργικότητα ενός συστήματος PUF βασίζεται στη ντετερμινιστική και επομένως επαναλήψιμη συμπεριφορά ενός φυσικού αντικειμένου, όταν σε αυτό εφαρμοστεί μια καλώς ορισμένη εξωτερική διέγερση. Εντούτοις, κατά την πειραματική διερεύνηση οποιουδήποτε συστήματος, η παρουσία του θορύβου παρατήρησης στην μετρητική διαδικασία μειώνει την ικανότητα αναπαραγωγής των εξαγόμενων δεδομένων, υποβαθμίζοντας έτσι την αξιοπιστία τους.

Βάσει των ανωτέρω γίνεται φανερό ότι η κατόπτευση του θορύβου παρατήρησης σε πειραματικό επίπεδο και η μείωση της επίδρασής του στις παραγόμενες αποκρίσεις αποτελεί τον ακρογωνιαίο λίθο για την πρακτική υλοποίηση μιας PUF. Όμως, κατά τη χρήση της σε πραγματικές συνθήκες, καθίσταται αναγκαία η εισαγωγή μιας επιπλέον υπολογιστικής διαδικασίας, η οποία θα επιτρέψει την μεγιστοποιημένη καταστολή του θορύβου αυτού, οδηγώντας σε αναπαραγώγιμα και ασφαλή κλειδιά, κατάλληλα για κάθε κρυπτογραφική χρήση.

Η περιγραφή της υπολογιστικής διαδικασίας που χρησιμοποιήθηκε για να καλυφθούν οι ανάγκες της παρούσας μελέτης ακολουθεί στις επόμενες παραγράφους. Συνοπτικά, η διαδικασία αυτή περιλαμβάνει διάφορες τεχνικές επεξεργασίας σήματος και συναρτήσεις κατακερματισμού (hash functions), οι οποίες, σε συνδυασμό με έναν κώδικα διόρθωσης λαθών (Error Correction Code - ECC) που χρησιμοποιείται στα πλαίσια ενός ασαφούς εξαγωγέα (fuzzy extractor), οδηγούν σε δυαδικές ακολουθίες απαλλαγμένες από αλλοιώσεις και σφάλματα λόγω μετρητικού θορύβου. Προτού όμως παρατεθούν οι συγκεκριμένες μέθοδοι κρίνεται αναγκαίο να παρουσιαστεί το γενικό πλαίσιο περιγραφής μιας PUF.

3.1.1 Γενικό Πλαίσιο Περιγραφής μιας PUF

Το γενικό πλαίσιο περιγραφής μιας PUF προτάθηκε από τον Armknecht το 2011 [8] και παρουσιάζεται στο σχήμα 3.1.



Σχήμα 3.1: Το γενικό πλαίσιο περιγραφής μιας PUF [8]

Σύμφωνα με το σχήμα αυτό, το σύνολο του υλικού και υπολογιστικού εξοπλισμού που απαιτείται για την κατασκευή και την ολοκληρωμένη λειτουργία μιας PUF συγκροτεί το λεγόμενο Physical Function Infrastructure (PFI). Το PFI περιλαμβάνει τρεις βασικές διεργασίες, τις Create, Eval και Extract, οι οποίες ορίζονται ακολούθως.

Διεργασία Create: Διεργασία μέσω της οποίας προκύπτει η πηγή πολυπλοκότητας του συστήματος, δηλαδή το φυσικό αντικείμενο p (physical component). Εκτελείται από τον κατασκευαστή και ως είσοδο δέχεται μια σταθερή παράμετρο $\alpha_{CR,}$ η οποία εκφράζει όλες τις επιλεγμένες και ελεγχόμενες συνθήκες κάτω από τις οποίες λαμβάνει χώρα η εν λόγω διεργασία. Για παράδειγμα στην περίπτωση της φωτονικής PUF, η παράμετρος α_{CR} περιλαμβάνει όλους τους παράγοντες που επηρεάζουν και διαμορφώνουν τα αμετάβλητα χαρακτηριστικά του χρησιμοποιούμενου οπτικού μέσου, όπως είναι η διάμετρος του πυρήνα μιας οπτικής ίνας ή η κατανομή του δείκτη διάθλασής της. Από την άλλη πλευρά, η ζητούμενη πολυπλοκότητα του p προέρχεται από τις τυχαίες διακυμάνσεις της ίδιας ακριβώς διαδικασίας (production variability), οι οποίες παράγουν τα μοναδικά δομικά χαρακτηριστικά που οδηγούν σε ασυσχέτιστες αποκρίσεις. Παραδείγματος χάριν, στο ενδεχόμενο μιας οπτικής ίνας τέτοιου είδους χαρακτηριστικά αποτελούν οι εγγενείς ανομοιογένειες του πυρήνα της ή οι τυχαίες ατέλειες των επιφανειών εισόδου και εξόδου αυτής.

$$\text{Create}\left(\alpha_{CR}\right) \rightarrow p \tag{3.1}$$

Διεργασία Eval: η διεργασία αυτή σε συνδυασμό με το χρησιμοποιούμενο p απαρτίζουν τον βασικό πυρήνα του συστήματος, την επονομαζόμενη φυσική συνάρτηση (Physical Function - PF). Όπως παρουσιάζεται και στο σχήμα 3.1, όταν ένα challenge c εφαρμοστεί στο αντικείμενο p μιας PF, αυτό διεγείρεται παράγοντας μια αναλογική απόκριση $\tilde{r}$, η οποία στην συνέχεια μετατρέπεται στην αντίστοιχη ψηφιακή της αναπαράσταση r μέσω της διεργασίας Eval. Οι ρυθμίσεις ψηφιοποίησης καθορίζονται από τον κατασκευαστή, αποτελώντας την παράμετρο εισόδου α_{PF}. Η διαδικασία Eval και η παράμετρος α_{PF} σε μία φωτονική PUF αντιστοιχούν στην συσκευή ανίχνευσης και τις προεπιλεγμένες ρυθμίσεις της (π.χ. κάμερα και ανάλυση αυτής).

$$PF_{p,\alpha_{PF}}\left(c\right) = \text{Eval}_{p}\left(c, \alpha_{PF}\right) \rightarrow r \tag{3.2}$$

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι κατά την εκτέλεση των διαδικασιών Create και Eval υπεισέρχονται δυο διαφορετικά είδη θορύβου· στη μεν Create ο επιθυμητός θόρυβος παραγωγής που είναι υπεύθυνος για την τυχαιότητα των p, στη δε Eval ο ανεπιθύμητος θόρυβος παρατήρησης, η επίδραση του οποίου εξαλείφεται μέσω της τρίτης διεργασίας, της διεργασίας Extract.

Διεργασία Extract: η διεργασία Extract μαζί με την προαναφερθείσα PF συναποτελούν το σύστημα φυσικής συνάρτησης (Physical Function System), όπως αυτό εμφανίζεται στο σχήμα 3.1. Κύρια λειτουργία της Extract είναι η διόρθωση των διαφοροποιήσεων που προκύπτουν λόγω θορύβου στις ψηφιακές αποκρίσεις r, όταν αυτές καταγράφονται με πανομοιότυπες τις προαναφερθείσες παραμέτρους c,p και α_{PF}. Αυτό επιτυγχάνεται με την χρήση ενός fuzzy extractor, ο οποίος αντιστοιχίζει όλα τα θορυβικά r σε μία και μοναδική δυαδική έξοδο z, βασιζόμενος στην χρήση ενός κώδικα διόρθωσης λαθών. Η είσοδος της διεργασίας α_{EX} περιλαμβάνει ένα σύνολο προεπιλεγμένων παραμέτρων που σχετίζονται με τον ECC και οι οποίες θα παρουσιαστούν αναλυτικά παρακάτω.

$$\mathrm{PFS}_{p,\alpha_{PF},\alpha_{EX}}(c,h) = \mathrm{Extract}_{\alpha_{EX}}\left[\mathrm{PF}_{p,\alpha_{PF}}(c),h\right] \rightarrow (z,h') \qquad (3.3)$$

Γενικά, η διεργασία Extract εκτελείται σε δύο στάδια. Το πρώτο από αυτά είναι το στάδιο της εγγραφής (enrolment), κατά το οποίο μια διέγερση c εφαρμόζεται στην υπό μελέτη PF για πρώτη φορά και παράγεται η δυαδική έξοδος z μαζί με ένα σύνολο από βοηθητικά δεδομένα h. Το δεύτερο είναι το στάδιο της αυθεντικοποίησης (authentication), το οποίο λαμβάνει χώρα σε κάθε επανεφαρμογή της διέγερσης, όπου επιχειρείται η ανακατασκευή της εξόδου z χρησιμοποιώντας τον αλγόριθμο ECC και τα βοηθητικά δεδομένα h που παράχθηκαν κατά την εγγραφή.

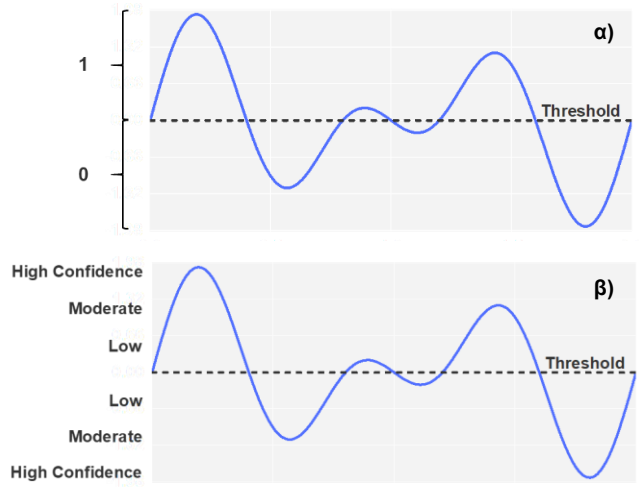
3.1.2 Σχεδιασμός Διεργασίας Extract

Στις ενότητες που ακολουθούν παρουσιάζονται οι επιμέρους διαδικασίες της διεργασίας Extract, συνοδευόμενες από το απαραίτητο θεωρητικό και μαθηματικό υπόβαθρό τους.

3.1.2.1 Κώδικας Ανίχνευσης και Διόρθωσης Λαθών

Εισαγωγικά, οι δυο θεμελιώδεις λειτουργίες οποιουδήποτε κώδικα διόρθωσης λαθών είναι η κωδικοποίηση και η αποκωδικοποίηση των πληροφορίων που διακινούνται μέσω ενός ενθόρυβου διαύλου επικοινωνίας. Ως κωδικοποίηση νοείται μια διαδικασία που εκτελείται από τον πομπό, μέσω της οποίας προστίθεται κάποιος αριθμός επιπλέον συμβόλων σε ένα μήνυμα προς μετάδοση (message), μετατρέποντάς το σε μια κωδική λέξη μεγαλύτερου μήκους (code word). Απεναντίας, η αποκωδικοποίηση λαμβάνει χώρα από τον δέκτη και αποτελεί την αντιστροφή της διαδικασίας, κατά την οποία εξάγεται από την αποσταλείσα κωδική λέξη ένα μήνυμα όσο το δυνατόν πιο κοντινό με το αρχικό. Τα επιπρόσθετα σύμβολα (redundant) με τα οποία πραγματοποιείται η επαύξηση του μηνύματος κατά την κωδικοποίηση είναι αυτά που υποβοηθούν την ανίχνευση και την διόρθωση των λαθών κατά την αποκωδικοποίηση.

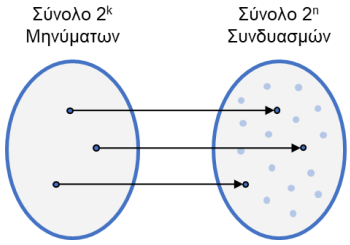
Εν γένει, οι τεχνικές κωδικοποίησης μπορούν να διαχωριστούν σε τρεις κύριες ομάδες [46], τις τμηματικές (block), τις συνελικτικές (convolutional) και τις σύνθετες (compound), οι οποίες αποτελούν έναν υβριδικό συνδυασμό των δύο πρώτων. Η κωδικοποίηση block βασίζεται κυρίως σε αλγεβρικές μεθόδους πεπερασμένων πεδίων, όπου το αρχικό μήνυμα χωρίζεται σε μη επικαλυπτόμενα τμήματα σταθερού μήκους k. Καθένα από τα τμήματα αυτά κωδικοποιείται ξεχωριστά και ανεξάρτητα, σε μία λέξη μήκους n, με τα (n-k) επιπλέον στοιχεία που προστίθενται στην άκρη του να προκύπτουν από την εφαρμογή μιας κατάλληλης συνάρτησης στα αρχικά σύμβολά του. Αντίθετα, στις συνελικτικές μεθόδους το παράθυρο τμηματοποίησης του αρχικού μηνύματος ολισθαίνει, με τα επιπλέον στοιχεία που υπολογίζονται να διαμοιράζονται στην παραγόμενη κωδική λέξη περιέχοντας όμως πληροφορία και από προηγούμενα blocks. Από την άλλη πλευρά, οι τεχνικές αποκωδικοποίησης συνήθως κατηγοριοποιούνται σε αυστηρής (hard) και ελαστικής απόφασης (soft decision), ανάλογα με τον αριθμό των επιπέδων κβάντισης που χρησιμοποιείται για την ψηφιοποίηση του αναλογικού σήματος και τον αριθμό των bits που χρειάζεται για την τελική αναπαράσταση κάθε συμβόλου [47]. Οι πρώτες υλοποιούνται με χρήση ενός επιπέδου κβάντισης μόνο, ορίζοντας την τελική τιμή του κάθε συμβόλου 1 ή 0 βάσει ενός προκαθορισμένου κατωφλίου. Οι δεύτερες περιλαμβάνουν στοιχεία που εκφράζονται με περισσότερα του ενός δυαδικά ψηφία, τα οποία διατηρούν την πληροφορία εγγύτητας των αναλογικών τιμών σε σχέση με το χρησιμοποιούμενο κατώφλι, παρέχοντας ουσιαστικά τον βαθμό εμπιστοσύνης τους. Η σχετική αντιπαραβολή των δύο ειδών παρουσιάζεται γραφικά στο 3.2.



Σχήμα 3.2: Δυαδικοποίηση σήματος με χρήση κατωφλίου και **α)** αποκωδικοποίηση hard decision **β)** αποκωδικοποίηση soft decision.

Τελικά, από τα παραπάνω είδη χρησιμοποιήθηκε ένας Bose-Chaudhuri-Hocquenghem (BCH) κώδικας διόρθωσης, ο οποίος αντιστοιχεί σε έναν τμηματικό γραμμικό αλγόριθμο κωδικοποίησης με έναν hard αποκωδικοποιητή. Ο κώδικας αυτός επιλέχθηκε λόγω της ευρείας χρήσης του, της απλής υλοποίησής του, της σχετικά χαμηλής πολυπλοκότητας του και επομένως των λιγότερων υπολογιστικών πόρων που απαιτεί σε σύγκριση με τις υπόλοιπες κατηγορίες.

Οι κώδικες BCH ανήκουν σε μια σημαντική υποκατηγορία των γραμμικών τμηματικών κωδικών, οι οποίοι είναι γνωστοί ως κυκλικοί κώδικες διόρθωσης [48]. Δέχονται ως είσοδο ένα δυαδικό μήνυμα k ψηφίων και παράγουν από αυτό μια κωδική λέξη μήκους n > k. Ουσιαστικά αποτελούν έναν αντιστρέψιμο γραμμικό μετασχηματισμό που αντιστοιχίζει με αμφιμονοσήμαντο τρόπο τα 2^k πιθανά μηνύματα εισόδου σε 2^k έγκυρες κωδικές λέξεις, οι οποίες απαρτίζουν ένα υποσύνολο των 2^n δυνατών επαναληπτικών διατάξεων που θα μπορούσαν να κατασκευαστούν από n δυαδικά στοιχεία.



Σχήμα 3.3: Γραμμικός τμηματικός κώδικας διόρθωσης, δηλαδή μια γραμμική 1-1 αντιστοιχία 2^k δυαδικών μηνύματων μήκους k, με 2^k έγκυρες κωδικές λέξεις μήκους n.

Η λειτουργία οποιουδήποτε κώδικα BCH καθορίζεται από τρεις κύριες παραμέτρους, τις n, k και d_{min}, οι οποίες αποτελούν και την προαναφερθείσα είσοδο a_{EX} της διεργασίας Extract. Η παράμετρος k συμβολίζει το μήκος των μηνυμάτων εισόδου του κώδικα, ενώ η n το μήκος των αντιστοίχων κωδικών λέξεων του. Η n λαμβάνει τιμές μόνο της μορφής $n = 2^m-1$, όπου m είναι ένας θετικός ακέραιος αριθμός με $m \geq 3$. Η παράμετρος d_{min} συμβολίζει την ελάχιστη απόσταση Hamming μεταξύ των έγκυρων κωδικών λέξεων του κώδικα, δηλαδή το μικρότερο πλήθος των θέσεων, για τις οποίες τα ψηφία αυτών μπορεί να διαφέρουν. Μέσω αυτής προσδιορίζεται το μέγιστο πλήθος σφαλμάτων t που δύναται να απαλειφθεί επιτυχώς για το δοθέν μήκος n, το οποίο ονομάζεται διορθωτική ικανότητα του BCH (error correction capability) και αποτιμάται από την σχέση $t = (d_{min}-1) / 2$. Δεδομένου του ζεύγους τιμών m και t προσδιορίζονται επίσης τα επιτρεπτά μήκη k του μηνύματος εισόδου, από τον αριθμό (n-k) των επιπλέον ψηφίων που χρειάζεται

να προστεθούν σε αυτό, ώστε να επιτευχθεί η ζητούμενη διόρθωση t λαθών, ο οποίος θα πρέπει να ικανοποιεί την συνθήκη (n-k) ≤ mt.

Συνοψίζοντας, δεδομένου ενός ζεύγους τιμών (m,t) ορίζεται ένας δυαδικός κώδικας BCH(n,k,d_{min}) με ικανότητα διόρθωσης t και:

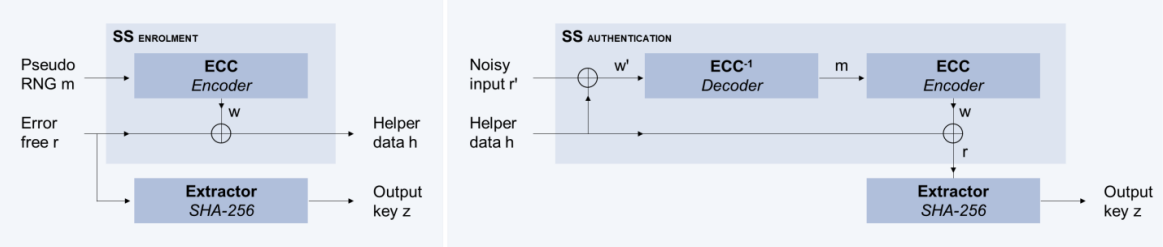
- Μήκος κωδικής λέξης $n = 2^m - 1$, όπου $m \geq 3$
- Αριθμός επιπλέον συμβόλων $n - k \leq mt$
- Ελάχιστη απόσταση Hamming $d_{min} \geq 2t + 1$

3.1.2.2 Fuzzy Extractor

Ο όρος fuzzy extractor αναφέρεται σε μια τεχνική παραγωγής κρυπτογραφικών κλειδιών που αρχικά αναπτύχθηκε για την ασφαλή πιστοποίηση βιομετρικών δεδομένων, αλλά η οποία στην πραγματικότητα μπορεί να δεχτεί ως είσοδο οποιοδήποτε είδος ενθόρυβης πληροφορίας και να το μετατρέψει σε μια αναπαραγώγιμη δυαδική έξοδο, κατάλληλη για κάθε κρυπτογραφική χρήση.

Η χρήση ενός fuzzy extractor είναι λοιπόν διττή και η λειτουργία του διαχωρίζεται σε δύο κύριες διαδικασίες [49]. Η πρώτη εξ αυτών αποσκοπεί στην εξαγωγή μιας τυχαίας δυαδικής ακολουθίας από τα διαθέσιμα θορυβικά δεδομένα, η οποία συμπιέζει και αποκρύπτει την αρχική πληροφορία, ενισχύοντας έτσι την συνολική ασφάλεια του συστήματος (privacy amplification). Αυτή συνήθως υλοποιείται με την εφαρμογή ενός εξαγωγέα τυχαιότητας απευθείας στα σύμβολα εισόδου (randomness extractor), ο οποίος πρακτικά αντιστοιχεί σε μια κρυπτογραφική συνάρτηση κατακερματισμού, όπως είναι η SHA-256 [50]. Η δεύτερη διαδικασία στοχεύει στην διόρθωση των σφαλμάτων που μπορεί να υπεισέλθουν στην παραχθείσα δυαδική έξοδο λόγω του μετρητικού θορύβου, καθιστώντας εφικτή την ακριβή ανακατασκευή της (information reconciliation). Αυτή γενικά επιτυγχάνεται μέσω ενός κώδικα ανίχνευσης και διόρθωσης λαθών, ο οποίος στα πλαίσια ενός ασφαλούς σχήματος (secure sketch - SS) εκτελείται σε δύο στάδια, αυτά της εγγραφής και της αυθεντικοποίησης.

Στο σχήμα 3.4 αποτυπώνεται η τελική μορφή του fuzzy extractor που υλοποιήθηκε για να καλυφθούν οι ανάγκες της παρούσας εργασίας. Το ασφαλές σχήμα που επιλέχθηκε να χρησιμοποιηθεί αντιστοιχεί σε ένα code-offset SS [49] [51], το οποίο πρακτικά συμπίπτει με το λεγόμενο fuzzy commitment scheme που προτάθηκε από τον A. Juels το 1999 [52].



Σχήμα 3.4: Υλοποίηση fuzzy extractor, με χρήση ενός code-offset secure sketch, για την ορθή ανάκτηση της πληροφορίας εισόδου r, και ενός εξαγωγέα τυχαιότητας SHA-256, για την συμπίεση και την ασφαλή απόκρυψη της.

Γενικά, κατά το στάδιο της εγγραφής οποιουδήποτε fuzzy extractor, αρχικά εισάγεται μια δυαδική ακολουθία $r \in \{0,1\}^n$ n ψηφίων, η οποία αποτελεί την πληροφορία αναφοράς του συστήματος που πρέπει να κρυπτογραφηθεί και να ανακτηθεί σε δεύτερο χρόνο. Από αυτήν κατασκευάζεται το ζητούμενο κρυπτογραφικό κλειδί $z \in \{0,1\}^{\ell}$, όπου $\ell < n$, μέσω ενός προκαθορισμένου εξαγωγέα τυχαιότητας. Το κλειδί αυτό στη συνέχεια αντιστοιχίζεται σε ένα

ανεξάρτητο μήνυμα $m \in \{0,1\}^k$, όπου $k < n$, το οποίο συνήθως παράγεται μέσω μιας γεννήτριας ψευδοτυχαίων αριθμών και μετατρέπεται μέσω του αλγορίθμου ECC σε μια κωδική λέξη $w \in \{0,1\}^n$. Κατόπιν, υπολογίζεται η XOR μεταξύ της ακολουθίας r και της ευρεθείσας κωδικής λέξης w, το αποτέλεσμα της οποίας αποτελεί την τελική έξοδο του συγκεκριμένου σταδίου, απαρτίζοντας τα λεγόμενα βοηθητικά δεδομένα h. Τα βοηθητικά δεδομένα h ουσιαστικά περιέχουν αυτούσια αλλά συγκεκαλυμένη την αρχική ακολουθία, γεγονός που καθιστά τη δημόσια διακίνηση τους ασφαλή, επιτρέποντας την ανάκτηση της ακολουθίας αυτής χωρίς να επιβάλλεται η καθαυτή αποθήκευση της.

Από την άλλη πλευρά, η ανακατασκευή της r από μια θορυβική έκδοσή της r' αποπειράται κατά το στάδιο της αυθεντικοποίησης, χρησιμοποιώντας τα βοηθητικά δεδομένα h που παράχθηκαν κατά την εγγραφή. Αρχικά, εξάγεται μια αλλοιωμένη κωδική λέξη w' από την XOR της θορυβικής ακολουθίας r' και των διαθέσιμων βοηθητικών δεδομένων h, η οποία στην συνέχεια αποκωδικοποιείται μέσω του χρησιμοποιούμενου κώδικα διόρθωσης σε ένα μήνυμα m'. Όταν το πλήθος των συμβόλων που διαφέρουν μεταξύ των ακολουθιών r και r' είναι μικρότερο από την διορθωτική ικανότητα του ECC, τότε η αποκατάσταση των σφαλμάτων κατά την αποκωδικοποίηση είναι επιτυχημένη και το μήνυμα m' ταυτίζεται με το αντίστοιχο m του προηγούμενου σταδίου. Σε αυτή την περίπτωση, το διορθωμένο μήνυμα επανακωδικοποιείται οδηγώντας στην σωστή κωδική λέξη w, η XOR της οποίας με τα βοηθητικά δεδομένα h καταλήγει στην αρχική ακολουθία r. Σε αυτήν εφαρμόζεται ο ίδιος εξαγωγέας τυχαιότητας με αυτόν της εγγραφής, αναπαράγοντας τελικά το ζητούμενο κρυπτογραφικό κλειδί z.

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι κάθε code-offset fuzzy extractor, όπως αυτός που παρουσιάστηκε στις προηγούμενες παραγράφους, μπορεί να χρησιμοποιηθεί ως μια ολοκληρωμένη και πλήρως λειτουργική διεργασία Extract, η οποία ενσωματώνεται αυτούσια και χωρίς επιπρόσθετα βήματα σε οποιαδήποτε PUF που παράγει εγγενώς δυαδικές αποκρίσεις. Εντούτοις για την υπό μελέτη περίπτωση, όπου οι καταγραφόμενες αποκρίσεις αντιστοιχούν σε ψηφιακές εικόνες με παρόμοια γεωμετρικά χαρακτηριστικά, καθίσταται αναγκαία η προσθήκη κάποιων επιπλέον μεθόδων επεξεργασίας, οι οποίες θα επιτρέψουν τον μετασχηματισμό των εικόνων αυτών σε ένα σύνολο από αντιπροσωπευτικές, αναπαραγώγιμες και απρόβλεπτες δυαδικές ακολουθίες.

3.1.2.3 Τεχνικές Επεξεργασίας Εικόνων

Όπως ήδη ειπώθηκε, η περαιτέρω επεξεργασία των διαθέσιμων πειραματικών εικόνων έχει ως αντικειμενικό σκοπό την εξαγωγή ενδιάμεσων δυαδικών ακολουθιών, οι οποίες θα πρέπει να ικανοποιούν τις βασικές ιδιότητες μιας PUF. Στα πλαίσια της παρούσας υλοποίησης λοιπόν, ο αντικειμενικός αυτός σκοπός επιτυγχάνεται παρεμβάλλοντας έναν συνδυασμό από επιπλέον μεθόδους, οι οποίες επιτελούν τις ακόλουθες λειτουργίες [53]:

- Ελάττωση των επιπτώσεων του πειραματικού θορύβου, ο οποίος αλλοιώνει τα βασικά χαρακτηριστικά των εικόνων, υποβαθμίζοντας την επαναληψιμότητα των ακολουθιών.
- Ενίσχυση και εξαγωγή των πιο αντιπροσωπευτικών γεωμετρικών γνωρισμάτων τους, ώστε εικόνες με παρεμφερές περιεχόμενο να οδηγούν σε όσο το δυνατόν πιο κοντινές ακολουθίες, ενώ εικόνες με ανόμοια μορφολογική δομή σε όσο το δυνατόν πιο ασυσχέτιστες.

- Μη-αντιστρεπτή συμπίεση, δυαδικοποίηση και τυχαιοποίηση των γνωρισμάτων αυτών, ώστε οι προκύπτουσες ακολουθίες να είναι κρυπτογραφικά ασφαλείς.

3.1.2.3.1 Ευθυγράμμιση Πειραματικών Εικόνων

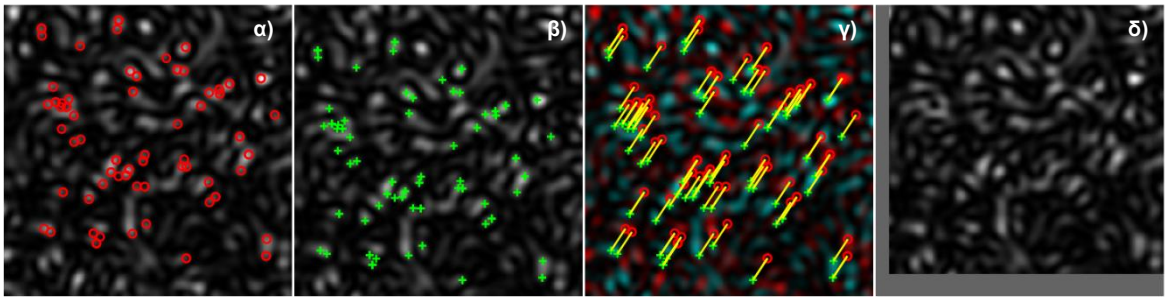
Η ευθυγράμμιση των πειραματικών δεδομένων αποσκοπεί στην υπολογιστική εξάλειψη των επιπτώσεων του θορύβου που αποδίδεται σε γραμμικές μετακινήσεις του επιπέδου παρατήρησης (π.χ. αστάθεια της απεικονιστικής συσκευής). Ουσιαστικά πρόκειται για την διόρθωση της σχετικής μετατόπισης αποκρίσεων που έχουν ληφθεί υπό πανομοιότυπες πειραματικές συνθήκες και διαθέτουν κοινά μορφολογικά χαρακτηριστικά, τα οποία όμως για κάποιον λόγο δεν ταυτίζονται χωρικά.

Γενικά, η εκτίμηση της μετατόπισης δύο αποκρίσεων πραγματοποιείται με την απευθείας σύγκριση της δομής τους, θεωρώντας τη μια εξ αυτών ως υπόδειγμα. Η εν λόγω σύγκριση συνήθως περιορίζεται σε συγκεκριμένα σημεία της εκάστοτε δομής, τα οποία ονομάζονται σημεία ενδιαφέροντος, και λαμβάνει χώρα μέσω ενός κατάλληλου κριτηρίου ομοιότητας, το οποίο επιτρέπει την αντιστοίχιση των ευρεθέντων σημείων σε ζεύγη.

Στην προκειμένη περίπτωση, ως αντιπαραβαλλόμενα σημεία ενδιαφέροντος χρησιμοποιούνται οι γωνίες των υπό μελέτη εικόνων, ο εντοπισμός των οποίων διεξάγεται με την μέθοδο ανίχνευσης Harris [54], η εξαγωγή τους με την μέθοδο FREAK [55] και η αντιστοίχιση τους σε ζεύγη με την ελαχιστοποίηση του αθροίσματος των τετραγωνικών τους διαφορών (Sum of Square Differences). Η σχετική μετατόπιση των αποκρίσεων εκτιμάται ανά άξονα από τους διάμεσους s_x και s_y των αποστάσεων που χωρίζουν όλες τις αντιστοιχισμένες γωνίες, ενώ η ζητούμενη διόρθωση λαμβάνει χώρα εφαρμόζοντας τον ακόλουθο ομοπαράλληλο μετασχηματισμό (affine transformation) [56] στην μία από αυτές:

$$\begin{bmatrix} 1 & 0 & s_x \\ 0 & 1 & s_y \\ 0 & 0 & 1 \end{bmatrix} \tag{3.4}$$

Στο σημείο αυτό θα πρέπει να σημειωθεί ότι στα άκρα οποιουδήποτε διορθωμένου στιγμιότυπου εμφανίζονται περιοχές που βγαίνουν εκτός πλαισίου. Οι περιοχές αυτές αποκόπτονται από όλες τις χρησιμοποιούμενες εικόνες, ώστε το τελικό μέγεθός τους να συμπίπτει.



Σχήμα 3.5: α) Στιγμιότυπο πειραματικού speckle pattern, συνοδευόμενο από τα ευρεθέντα σημεία ενδιαφέροντος του. **β)** Το ίδιο speckle, μετατοπισμένο κατά -20 pixels στον άξονα x και -30 pixels στον άξονα y. **γ)** Επικαλυπτόμενη απεικόνιση των δυο εικόνων, με τα ζεύγη των αντιστοιχισμένων γωνιών τους. **δ)** Το διορθωμένο speckle β, ως προς το speckle της εικόνας α.

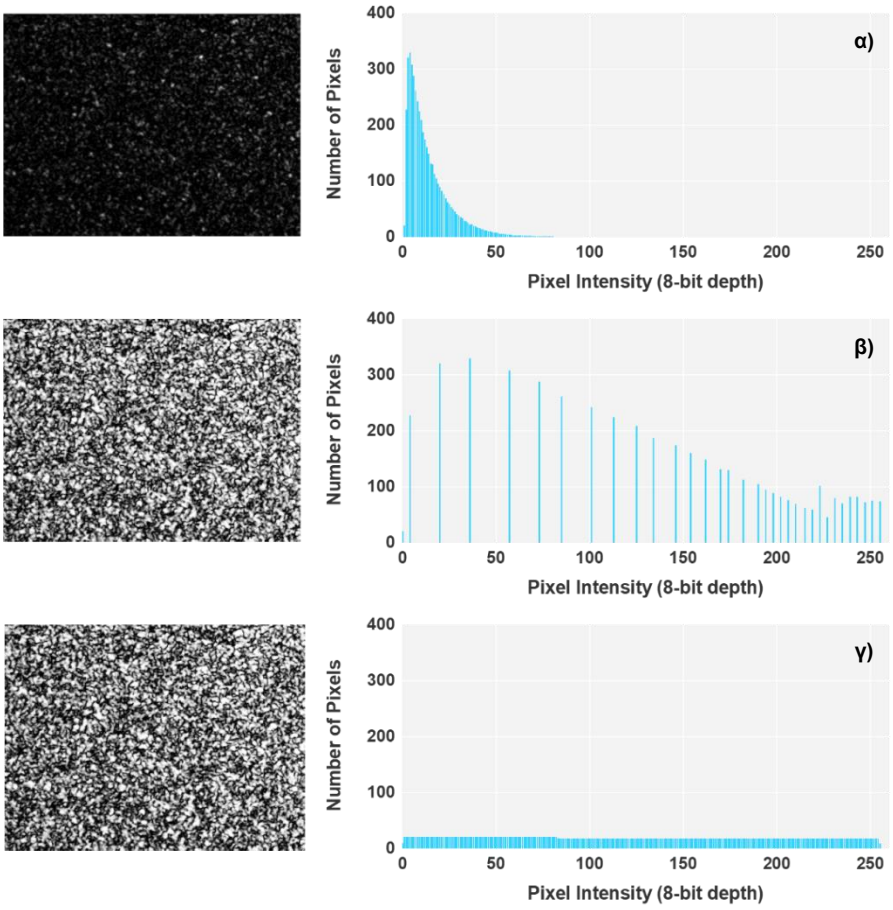
Θα πρέπει επίσης να υπογραμμισθεί ότι ο παραπάνω μετασχηματισμός εκφράζει μόνο γραμμικές μετακινήσεις στο επίπεδο xy, καθώς κατά την διάρκεια των πειραματικών μετρήσεων δεν παρατηρήθηκαν μεταβολές στην κλιμάκωση και την

σχετική γωνία των εικόνων που θα μπορούσαν να επηρεάσουν την επαναληψιμότητα τους.

3.1.2.3.2 Ακριβής Ισοστάθμιση Ιστογραμμάτων

Η ισοστάθμιση ιστογράμματος (histogram equalization) είναι μία από τις πιο δημοφιλείς μεθόδους επεξεργασίας εικόνων, η οποία χρησιμοποιείται για την αύξηση της ευκρίνειας σε φωτογραφίες με πολύ χαμηλή αντίθεση. Ουσιαστικά πρόκειται για έναν γραμμικό και αντιστρεπτό μετασχηματισμό που εφαρμόζεται στις τιμές των διαθέσιμων εικονοστοιχείων, προκειμένου το ιστόγραμμα τους να διευρυνθεί σε όλο το δυναμικό εύρος εντάσεων και να αποκτήσει μια σχεδόν ομοιόμορφη κατανομή.

Εν γένει, η ισοστάθμιση ιστογράμματος πραγματοποιείται λαμβάνοντας υπόψιν μόνο το χρωματικό βάθος K της υπό μελέτη εικόνας. Με άλλα λόγια, οι υπάρχουσες εντάσεις αναδιανέμονται σε K κλάσεις ισοδυναμίας, όσες δηλαδή και το συνολικό πλήθος των χρωματικών διαβαθμίσεων, χωρίς όμως να συνυπολογίζεται η χωρική διευθέτηση των τιμών στο επίπεδο. Αυτό επιτυγχάνεται συνήθως ως εξής: αρχικά προσδιορίζεται η αθροιστική συνάρτηση συχνότητας των εντάσεων της εικόνας και από το γινόμενο των στοιχείων αυτής με την τιμή (K-1) προκύπτουν οι καινούριες κλάσεις ισοδυναμίας του τροποποιημένου ιστογράμματος, με τις οποίες αντικαθίστανται μία προς μία όλες οι παλιές τιμές έντασης των pixels.



Σχήμα 3.6: α) Speckle με ανάλυση 600x800 pixels και χρωματικό βάθος 2^8 bits, συνοδευόμενο από το αντίστοιχο ιστόγραμμα έντασεών του. **β)** Το ίδιο speckle με το τροποποιημένο ιστόγραμμα που προέκυψε από την συμβατική τεχνική ιστοστάθμισης. **γ)** Τα αποτελέσματα που αντιστοιχούν στην μέθοδο της ακριβούς ισοστάθμισης.

Εντούτοις για τις ανάγκες της παρούσας εργασίας επιλέχθηκε μια ακριβέστερη τεχνική ισοστάθμισης, η οποία αποτελεί επέκταση της ήδη περιγραφείσας. Η προσέγγιση αυτή περιλαμβάνει το επιπλέον βήμα της αυστηρής διατάξεως που

πρακτικά αντιστοιχεί στην λεξικογραφική ταξινόμηση των pixels και το οποίο καθιστά εφικτή την προσαρμογή ενός δεδομένου ιστογράμματος σε μια οποιαδήποτε συνάρτηση κατανομής [57],[58].

Ειδικότερα, όλα τα εικονοστοιχεία μιας εικόνας συγκεντρώνονται σε ένα μονοδιάστατο διάνυσμα $X \in \mathbb{R}^N$, όπου N ο συνολικός αριθμός τους, και κατατάσσονται με αύξουσα σειρά έντασης. Εάν οι εντάσεις δύο pixels συμπίπτουν, η σχετική τους θέση στο διάνυσμα X καθορίζεται από την μέση τιμή των άμεσα γειτονικών τους εικονοστοιχείων. Στην περίπτωση όπου και αυτή ταυτίζεται, η περιοχή γειτνίασης που εξετάζεται γύρω από τα υπό μελέτη pixels αυξάνει, μέχρις ότου εντοπισθεί εκείνο που περιβάλλεται από την υψηλότερη μέση ένταση. Αυτό τελικά θα προηγείται και στο διάνυσμα X. Αφού λοιπόν ταξινομηθούν με τον άνωθεν τρόπο όλα τα εικονοστοιχεία της εικόνας εντός του X, στην συνέχεια διαχωρίζονται σε K ομάδες, οι οποίες είναι και οι κλάσεις ισοδυναμίας του καινούριου ιστογράμματος. Το πλήθος των στοιχείων κάθε μίας ομάδας καθορίζεται από την προεπιλεγμένη συνάρτηση κατανομής, με τις αρχικές εντάσεις της εικόνας εν τέλει να αντικαθίστανται από την τιμή κλάσης στην οποία έχουν καταλήξει

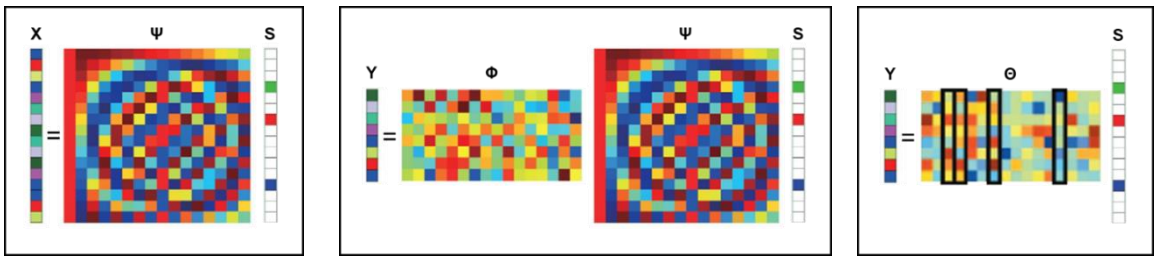
3.1.2.3.3 Παραγωγή Δυαδικών Ακολουθιών

Για την μετατροπή των διαθέσιμων πειραματικών εικόνων σε ένα σύνολο από αντιπροσωπευτικές δυαδικές ακολουθίες που ικανοποιούν τις τρεις βασικές ιδιότητες μιας PUF δοκιμάστηκαν τέσσερεις διαφορετικές τεχνικές: η Random Binary Method (RBM), η Gabor Binary Method (GBM), η Singular Value Decomposition (SVD) και η Non-Negative Matrix Factorization (NMF). Οι τεχνικές RBM και GBM αντιστοιχούν σε δύο εναλλακτικές υλοποιήσεις της λεγόμενης συμπιεστικής δειγματοληψίας (compressive sensing), οι θεμελιώδεις αρχές της οποίας παρατίθενται στο Παράρτημα Ι, ενώ οι SVD και NMF προκύπτουν από βασικές έννοιες της γραμμικής άλγεβρας και της θεωρίας πινάκων, ουσιαστικά αποτελώντας δύο εναλλακτικές μεθόδους παραγοντοποίησης μητρών.

3.1.2.3.3.1 Random Binary Method (RBM)

Περιληπτικά, η συμπιεστική δειγματοληψία αποτελεί μια γενική μεθοδολογία για την εξαγωγή και την συμπίεση των χαρακτηριστικών γνωρισμάτων ενός σήματος, με απώτερο σκοπό την δυνατότητα ανακατασκευής του από ένα πλήθος δειγμάτων αρκετά μικρότερο από αυτό που ορίζει το θεώρημα του Nyquist. Αυτό επιτυγχάνεται επιστρατεύοντας τις ιδιότητες της αραιότητας και της ασυμφωνίας. [59]

Η ιδιότητα της αραιότητας (sparsity) εκφράζει την ιδέα ότι τα περισσότερα σήματα στην φύση, όταν εκφραστούν σε μια κατάλληλη βάση αναπαράστασης, μπορούν να συνοψιστούν από έναν πολύ μικρό αριθμό στοιχείων. Με άλλα λόγια, για ένα σήμα X δύναται να εντοπιστεί ένας μαθηματικός μετασχηματισμός Ψ που επιτρέπει μια αραιή περιγραφή S αυτού, η οποία περιέχει όλες τις αναγκαίες πληροφορίες για την ακριβή ανακατασκευή του. Από την άλλη πλευρά, η ιδιότητα της ασυμφωνίας (incoherence) επεκτείνει τον δυισμό μεταξύ των πεδίων του χρόνου και της συχνότητας: όπως το φάσμα ενός σήματος με μηδενική έκταση στο χρόνο εμπεριέχει όλες τις συχνότητες, έτσι και ένα σήμα που έχει μια αραιή αναπαράσταση S στην βάση Ψ θα πρέπει να εκτείνεται σε όλο το πεδίο μέτρησής του. Με άλλα λόγια, για μια διανυσματική βάση Ψ δύναται να εντοπιστεί ένας μαθηματικός μετασχηματισμός Φ, οι στήλες του οποίου έχουν πολύ πυκνή αναπαράσταση στη Ψ σε αντίθεση με το προς ανακατασκευή σήμα X και η εφαρμογή του σε αυτό αποτελεί την αποδοτικότερη μέθοδο δειγματοληψίας του.



Σχήμα 3.7: α) Αραιότητα: X = ΨS. Ένα σήμα X μπορεί να γραφεί ως ένας γραμμικός συνδυασμός των στηλών μιας ορθοκανονικής βάσης Ψ, με το διάνυσμα των συντελεστών στάθμισης S να αποτελεί την αραιή αναπαράσταση του [60] **β)** Συμπιεστική δειγματοληψία στο πεδίο καταγραφής του σήματος: Y = ΦX = Φ(ΨS), όπου Ψ η βάση αραιής αναπαράστασης, Φ η βάση δειγματοληψίας και Y η συμπιεσμένη έκδοση του αρχικού σήματος X [60] **γ)** Συμπιεστική δειγματοληψία στο πεδίο μετασχηματισμού του σήματος: Y = (ΦΨ)S = ΘS, όπου Θ = ΦΨ ο πίνακας συμπιεστικής δειγματοληψίας και S η αραιή αναπαράσταση του αρχικού σήματος X [60]

Βάσει των παραπάνω γίνεται εμφανές και το κυριότερο μειονέκτημα που παρουσιάζουν οι συμβατικές τεχνικές ανάκτησης σήματος έναντι των μεθόδων που βασίζονται στην θεωρία συμπιεστικής δειγματοληψίας: ενώ οι πρώτες περιλαμβάνουν τρία βήματα, την λήψη ολόκληρου του σήματος, τον μετασχηματισμό του στην προαναφερθείσα βάση Ψ και την δειγματοληψία των στοιχείων που το αναπαριστούν με αραιό τρόπο, στις δεύτερες, οι διαδικασίες δειγματοληψίας και συμπίεσης λαμβάνουν χώρα με ένα μόνο βήμα, το οποίο μάλιστα εκτελείται απευθείας στο πεδίο καταγραφής του σήματος μέσω του πίνακα Φ.

Σε αυτό το πλαίσιο λοιπόν, το πρόβλημα της εξαγωγής των ζητούμενων δυαδικών ακολουθιών από τα διαθέσιμα πειραματικά δεδομένα μεταπίπτει στην εύρεση μιας κατάλληλα κατασκευασμένης υπέρθεσης Θ = ΦΨ, τα διανύσματα της οποίας πρέπει να είναι όσο το δυνατόν περισσότερο ασύμφωνα, ώστε να μεγιστοποιείται η πληροφορία που διατηρείται από αυτά με τον ελάχιστο αριθμό δειγμάτων. Η πιο προφανής βάση που μπορεί να χρησιμοποιηθεί για τον σκοπό αυτό είναι η διανυσματική βάση Fourier, μέσω της οποίας πραγματοποιείται η μετάβαση από το πεδίο καταγραφής ενός σήματος στο πεδίο της συχνότητας και καθίσταται εφικτή η λήψη της μιγαδικής φασματικής απόκρισής του.

Σύμφωνα με την θεωρία Fourier, οποιοδήποτε πεπερασμένο ψηφιακό σήμα μπορεί να αναπαρασταθεί ως ένα ανάπτυγμα αρμονικών συνιστωσών, εφαρμόζοντας τον διακριτό μετασχηματισμό Fourier σε αυτό. Η δισδιάστατη μορφή του εν λόγω μετασχηματισμού (Discrete Fourier Transformation - DFT) δίνεται από την σχέση:

$$\Im(u,v) = \sum_{p=0}^{N_1-1}\sum_{q=0}^{N_2-1} X(p,q)\,\exp\left[-2\pi j\left(\frac{up}{N_1}+\frac{vq}{N_2}\right)\right] \qquad (3.5)$$

όπου στην προκειμένη περίπτωση το σήμα X(p,q) είναι μια εικόνα ανάλυσης $N_1 \times N_2$, p,q είναι οι συντεταγμένες των pixels στο επίπεδο και u,v οι διακριτές μεταβλητές χωρικής συχνότητας ανά διάσταση [61]. Το μέτρο $|\Im(u,v)| = \{Res[\Im(u,v)]^2+Im[\Im(u,v)]^2\}^{1/2}$ του άνωθεν μετασχηματισμού αποτελεί το λεγόμενο φάσμα πλάτους της εικόνας X(p,q) και καθορίζει το ποσό κάθε αρμονικής συνιστώσας που εμφανίζεται σε αυτήν, ενώ η γωνία $\angle[\Im(u,v)] = \arctan\{Im[\Im(u,v)] / Res[\Im(u,v)]\}$ αποτελεί το φάσμα φάσης της και καθορίζει την ακριβή θέση της εκάστοτε συνιστώσας στο επίπεδο. Τέλος, η επιστροφή στην αρχική X(p,q) πραγματοποιείται μέσω του αντίστροφου διακριτού μετασχηματισμού Fourier (Inverse Discrete Fourier Transform - IDFT), ο οποίος δίνεται από την ακόλουθη σχέση:

$$X(p,q) = \frac{1}{N_1 N_2} \sum_{u=0}^{N_1-1} \sum_{v=0}^{N_2-1} \Im(u,v) \exp\left[2\pi j \left(\frac{up}{N_1} + \frac{vq}{N_2} \right) \right] \quad (3.6)$$

Στο σχήμα 3.8 παρουσιάζονται δύο παραδείγματα φωτογραφιών μαζί με τα αντίστοιχα φάσματα του πλάτους και της φάσης τους, ώστε να γίνει καλύτερα αντιληπτή η εφαρμογή και η ερμηνεία των παραπάνω εξισώσεων στο πεδίο επεξεργασίας εικόνας. Όπως φαίνεται λοιπόν και από το σχήμα 3.8, το φάσμα πλάτους μιας φωτογραφίας εμπεριέχει το πλήθος των χρωματικών διαβαθμίσεων της, ενώ το φάσμα φάσης της τα γεωμετρικά γνωρίσματα αυτής. Με άλλα λόγια, το πραγματικό και το φανταστικό μέρος του μιγαδικού φάσματος μιας εικόνας περιλαμβάνει όλη την πληροφορία που χρειάζεται για την ικανοποιητική ανασύνθεση της από ένα πλήθος στοιχείων, το οποίο, όταν επιλέγεται σύμφωνα με τις αρχές της συμπιεστικής δειγματοληψίας, δύναται να είναι αρκετά μικρότερο από αυτό που ορίζει το θεώρημα του Nyquist.

Εν προκειμένω, ως πρώτη μέθοδος εξαγωγής δυαδικών ακολουθιών επιλέχθηκε η τυχαία καταγραφή και δυαδικοποίηση στοιχείων από το μιγαδικό φάσμα των speckles. Εντούτοις, η προσέγγιση αυτή δεν εγγυάται απόλυτα την διατήρηση του μέγιστου όγκου πληροφορίας, καθώς ενέχει τον κίνδυνο λήψης δεδομένων από περιοχές με μηδενικό συχνοτικό περιεχόμενο, επομένως, θεωρήθηκε σκόπιμο να προστεθεί ένα επιπλέον βήμα κατά την υλοποίηση της. Συγκεκριμένα, ενσωματώθηκε το βήμα της διαμόρφωσης φάσματος [62], το οποίο συνήθως συντελείται με την εισαγωγή πλασματικού θορύβου στην εικόνα, επιτυγχάνοντας την διεύρυνση του εύρους ζώνης της χωρίς απώλεια ισχύος και την εξάλειψη των συχνοτικών περιοχών με μηδενική πληροφορία.

Συνεπώς, η τελική μορφή της παρούσας τεχνικής, η οποία θα αναφέρεται στο εξής ως RBM, μπορεί να συνοψιστεί από την εξίσωση [22][63]:

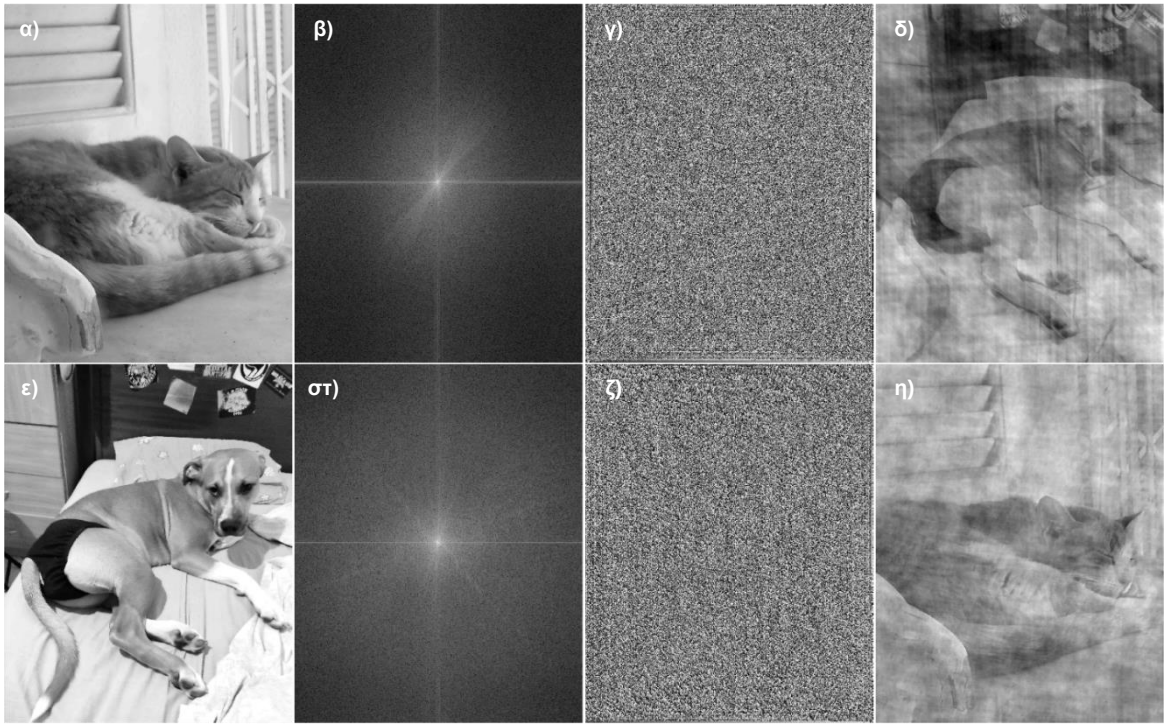
$$Y = H\left(\sqrt{\frac{N}{M}} S \Im B \right) X = H\left\{ \sqrt{\frac{N}{M}} S\left[W_2 (B \circ X) W_1 \right] \right\} \quad (3.7)$$

όπου το σύμβολο ◦ αντιπροσωπεύει τον πολλαπλασιασμό στοιχείο προς στοιχείο, το $X \in \mathbb{R}^{N1 \times N2}$ ένα κανονικοποιημένο speckle pattern και το $Y \in \{0,1\}^M$ την ζητούμενη δυαδική αναπαράσταση αυτού. Η κανονικοποίηση μιας εικόνας λαμβάνει χώρα μέσω του τύπου:

$$X_{pq} = \frac{X_{pq} - \bar{X}}{\sigma} \quad (3.8)$$

με $\bar{X}$ την μέση τιμή και σ την τυπική απόκλιση των τιμών φωτεινότητας που περιλαμβάνει. Η διαπλάτυνση του φάσματός της από την άλλη πλευρά, πραγματοποιείται από το γινόμενο αυτής με τον πίνακα B. Ο $B \in \mathbb{R}^{N1 \times N2}$ αποτελεί έναν ψευδοτυχαίο πίνακα που περιέχει μόνο τις τιμές ±1, για τις οποίες ισχύει η σχέση $Pr[B_{pq} = 1] = Pr[B_{pq} = -1] = 0.5$, δηλαδή το ενδεχόμενο εμφάνισης τους είναι ισοπίθανο. Οι $W_1 \in \mathbb{C}^{N1 \times N1}$ και $W_2 \in \mathbb{C}^{N2 \times N2}$ αντιστοιχούν στις μήτρες του δισ-διάστατου DFT, τα στοιχεία των οποίων υπολογίζονται από την σχέση $W_{pq} = [\exp(-2pj/N_i)]^{pq}/\sqrt{N_i}$ με i =1,2 και η εφαρμογή τους οδηγεί από το πεδίο του χώρου στο πεδίο της συχνότητας. Ο S συμβολίζει έναν πίνακα M ακεραίων τιμών που επιλέγονται με ψευδοτυχαίο τρόπο από μία ομοιόμορφη κατανομή U(0,N), όπου $N = N_1 N_2$, και οι οποίες αντιστοιχούν στους δείκτες θέσεως των στοιχείων του μιγαδικού φάσματος που απαρτίζουν την απεικόνιση $Y = S\{\Im[BX]\} \in \mathbb{R}^M$. Ο συντελεστής $\sqrt{(N/M)}$ κανονικοποιεί την εν λόγω απεικόνιση, η οποία ουσιαστικά

προκύπτει από την οριζόντια συνένωση δύο διανυσμάτων με μήκος M/2 και τιμές τα επιλεγμένα στοιχεία του πραγματικού και φανταστικού μέρους από το μιγαδικό φάσμα $\Im[BX]$, ώστε να αποκτήσει περίπου την ίδια ενέργεια με την αρχική εικόνα X. Τέλος, η συνάρτηση H εκτελεί δύο λειτουργίες: κανονικοποιεί τα στοιχεία της Y, λαμβάνοντας υπόψιν την απόκλιση που παρουσιάζει το ιστόγραμμα των τιμών τους από μια ιδανική κανονική κατανομή και εκτελεί την δυαδικοποίηση αυτών βάσει των αντίστοιχων προσήμων τους.



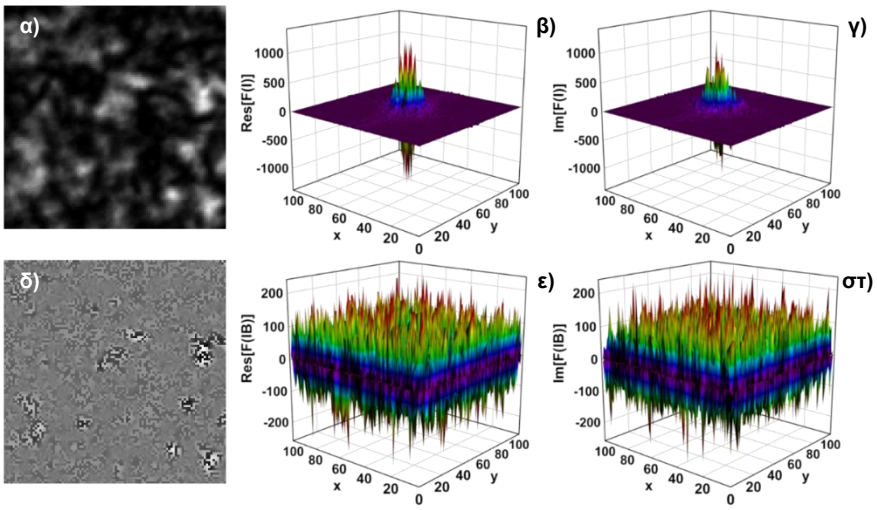
Σχήμα 3.8: α) Φωτογραφία της Βελουτέλας, μαζί με τα φάσματα του **β)** πλάτους και της **γ)** φάσης της, όπως προκύπτουν από την εφαρμογή του DFT σε αυτήν. **ε)** Εικόνα της Αλίκης, μαζί με τα φάσματα του **στ)** πλάτους και της **ζ)** φάσης της, όπως προκύπτουν από την εφαρμογή του DFT σε αυτήν. **δ)** Εφαρμογή του IDFT με το φάσμα πλάτους της Βελουτέλας και το φάσμα φάσης της Αλίκης. **η)** Εφαρμογή του IDFT με το φάσμα πλάτους της Αλίκης και το φάσμα φάσης της Βελουτέλας.

Αναλυτικότερα, η κανονικοποίηση της αναπαράστασης Y = S{$\Im[BX]$} λαμβάνει χώρα με την μετακίνηση όλων των στοιχείων αυτής κατά μία απόσταση d, η φορά της οποίας καθορίζεται από το πρόσημο της διάμεσης τιμής τους (median).

$$Y_i = \begin{cases} Y_i + |d| \ , \ \text{median} < 0 \\ Y_i - |d| \ , \ \text{median} > 0 \end{cases} \qquad (3.9)$$

Θα πρέπει να υπογραμμισθεί ότι η εν λόγω μετακίνηση πραγματοποιείται μόνο εάν ο συντελεστής ασυμμετρίας (skewness) της Y υπερβαίνει ένα προκαθορισμένο κατώφλι, η τιμή του οποίου εντοπίζεται εμπειρικά.

Από την άλλη πλευρά, η δυαδικοποίηση των τελικών τιμών της ακολουθίας εκτελείται ως εξής: τα θετικά στοιχεία αυτής λαμβάνουν την τιμή 1, τα αρνητικά στοιχεία της την τιμή 0, ενώ τα μηδενικά παραμένουν 0, όταν η προαναφερθείσα διάμεση τιμή τους είναι θετική. Στην αντίθετη περίπτωση μετατρέπονται σε μονάδες.



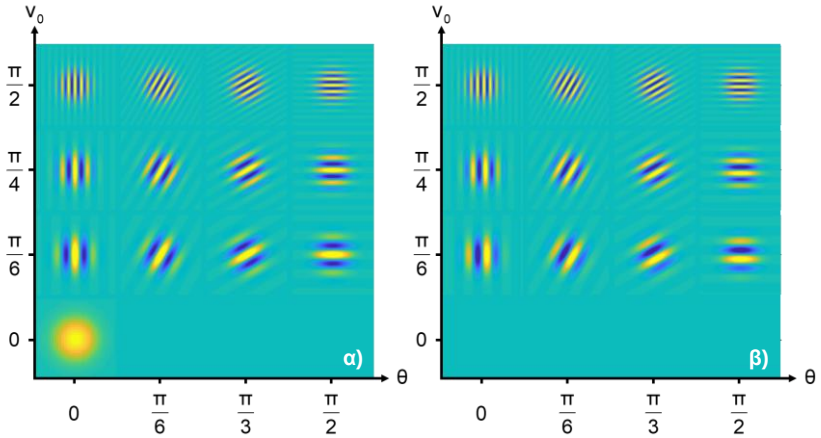
Σχήμα 3.9: α) Πειραματική εικόνα ενός speckle μαζί με το **β)** πραγματικό και το **γ)** φανταστικό μέρος του μετασχηματισμού Fourier της. **δ)** Το ίδιο speckle pattern μετά την ψευδοτυχαία διαμόρφωσή του μέσω του πίνακα B, μαζί με το **ε)** πραγματικό και **στ**) φανταστικό μέρος του μετασχηματισμού Fourier αυτού.

3.1.2.3.3.2 Gabor Binary Method (GBM)

Η δεύτερη βάση αραιής αναπαράστασης που επιλέχθηκε να χρησιμοποιηθεί για την εξαγωγή των ζητούμενων δυαδικών ακολουθιών είναι η δισδιάστατη συνάρτηση Gabor, η οποία ορίζεται ως το γινόμενο ενός επιπέδου κύματος με μια Gaussian συνάρτηση:

$$g(\vec{r}) = \exp\left[i\vec{v}\left(\vec{r}\cdot\vec{\kappa}\right)\right]\left\{\frac{1}{s\sqrt{2\pi}}\exp\left(-\frac{1}{4s^2}\left|\vec{r}-\vec{\kappa}\right|^2\right)\right\} \qquad (3.10)$$

όπου r = (x,y) είναι το διάνυσμα θέσεως ενός σημείου στο επίπεδο, κ = (κ_1,κ_2) οι συντεταγμένες της γκαουσιανής κορυφής σε αυτό, με s την τυπική απόκλισή της και v = v_0 (cosθ,sinθ) το κυματάνυσμα του επιπέδου κύματος. Ουσιαστικά, πρόκειται για ένα ζωνοπερατό φίλτρο σε δύο διαστάσεις, το χωρικό εύρος (scale) του οποίου καθορίζεται από την τυπική απόκλιση της Gaussian, ενώ η χωρική συχνότητά (spatial frequency) του και η κατεύθυνση αυτού (orientation) προσδιορίζεται από τον κυματάριθμο v_0 και την φάση του χρησιμοποιούμενου κυματανύσματος αντιστοίχως.



Σχήμα 3.10: α) Το πραγματικό και **β)** το φανταστικό μέρος της συνάρτησης Gabor, όπως αυτή διαμορφώνεται με την συστηματική μεταβολή της χωρικής συχνότητας και της κατεύθυνσή της.

Εν γένει, η χρήση των φίλτρων Gabor στο τομέα της επεξεργασίας εικόνας είναι ευρέως διαδεδομένη, καθώς οι ιδιότητες από τις οποίες χαρακτηρίζονται τα

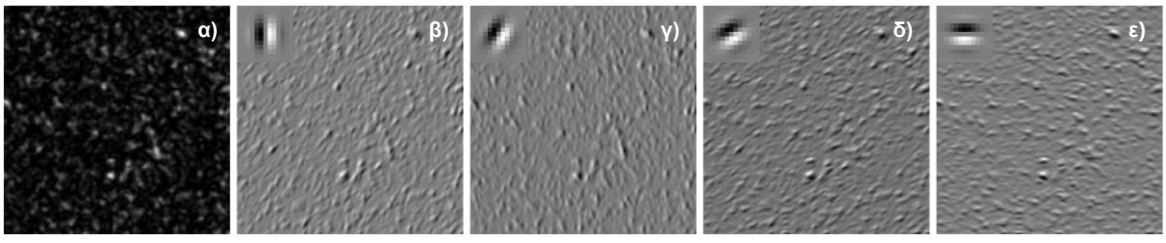
καθιστούν ιδανικά για την εξαγωγή των διαφόρων υφών που μπορεί να συνυπάρχουν σε μια φωτογραφία. Για παράδειγμα, ένα φίλτρο Gabor με κατάλληλα επιλεγμένη κατεύθυνση συντονίζεται στο φάσμα συχνοτήτων μιας υφής με παρόμοιο προσανατολισμό, παρουσιάζοντας μια ισχυρή απόκριση εν παρουσία της, η οποία επιτρέπει τον διαχωρισμό αυτής από υφές που περιέχουν το μεγαλύτερο μέρος της ισχύος τους σε άλλες περιοχές του φάσματος. [64]

Επί του πρακτέου τώρα, για τις ανάγκες της παρούσας εργασίας και την παραγωγή των ζητούμενων δυαδικών ακολουθιών επιλέχθηκε ως βάση αραιής αναπαράστασης των διαθέσιμων πειραματικών speckle patterns το φανταστικό μέρος μιας συστοιχίας φίλτρων Gabor με σταθερή χωρική συχνότητα v_0 αλλά μεταβαλλόμενη κατεύθυνση. Η εφαρμογή των φίλτρων αυτών οδηγεί σε ένα ισάριθμο σύνολο αποτελεσμάτων για κάθε εικόνα, τα οποία στη συνέχεια δειγματοληπτούνται ακολούθως: έκαστο φιλτραρισμένο αποτέλεσμα διαχωρίζεται σε μη επικαλυπτόμενα τμήματα ιδίων διαστάσεων με αυτές των εφαρμοζόμενων φίλτρων, από τα οποία επιλέγεται το κάτω δεξιά στοιχείο. Έπειτα, όλα τα επιλεχθέντα στοιχεία συγκεντρώνονται και διατάσσονται σε φθίνουσα σειρά εντός ενός μονοδιάστατου ανύσματος, από τα οποία εξάγονται τα Μ με την μεγαλύτερη τιμή, όπου Μ είναι το ζητούμενο μήκος της τελικής δυαδικής ακολουθίας. Τα Μ αυτά στοιχεία αντιστοιχούν και στις ισχυρότερες αποκρίσεις των εφαρμοζόμενων φίλτρων, αντιπροσωπεύοντας τα κυριότερα χαρακτηριστικά γνωρίσματα της υπό μελέτη εικόνας. Κατόπιν, για κάθε ένα από αυτά τα Μ στοιχεία κατασκευάζεται ένα καινούριο φίλτρο Gabor, με διαστάσεις πανομοιότυπες με αυτές της αρχικής εικόνας, κέντρο $\kappa = (\kappa_1,\kappa_2)$ της γκαουσιανής, το οποίο συμπίπτει με τις συντεταγμένες του εν λόγω στοιχείου στο επίπεδο και κατεύθυνση ίδια με αυτήν του φίλτρου από το οποίο προήλθε. Το φίλτρο αυτό στην συνέχεια μετατρέπεται σε στήλη, με το σύνολο όλων των στηλών που προκύπτουν από αυτήν τη διαδικασία να συνενώνεται σε έναν πίνακα, ο οποίος είναι και ο ζητούμενος πίνακας συμπιεστικής δειγματοληψίας Θ.

Συνεπώς, η τελική μορφή της παρούσας τεχνικής, η οποία θα αναφέρεται στο εξής ως GBM, μπορεί να συνοψιστεί από την εξίσωση [22]:

$$Y = H(\Theta X) \tag{3.11}$$

όπου το X αντιστοιχεί σε ένα speckle μετασχηματισμένο σε στήλη και κανονικοποιημένο σύμφωνα με την σχέση (3.8), το Y στη ζητούμενη δυαδική αναπαράσταση αυτού και το Η την συνάρτηση κανονικοποίησης και δυαδικοποίησης της προηγούμενης ενότητας.



Σχήμα 3.11: α) Πειραματική απόκριση 300×300 εικονοστοιχείων μαζί με τα αποτελέσματα φιλτραρίσματός της από μία τράπεζα φίλτρων Gabor διαστάσεων 50×50 pixels, scale = 1.5, v_0 = π/3 και προσανατολισμό **β)** θ = 0, **γ)** θ = π/6, **δ)** π/3 και **ε)** π/2 αντιστοίχως.

3.1.2.3.3.3 Singular Value Decomposition (SVD)

Η τρίτη τεχνική που επιλέχθηκε να χρησιμοποιηθεί για την παραγωγή των ζητούμενων δυαδικών ακολουθιών βασίζεται σε μια επέκταση της θεωρίας διαγωνοποίησης, η οποία ονομάζεται ανάλυση σε ιδιάζουσες τιμές (Singular Value

Decomposition). Σύμφωνα με τη θεωρία αυτή, οποιαδήποτε πραγματική μήτρα της μορφής $X \in \mathbb{R}^{N1\times N2}$ δύναται να εκφραστεί ως γινόμενο τριών πινάκων:

$$X = U\Sigma V^T \tag{3.12}$$

όπου $U \in \mathbb{R}^{N1\times N1}$, $\Sigma \in \mathbb{R}^{N1\times N2}$ και $V \in \mathbb{R}^{N2\times N2}$, με το V^T να συμβολίζει τον ανάστροφο του τελευταίου. Ειδικότερα, ο Σ είναι ένας ορθογώνιος διαγώνιος πίνακας, ο οποίος περιέχει τοποθετημένες σε φθίνουσα σειρά τις τετραγωνικές ρίζες των μη μηδενικών ιδιοτιμών $\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_{N2}$, όπως αυτές προκύπτουν για τον πίνακα X^TX. Οι ιδιοτιμές αυτές είναι και οι λεγόμενες ιδιάζουσες τιμές (Singular Values - SV) του πίνακα X, το σύνολο των οποίων είναι μοναδικό, αποτελώντας ένα ανεπανάληπτο και χαρακτηριστικό γνώρισμα της υπό μελέτη μήτρας.

$$\Sigma = \mathrm{diag}\left(\sigma_1,\sigma_2,\sigma_3,\ldots,\sigma_{N_2}\right) \text{ με } \sigma_1 \geq \sigma_2 \geq \sigma_3 \geq \ldots \geq \sigma_{N_2} \tag{3.13}$$

Αντίθετα, οι U, V είναι δύο τετραγωνικοί και μοναδιακοί πίνακες ($UU^T = VV^T = \hat{1}$) που μπορεί να προκύψουν αυτούσιοι για περισσότερες από μία μήτρες X, με τις στήλες τους να αντιστοιχούν σε ένα σύνολο από ορθοκανονικά ιδιοδιανύσματα, τα οποία εξάγονται από τους πίνακες XX^T και X^TX αντιστοίχως. Η διάταξη των ιδιοδιανυσμάτων αυτών, τα οποία αποκαλούνται αριστερά και δεξιά ιδιάζοντα διανύσματα του πίνακα X (Singular Components - SC), ακολουθεί την ίδια φθίνουσα σειρά των ιδιοτιμών από τις οποίες έχουν προέλθει.

Εν γένει η τάξη (rank) του πίνακα X ισούται με το πλήθος των ιδιάζουσων τιμών του. Εντούτοις στη πλειοψηφία των περιπτώσεων οι ευρεθείσες αυτές τιμές φθίνουν ραγδαία όσο η τάξη του πίνακα αυξάνεται, με τις ιδιοτιμές μικρότερου μεγέθους, οι οποίες συνήθως είναι πιο ευάλωτες σε θορυβικές αλλοιώσεις, να μπορούν να παραληφθούν. Το γεγονός αυτό πρακτικά υποδηλώνει ότι μία μήτρα X δύναται να αναπαρασταθεί ικανοποιητικά από ένα γινόμενο πινάκων U, Σ, V με μικρότερο μέγεθος από το προβλεπόμενο, οδηγώντας στην ταυτόχρονη συμπίεση και αποθορυβοποίησή αυτής. [65][66]

Εν προκειμένω, στο σχήμα που ακολουθεί επιδεικνύεται ένα παράδειγμα εφαρμογής της παραπάνω διαδικασίας σε μια ψηφιακή φωτογραφία ανάλυσης 512×512 pixels και τάξη πίνακα ίση με 512. Όπως λοιπόν φαίνεται και από τα αντίστοιχα αποτελέσματα, μια σχεδόν τέλεια αναπαράσταση της παρουσιαζόμενης εικόνας δύναται να επιτευχθεί χρησιμοποιώντας μόνο 200 εκ των ιδιάζουσων τιμών της, δηλαδή να ανακατασκευαστεί ικανοποιητικά μόνο με 244800 στοιχεία αντί των 262144 αρχικών.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι οι ιδιάζουσες τιμές μιας φωτογραφίας, εμπεριέχουν όλη την πληροφορία που χρειάζεται για την ανάκτηση της φωτεινότητά της, ενώ τα ιδιάζοντα διανύσματα αυτής όλες τις πληροφορίες για την πλήρη ανακατασκευή των γεωμετρικών χαρακτηριστικών της [66]. Με άλλα λόγια, η εξαγωγή των κυριότερων γνωρισμάτων μιας εικόνας επιτυγχάνεται από τα διανύσματα που προκύπτουν από τις ιδιάζουσες τιμές με το μεγαλύτερο μέγεθος.

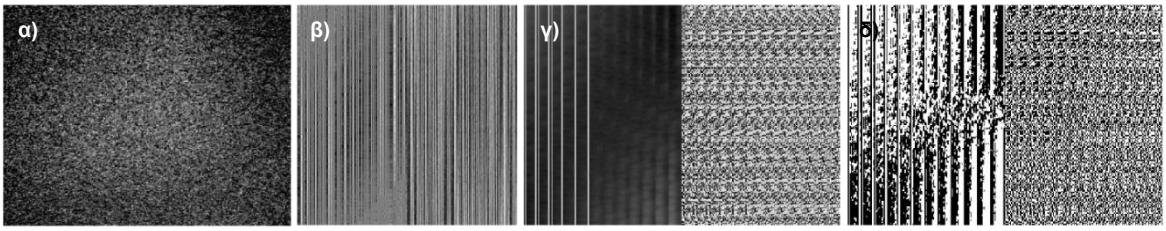
Υπό αυτό το πλαίσιο, ο αλγόριθμος που επιλέχθηκε να δοκιμαστεί για την μετατροπή των διαθέσιμων πειραματικών αποκρίσεων σε αντιπροσωπευτικές δυαδικές ακολουθίες είναι μια απλουστευμένη και τροποποιημένη εκδοχή της υλοποίησης που προτάθηκε από τον Kozat το 2004 [67] και ο οποίος περιλαμβάνει τα κάτωθι βήματα:

Σχήμα 3.12: α) Αρχική εικόνα ανάλυσης 512x512 pixels και τάξης ίση με 512. Ανακατασκευή της εικόνας χρησιμοποιώντας **β)** 5, **γ)** 10, **δ)** 20 **ε)** 50 και **στ)** 200 ιδιάζουσες τιμές.

Αρχικά, το πειραματικό speckle pattern, αφού κανονικοποιηθεί με χρήση της εξίσωσης (3.8) διαιρείται σε q_1 επικαλυπτόμενα τετραγωνικά τμήματα μεγέθους $k_1 \times k_1$. Σε κάθε ένα από αυτά εφαρμόζεται η προαναφερθείσα ανάλυση σε ιδιάζουσες τιμές, με τα αριστερά u και δεξιά ιδιοδιανύσματα v που αντιστοιχούν στην μεγαλύτερη ιδιάζουσα τιμή εκάστου τμήματος να συνενώνονται, προκειμένου να κατασκευαστεί μια ενδιάμεση εικόνα $\Gamma_1 = [u_1,u_2,\ldots,u_{q_1},v_1,v_2,\ldots,v_{q_1}]$. Εν συνεχεία, η ενδιάμεση αυτή εικόνα χωρίζεται σε ένα πλήθος q_2 αλληλεπικαλυπτόμενων τμημάτων με μέγεθος $k_2 \times k_2$, σε κάθε ένα από τα οποία εφαρμόζεται και πάλι η ανάλυση σε ιδιάζουσες τιμές. Κατόπιν, τα αριστερά και δεξιά ιδιάζοντα διανύσματα που προκύπτουν από τις μεγαλύτερες ιδιάζουσες τιμές εκάστου τμήματος συνενώνονται, οδηγώντας σε μια δεύτερη εικόνα $\Gamma_2 = [u_1,u_2,\ldots,u_{q_2},v_1,v_2,\ldots,v_{q_2}]$, τα στοιχεία της οποίας δυαδικοποιούνται βάσει της ακόλουθης σχέσης:

$$\Gamma_2(i,j) = \begin{cases} 1 \text{ εάν } \Gamma_2(i,j) \geq \Gamma_2(i,j+1) \\ 0 \text{ εάν } \Gamma_2(i,j) < \Gamma_2(i,j+1) \end{cases} \quad (3.14)$$

όπου το i συμβολίζει την σειρά στην οποία ανήκει το υπό μελέτη σημείο $\Gamma_2(i,j)$ ενώ το j την αντίστοιχη στήλη αυτού. Από την προκύπτουσα δυαδική εικόνα εν τέλει επιλέγονται M ψηφία με ψευδοτυχαίο τρόπο, τα οποία είναι και αυτά που αποτελούν την ζητούμενη δυαδική ακολουθία. Εν προκειμένω, στο σχήμα 3.13 παρουσιάζεται ένα πειραματικό speckle pattern μαζί με τις εικόνες Γ_1 και Γ_2 όπως προκύπτουν εφαρμόζοντας σε αυτό την άνωθεν περιγραφείσα διαδικασία.



Σχήμα 3.13: α) Απόκριση 650×850 εικονοστοιχείων μαζί με την **β)** ενδιάμεση εικόνα Γ_1 που προκύπτει από την εφαρμογή της πρώτης SVD, την **γ)** τελική εικόνα Γ_2 που προκύπτει από την εφαρμογή της δεύτερης SVD και **δ)** την δυαδικοποιημένη εκδοχή της Γ_2. Οι παράμετροι των SVD που εφαρμόστηκαν είναι $k_1 = 450$, $p = 225$ και $k_2 = 200$, $q = 144$ αντιστοίχως.

3.1.2.3.3.4 Negative Matrix Factorization (NMF)

Η τέταρτη και τελευταία τεχνική που χρησιμοποιήθηκε για την εξαγωγή των ζητούμενων ακολουθιών αντιστοιχεί σε μια εναλλακτική μέθοδο παραγοντοποίησης μητρών, μέσω της οποίας ένας πίνακας $X \in {}_{+}\mathbb{R}^{N1\times N2}$, με στοιχεία μεγαλύτερα ή ίσα του 0, αποπειράται να εκφραστεί προσεγγιστικά από το γινόμενο δύο επίσης θετικών πινάκων:

$$X \approx WH \tag{3.15}$$

όπου $W \in {}_{+}\mathbb{R}^{N1\times K}$ και $H \in {}_{+}\mathbb{R}^{K\times N2}$ αντιστοίχως, με τη τάξη τους K συνήθως να επιλέγεται έτσι ώστε να ισχύει η ανισότητα $K << \min(N_1,N_2)$. Με άλλα λόγια, πρόκειται για μια προσεγγιστική μέθοδο παραγοντοποίησης που ουσιαστικά λαμβάνει χώρα μέσω ενός ευρεστικού αλγόριθμου, ο οποίος αναζητά ένα ζεύγος κατάλληλων πινάκων W και H, με γινόμενο όσο το δυνατόν πιο κοντινό στον υπό μελέτη πίνακα X. Αυτό επιτυγχάνεται με την εισαγωγή μια συνάρτηση κόστους D(X-WH), η ελαχιστοποίηση της οποίας επιτρέπει την εύρεση των βέλτιστων δυνατών πινάκων, αποτιμώντας το σφάλμα των δοθέντων λύσεων.

Ειδικότερα, η συνάρτηση κόστους που επιλέχθηκε να χρησιμοποιηθεί αντιστοιχεί στην νόρμα Frobenious, η οποία ορίζεται ως η τετραγωνική ρίζα του αθροίσματος από τα τετράγωνα των στοιχείων ενός πίνακα, ενώ οι αναδρομικές σχέσεις ελαχιστοποίησής της δίνονται από τις εξισώσεις [68]:

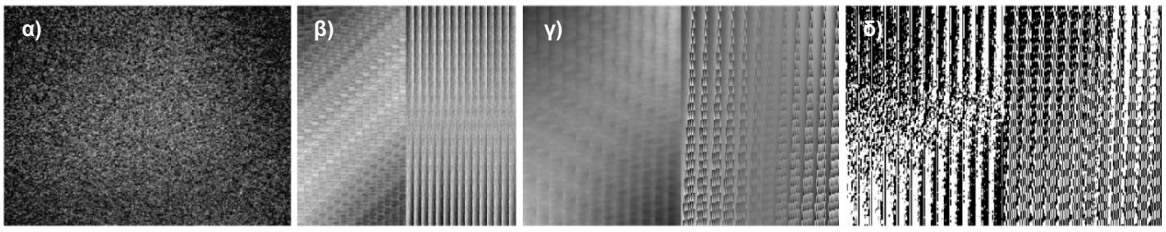
$$H = \frac{H \circ \left(W^{T}X\right)}{W^{T}WH + 10^{-9}} \tag{3.16}$$

$$W = \frac{W \circ \left(XH^{T}\right)}{WHH^{T} + 10^{-9}} \tag{3.17}$$

όπου ο επιπλέον όρος 10^{-9} προστίθεται και στους δύο παρονομαστές προκειμένου να αποφευχθεί μια ενδεχόμενη διαίρεση με την τιμή μηδέν. Σε αυτό το πλαίσιο, ο τελικός αλγόριθμος της εν λόγω τεχνικής, ο οποίος βασίστηκε στην υλοποίηση που προτάθηκε από τον Monga το 2007 [68], συνίσταται από τα ακόλουθα βήματα:

Αρχικά, το πειραματικό speckle pattern[5] διαιρείται σε q_1 επικαλυπτόμενα και τετραγωνικά τμήματα μεγέθους $k_1 \times k_1$. Σε κάθε ένα από αυτά εφαρμόζεται ο αλγόριθμος NMF, με τις πρώτες στήλες των ευρεθέντων πινάκων να κανονικοποιούνται βάσει της νόρμας Frobenious τους και να συνενώνονται, προκειμένου να κατασκευαστεί μια ενδιάμεση εικόνα $\Gamma_1 = [w_1,w_2,\ldots,w_{q_1}, h_1,h_2,\ldots,h_{q_1}]$. Εν συνεχεία, η ενδιάμεση αυτή εικόνα χωρίζεται σε ένα πλήθος q_2 επικαλυπτόμενων τμημάτων με μέγεθος $k_2 \times k_2$, σε κάθε ένα από τα οποία εφαρμόζεται και πάλι ο αλγόριθμος NMF. Κατόπιν, οι πρώτες στήλες των πινάκων εκάστου τμήματος κανονικοποιούνται και συνενώνονται ξανά, οδηγώντας σε μια δεύτερη εικόνα $\Gamma_2 = [w_1,w_2,\ldots,w_{q_2},h_1,h_2,\ldots,h_{q_2}]$, τα στοιχεία της οποίας δυαδικοποιούνται βάσει της εξίσωσης (3.14). Από την προκύπτουσα δυαδική εικόνα εν τέλει επιλέγονται M ψηφία με ψευδο-τυχαίο τρόπο, τα οποία είναι και αυτά που αποτελούν την ζητούμενη δυαδική ακολουθία. Στο ακόλουθο σχήμα παρουσιάζεται ένα πειραματικό speckle pattern μαζί με τις εικόνες Γ_1 και Γ_2 όπως προκύπτουν από αυτό εφαρμόζοντας την περιγραφείσα διαδικασία.

[5] Στην παρούσα τεχνική η χρησιμοποιούμενη εικόνα δεν κανονικοποιείται καθόλου, ώστε να πληροί τον περιορισμό των αρνητικών στοιχείων.



Σχήμα 3.14: α) Απόκριση 650×850 εικονοστοιχείων μαζί με την **β)** ενδιάμεση εικόνα Γ_1 που προκύπτει από την εφαρμογή της πρώτης NMF, την **γ)** τελική εικόνα Γ_2 που προκύπτει από την εφαρμογή της δεύτερης NMF και **δ)** την δυαδικοποιημένη εκδοχή της Γ_2. Οι παράμετροι των NMF που εφαρμόστηκαν είναι $k_1 = 450$, $p = 225$ και $k_2 = 200$, $q = 144$ αντιστοίχως.

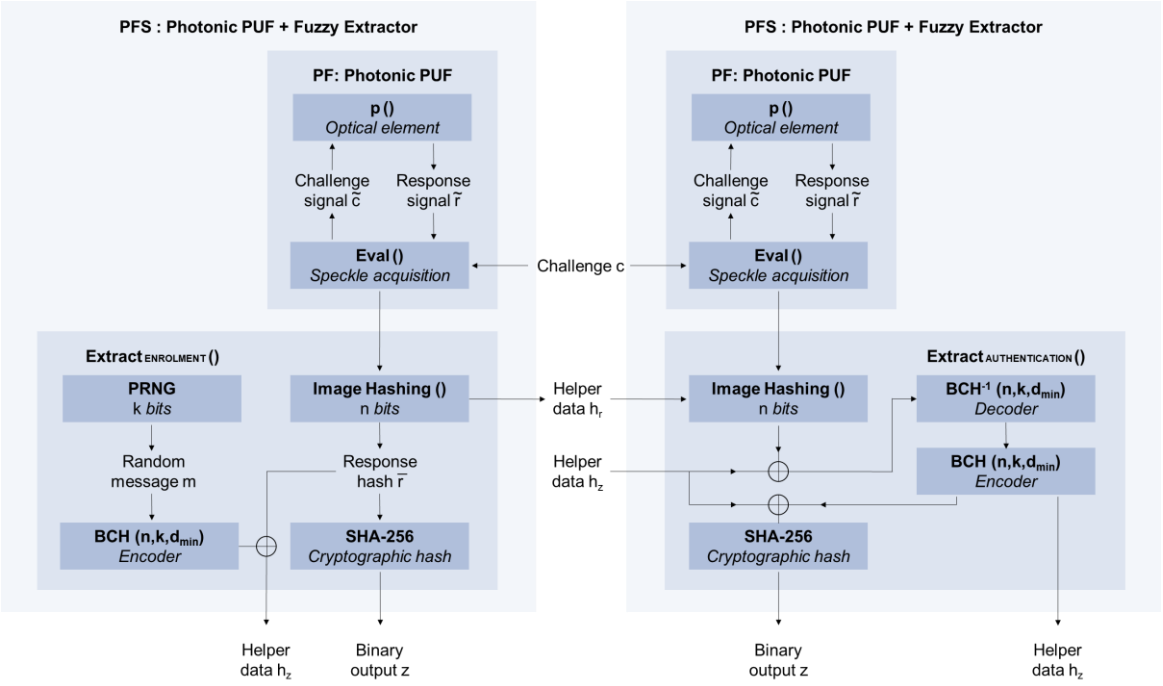
3.1.3 Τελική Υλοποίηση Διεργασίας Extract

Ανακεφαλαιώνοντας, η τελική υλοποίηση της διεργασίας Extract συνίσταται από τρεις κύριες διαδικασίες

- μια συνάρτηση κατακερματισμού εικόνων, μέσω της οποίας πραγματοποιείται η μετατροπή των πειραματικών αποκρίσεων σε δυαδικές ακολουθίες, οι οποίες πληρούν τις τρεις βασικές ιδιότητες μιας PUF (Image Hashing). Η διαδικασία αυτή ουσιαστικά αντιστοιχεί στην εφαρμογή των μεθόδων που αναφέρθηκαν στις ενότητες της παραγράφου 3.1.2.3, οι οποίες διενεργούν την ευθυγράμμιση, την ισοστάθμιση και την δυαδικοποίηση των χαρακτηριστικών γεωμετρικών γνωρισμάτων που εξάγονται από τα καταγραφέντα speckles.
- ένα code-offset secure scheme, το οποίο καθιστά εφικτή την ανακατασκευή των δυαδικών ακολουθιών που προκύπτουν από την προηγούμενη συνάρτηση εν ευθέτω χρόνω, αντιστοιχίζοντας κάθε μία από αυτές σε ένα μήνυμα, βάσει του οποίου διορθώνονται τα προκύπτοντα σφάλματα με χρήση του BCH code.
- και έναν εξαγωγέα τυχαιότητας (SHA-256) που κρυπτογραφεί τις διορθωμένες δυαδικές ακολουθίες, προάγοντας την συνολική ασφάλεια του συστήματος.

Οι τρεις αυτές διαδικασίες εκτελούνται στο πλαίσιο ενός fuzzy extractor, σε δύο στάδια, τα οποία παρουσιάζονται αναλυτικά στο σχήμα 3.15. Το πρώτο εξ αυτών είναι το στάδιο της εγγραφής, κατά το οποίο εφαρμόζεται για πρώτη φορά μια διέγερση c σε ένα οπτικό στοιχείο p και παράγεται η κρυπτογραφημένη δυαδική ακολουθία z της καταγραφείσας απόκρισής του με ένα σύνολο από βοηθητικά δεδομένα $h = \{h_r, h_z\}$. Το σκέλος h_r των βοηθητικών αυτών δεδομένων περιέχει όλες τις πληροφορίες που απαιτούνται για την ακριβή επανεφαρμογή της συνάρτησης κατακερματισμού εικόνων σε δεύτερο χρόνο, ενώ το σκέλος h_z αντιστοιχεί στην XOR της μη κρυπτογραφημένης δυαδικής ακολουθίας και του μηνύματος m που χρησιμοποιείται για την επικείμενη διόρθωση των λαθών κατά το επόμενο στάδιο. Το επόμενο και τελευταίο στάδιο είναι αυτό της αυθεντικοποίησης, όπου το οπτικό στοιχείο p διεγείρεται από το ίδιο challenge c ξανά και επιχειρείται η ανάκτηση της ακολουθίας z, με χρήση των βοηθητικών δεδομένων h.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι τα βοηθητικά δεδομένα h_r στην περίπτωση της τεχνικής RBM περιλαμβάνουν τους πίνακες U και S, ενώ στις τεχνικές SVD και NMF περιέχουν απλά τους ψευδοτυχαίους δείκτες θέσεως από τα ψηφία που απαρτίζουν τις τελικές δυαδικές ακολουθίες. Τέλος, τα βοηθητικά δεδομένα της GBM αντιστοιχούν στις συντεταγμένες των σημείων από τα οποία προέκυψαν οι ισχυρότερες αποκρίσεις των φίλτρων Gabor, μαζί με το αντίστοιχο αυτό φίλτρο.



Σχήμα 3.15: Το συνολικό πλαίσιο περιγραφής μιας PUF, στο οποίο έχει ενσωματωθεί η τελική υλοποίηση της διεργασίας Extract, όπως αυτή εκτελείται στα δύο στάδια ενός fuzzy extractor.

3.1.3.1 Μαθηματικός Ορισμός Robustness, Unpredictability, Unclonability

Υπό το γενικό πλαίσιο περιγραφής ενός συστήματος PUF, όπως αυτό διαμορφώνεται με την ολοκληρωμένη υλοποίηση της διεργασίας Extract και των δύο προαναφερθέντων σταδίων της (σχήμα 3.15), ο ορισμός της εξίσωσης (3.3) δύναται να επαναδιατυπωθεί υπό την μορφή τριών διαφορετικών πιθανοτήτων, οι οποίες αποτελούν την μαθηματική έκφραση των βασικών ιδιοτήτων μιας PUF [8][69].

Συγκεκριμένα, διατηρώντας σταθερές τις παραμέτρους α_{PF} και α_{EX} των διεργασιών Eval και Extract, οι οποίες αντιπροσωπεύουν τις χρησιμοποιούμενες ρυθμίσεις της κάμερας και του κώδικα BCH αντιστοίχως, προκύπτουν οι ακόλουθοι ορισμοί, για τους οποίους ισχύουν οι σχέσεις $h = \{h_r, h_z\}$ και ε = empty σε κάθε περίπτωση.

Το robustness ενός PFS ορίζεται ως η πιθανότητα του να προκύψει μια πανομοιότυπη δυαδική έξοδος z και από τα δύο στάδια του fuzzy extractor, όταν στο ίδιο αντικείμενο p εφαρμόζεται μια μοναδική διέγερση c

$$\text{Robustness} = \Pr\left[\text{PFS}_p(c,h) \to (z,h) : \text{PFS}_p(c,\varepsilon) \to (z,h)\right] \qquad (3.18)$$

Ομοίως, το unpredictability ενός PFS είναι η πιθανότητα να προκύψει η ίδια έξοδος z από αποκρίσεις που παράγονται με την εφαρμογή δύο διαφορετικών διεγέρσεων c και c′ σε ένα p, χρησιμοποιώντας για την αυθεντικοποίηση της δεύτερης τα βοηθητικά δεδομένα h που δημιουργήθηκαν κατά την εγγραφή της πρώτης.

$$\text{Unpredictability} = \left[\text{PFS}_p(c',h) \to (z,h) : \text{PFS}_p(c,\varepsilon) \to (z,h)\right] \qquad (3.19)$$

Τέλος, ως unclonability ενός PFS ορίζεται η πιθανότητα να προκύψει μια πανομοιότυπη δυαδική έξοδος z από αποκρίσεις που παράγονται με την εφαρμογή μιας διέγερσης c σε δύο διαφορετικά αντικείμενα p και p′, χρησιμοποιώντας τα βοηθητικά δεδομένα h που παράχθηκαν κατά την εγγραφή του p για την αυθεντικοποίηση του p′:

$$\text{Unclonability} = \left[\text{PFS}_{p'}(c,h) \to (z,h) : \text{PFS}_p(c,\varepsilon) \to (z,h)\right] \qquad (3.20)$$

3.2 Ανάλυση Δεδομένων

Όπως έχει ήδη αναφερθεί στις προηγούμενες παραγράφους, η παρούσα διδακτορική διατριβή εστιάζει στην διερεύνηση των τριών κύριων ιδιοτήτων μιας PUF˙ το robustness, το unpredictability και το unclonability. Για τις ανάγκες λοιπόν της εν λόγω διερεύνησης, διεξήχθη μια σειρά κατάλληλων πειραμάτων, προκειμένου να παραχθούν τα δεδομένα που απαιτούνται για την ποσοτικοποίηση εκάστης ιδιότητας σύμφωνα με τις εξισώσεις (3.18), (3.19) και (3.20). Τα δεδομένα αυτά μπορούν να ταξινομηθούν σε 3 αντίστοιχες κατηγορίες.

- Δεδομένα robustness: πρόκειται για speckle patterns που καταγράφονται κάτω από πανομοιότυπες πειραματικές συνθήκες, υπό την επαναληπτική εφαρμογή ενός μόνο challenge c στο ίδιο οπτικό μέσο p .
- Δεδομένα unpredictability: speckles που προέρχονται από την εφαρμογή όλων των διαθέσιμων διεγέρσεων c στο ίδιο ανομοιογενές μέσο p, διατηρώντας όλες τις υπόλοιπες πειραματικές συνθήκες σταθερές.
- Δεδομένα unclonability: speckle patterns, τα οποία λαμβάνονται εφαρμόζοντας μια μόνο διέγερση c σε ένα σύνολο από διαφορετικά ανομοιογενή υλικά μέσα p, διατηρώντας όλες τις υπόλοιπες πειραματικές συνθήκες σταθερές.

Εν συνεχεία δοκιμάστηκαν διάφορες μετρικές και μέθοδοι ώστε να καταστεί εφικτή η συγκριτική αξιολόγηση των παραγόμενων μετρήσεων σε δύο διαφορετικά επίπεδα: στο επίπεδο των πειραματικών εικόνων και στο επίπεδο των δυαδικών ακολουθιών. Από τις μετρικές και μεθόδους που δοκιμάστηκαν επιλέχθηκαν:

- η Ευκλείδεια απόσταση και ο συντελεστής διασυσχέτισης Pearson για την ποσοτικοποίηση της ομοιότητας μεταξύ των πειραματικών speckle patterns
- η απόσταση Hamming για την ποσοτικοποίηση της ομοιότητας μεταξύ των εξαγόμενων δυαδικών ακολουθιών.
- και το λογισμικό πακέτο ελέγχων του NIST για την αξιολόγηση της τυχαιότητας των εξαγόμενων δυαδικών ακολουθιών.

Στο σημείο αυτό κρίνεται σκόπιμο να αναφερθεί ότι τα αποτελέσματα που προκύπτουν από τη σύγκριση δεδομένων που αφορούν μετρήσεις robustness απαντώνται συνήθως στη βιβλιογραφία ως intra - class αποτελέσματα, ενώ οι συγκρίσεις μεταξύ δεδομένων, τα οποία έχουν ληφθεί για την ποσοτικοποίηση του unpredictability (ή του unclonability) οδηγούν στα λεγόμενα inter - class αποτελέσματα αντιστοίχως.

Στις επόμενες ενότητες του παρόντος κεφαλαίου λοιπόν παρουσιάζονται εν συντομία τα μαθηματικά εργαλεία που χρησιμοποιήθηκαν για τη στατιστική ανάλυση, την περιγραφή και την ερμηνεία των διαθέσιμων πειραματικών αποτελεσμάτων.

3.2.1 Μετρικές Αξιολόγησης

3.2.1.1 Ευκλείδεια Απόσταση

Η Ευκλείδεια απόσταση (Euclidean Distance) d_E εκφράζει την γεωμετρική απόσταση μεταξύ δύο διανυσμάτων, $X = \{x_1,x_2,\ldots,x_n\}$ και $Y = \{y_1,y_2,\ldots,y_n\}$, τα οποία είναι ορισμένα στον n-διάστατο Ευκλείδειο χώρο $\mathbb{R}^n$

$$d_E(X,Y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \tag{3.21}$$

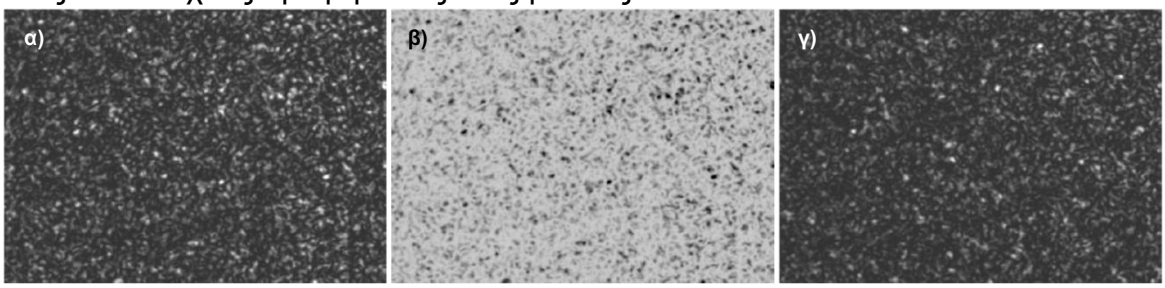
Σε επίπεδο εικόνων, όπου οι όροι x_i, y_i του άνωθεν αθροίσματος αντιπροσωπεύουν τις τιμές εντάσεως των εικονοστοιχείων τους και το σύμβολο n αντιστοιχεί στον συνολικό αριθμό αυτών, το μέγεθος της Ευκλείδειας απόστασης επηρεάζεται σημαντικά από το χρωματικό βάθος και την ανάλυση των υπό μελέτη φωτογραφιών. Το γεγονός αυτό καθιστά την Ευκλείδεια απόσταση λιγότερο πρακτική όσον αφορά την σύγκριση ετερογενών αποτελεσμάτων που προκύπτουν από αποκρίσεις οι οποίες έχουν καταγραφεί με τις εν λόγω παραμέτρους διαφορετικές.

3.2.1.2 Συντελεστής Διασυσχέτισης Pearson

Ο συντελεστής διασυσχέτισης ρ αποτελεί μία στατιστική μετρική, η οποία εκφράζει τον βαθμό γραμμικής συνδιακύμανσης δύο ή περισσότερων μεταβλητών. Για δύο σύνολα δεδομένων $X = \{x_1,x_2,\ldots,x_n\}$, $Y = \{y_1,y_2,\ldots,y_n\}$ δίνεται από την σχέση:

$$\rho(X,Y) = \frac{\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{n}(y_i-\bar{y})^2}} \qquad (3.22)$$

όπου τα x_i, y_i συμβολίζουν τις i-οστές παρατηρήσεις εκάστου συνόλου και τα $\bar{x}$, $\bar{y}$ τους αντιστοίχους αριθμητικούς τους μέσους.



Σχήμα 3.16: α,γ) Πειραματικά speckle patterns που λήφθηκαν με την ίδια διάταξη αλλά υπό διαφορετικές συνθήκες ακτινοβόλησης. **β)** Αρνητικό αντίστοιχο του πρώτου εκ των δύο speckles, το οποίο παράχθηκε υπολογιστικά αντιστρέφοντας τις τιμές των καταγεγραμμένων διαβαθμίσεων του γκρι. Οι συντελεστές διασυσχέτισης των εικονιζόμενων φωτογραφιών είναι ρ(α,α) = +1, ρ(α,β) = -1, ρ(α,γ) = 0.385 και ρ(β,γ) = -0.385 αντιστοίχως.

Γενικά, ο συντελεστής διασυσχέτισης ρ ορίζεται στο διάστημα [-1,1], με το πρόσημό του να υποδηλώνει την κατεύθυνση της συνδιακύμανσης. Με άλλα λόγια, σύνολα με ρ > 0 παρουσιάζουν μια ομόρροπη συμμεταβολή των στοιχείων τους, όπου το 1 σηματοδοτεί την πλήρη και θετική γραμμική τους συσχέτιση. Αντιθέτως, μεταβλητές με ρ < 0 εμφανίζουν αντίρροπη συνδιακύμανση στοιχείων, όπου το -1 σημαίνει μια τέλεια αντιστρόφως ανάλογη σχέση. Τέλος, συντελεστές πλησίον του 0 υποδεικνύουν μια ασθενέστερη γραμμική εξάρτηση, η οποία εξαλείφεται πλήρως για την τιμή ρ = 0.

Υπό αυτό το πλαίσιο, θεωρώντας ότι τα σύνολα X,Y της άνωθεν εξίσωσης αντιστοιχούν σε ένα ζεύγος από πειραματικά στιγμιότυπα που έχουν ληφθεί με μια κοινή ανάλυση n pixels, ο συντελεστής διασυσχέτισης ρ δύναται να χρησιμοποιηθεί για την ποσοτική περιγραφή των μορφολογικών διαφοροποιήσεων τους. Στο σχήμα 3.16 παρουσιάζονται τρία τέτοια παραδείγματα εικόνων, συνοδευόμενα από τις προκύπτουσες τιμές του ρ τους.

Όπως είναι λοιπόν αναμενόμενο, ο ρ δύο ακριβώς ίδιων εικόνων προκύπτει ίσος με 1, ενώ φωτογραφίες με πανομοιότυπα γεωμετρικά χαρακτηριστικά αλλά αντίστροφες τιμές εντάσεων οδηγούν στην τιμή -1. Από την άλλη πλευρά, εικόνες με ανόμοια μορφολογική δομή αντιστοιχούν σε μειωμένες τιμές του συντελεστή ρ,

ο οποίος μάλιστα μηδενίζεται όταν η χωρική κατανομή της έντασής τους είναι τελείως ανόμοια.

3.2.1.3 Απόσταση Hamming

Η απόσταση Hamming d_H μεταξύ δύο δυαδικών ακολουθιών $X = \{x_1,x_2,\ldots,x_n\} \in \{0,1\}^n$ και $Y = \{y_1,y_2,\ldots,y_n\} \in \{0,1\}^n$ ορίζεται ως ο αριθμός των θέσεων στις οποίες τα ψηφία των ακολουθιών αυτών διαφέρουν. Με άλλα λόγια η απόσταση Hamming καταμετρά το ελάχιστο πλήθος αντικαταστάσεων που πρέπει να πραγματοποιηθούν προκειμένου η μία ακολουθία να μετατραπεί στην άλλη.

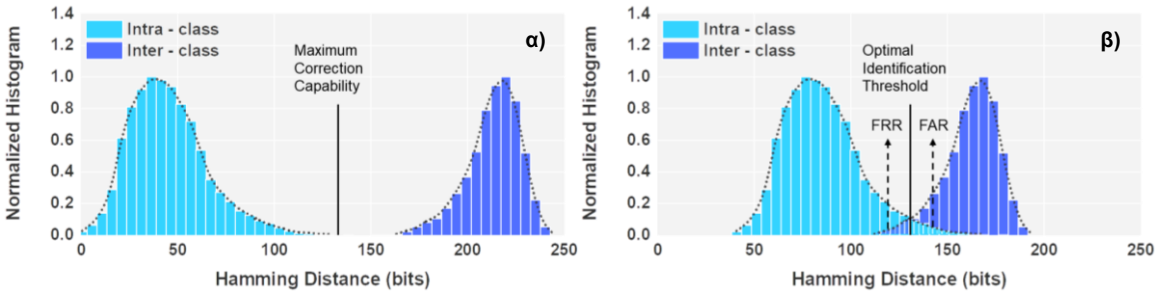
$$d_H(X,Y) = \sum_{i=1}^{n} x_i \oplus y_i \tag{3.23}$$

Εν γένει, η απόσταση Hamming αποτελεί ίσως τη σημαντικότερη μετρική της παρούσας εργασίας, καθώς η χρήση της προσφέρει μια ολοκληρωμένη εικόνα της απόδοσης που παρουσιάζει το εκάστοτε σύστημα PUF σε επίπεδο εφαρμογής. Ειδικότερα, καθορίζει τις τιμές που πρέπει να λάβουν οι παράμετροι του κώδικα BCH, ώστε η αποκατάσταση των σφαλμάτων να είναι επιτυχής, καταδεικνύει το ενδεχόμενο ύπαρξης ψευδώς θετικής ή αρνητικής αυθεντικοποίησης, ενώ παρέχει μια αξιόπιστη αλλά ταχεία εκτίμηση των πιθανοτήτων (3.18) - (3.20).

3.2.2 Εφαρμογή Μετρικών Αξιολόγησης

Η πλέον διαδεδομένη μεθοδολογία που ακολουθείται για την προκαταρκτική αξιολόγηση της επίδοσης που παρουσιάζει οποιοδήποτε σύστημα PUF είναι η γραφική απεικόνιση των αποτελεσμάτων από τις παραπάνω μετρικές, υπό την μορφή κανονικοποιημένων ιστογραμμάτων. Τα εν λόγω ιστογράμματα συνήθως αναπαρίστανται σε ζεύγη, intra και inter - class κατανομών, προκειμένου να διερευνηθεί η ύπαρξη αλληλοεπικάλυψης τους, η οποία εν γένει θεωρείται ανεπιθύμητη, αφού η παρουσία της κατά κανόνα υποδηλώνει το ενδεχόμενο ψευδώς θετικών ή αρνητικών αυθεντικοποιήσεων.

Στο πλαίσιο της τρέχουσας υποενότητας λοιπόν παρουσιάζεται εν συντομία η εφαρμογή της αναφερθείσας μεθοδολογίας, εστιάζοντας αποκλειστικά στην ανάλυση, την εξαγωγή και την ερμηνεία συμπερασμάτων από τις παραγόμενες κατανομές της απόστασης Hamming η οποία, όπως έχει ήδη αναφερθεί, αποτελεί και την σημαντικότερη μετρική της παρούσας εργασίας. Εν προκειμένω, στο σχήμα 3.17 επιδεικνύονται δύο ενδεικτικά παραδείγματα από ζεύγη ιστογραμμάτων Hamming, εκ των οποίων οι κατανομές intra - class προέρχονται από δεδομένα robustness, ενώ οι κατανομές inter - class από δεδομένα unpredictability (ή unclonability). Θα πρέπει επιπλέον να σημειωθεί ότι τα εν λόγω ιστογράμματα αντιστοιχούν σε αποτελέσματα συγκρίσεων μεταξύ ακολουθιών με μήκος n = 511 bits.



Σχήμα 3.17: Ζεύγη intra - class και inter - class ιστογραμμάτων από αποστάσεις Hamming **α)** με απουσία επικάλυψης, η οποία αποτελεί την ιδανική συνθήκη λειτουργίας ενός συστήματος PUF και

β) με παρουσία επικάλυψης, η οποία εν γένει θεωρείται ανεπιθύμητη, καθώς η ύπαρξη της υποδηλώνει το ενδεχόμενο ψευδώς θετικών ή αρνητικών αυθεντικοποιήσεων.

Στο σημείο αυτό κρίνεται σκόπιμο επίσης να διασαφηνιστεί ότι οι κατανομές τύπου intra - class ουσιαστικά αντικατοπτρίζουν τις διαφοροποιήσεις των δυαδικών ακολουθιών που προκαλούνται από τον θόρυβο παρατήρησης, ο οποίος υπεισέρχεται στις καταγραφόμενες αποκρίσεις κατά την διεξαγωγή της πειραματικής διαδικασίας. Για ένα ιδανικό σύστημα PUF με μηδενικό θόρυβο, οι διαφοροποιήσεις αυτές προφανώς δεν υφίστανται και όλες οι αποστάσεις Hamming ισούνται με το μηδέν· σε αυτή την περίπτωση, η εφαρμογή του fuzzy extractor καθίσταται περιττή και η ύπαρξη του BCH τελείως ανούσια. Υπό πραγματικές συνθήκες, όμως, όπου το σύστημα αποκλίνει από το ιδεατό, όσο ο θόρυβος αυτού αυξάνει και οι προκαλούμενες διαφοροποιήσεις των δυαδικών ακολουθιών ενισχύονται, τόσο η διασπορά των κατανομών intra - class διευρύνεται και η μέγιστη τιμή τους απομακρύνεται από το μηδέν. Οι εν λόγω διαφοροποιήσεις λοιπόν είναι και αυτές που πρέπει να διορθωθούν μέσω του χρησιμοποιούμενου κώδικα BCH, ούτως ώστε να εξασφαλιστεί και η ζητούμενη επαναληψιμότητα του συστήματος. Από την άλλη πλευρά, οι κατανομές τύπου inter - class αναπαριστούν τις διαφοροποιήσεις που προκαλούνται είτε από την μεταβολή της εφαρμοζόμενης διέγερσης είτε από την αντικατάσταση του υπό μελέτη φυσικού αντικειμένου. Οι διαφοροποιήσεις αυτές είναι ίσες με το 50% των υπό μελέτη δυαδικών ακολουθιών για ένα ιδανικό σύστημα PUF, δηλαδή 255 bits για το θεωρούμενο μήκος n = 511 bits του σχήματος 3.17. Εντούτοις, στην πραγματικότητα οι διαφοροποιήσεις αυτές εμπεριέχουν πάντοτε και την συνεισφορά του προαναφερθέντος μετρητικού θορύβου, γεγονός που υποδηλώνει ότι η πειραματική καταστολή, αλλά και η υπολογιστική διόρθωση των σφαλμάτων που αυτός επιφέρει, οδηγεί τελικά στην υποβάθμιση της ασφάλειας του συστήματος, καθιστώντας τις δυαδικές εξόδους πολύ πιο προβλέψιμες.

Βάσει των ανωτέρω λοιπόν γίνεται φανερό ότι μέσω των ιστογραμμάτων τύπου intra - class αρχικά καθίσταται εφικτή μια προκαταρτική εκτίμηση της ελάχιστης διορθωτικής ικανότητας t του κώδικα BCH(n,k,d_{min}) που πρέπει να χρησιμοποιηθεί, έτσι ώστε να διασφαλιστεί η ζητούμενη αναπαραγωγιμότητα των εξαγόμενων δυαδικών ακολουθιών. Συγκεκριμένα, η ελάχιστη αυτή διορθωτική ικανότητα εντοπίζεται στο άνω άκρο των εν λόγω ιστογραμμάτων, το οποίο αντιπροσωπεύει και το μέγιστο πλήθος σφαλμάτων προς διόρθωση. Ταυτόχρονα, εάν στην ίδια γραφική παράσταση συμπεριληφθούν και οι αντίστοιχες κατανομές τύπου inter - class μπορεί επιπλέον να εκτιμηθεί και η μέγιστη διορθωτική ικανότητα του BCH που επιτρέπεται να χρησιμοποιηθεί, προτού αυτός αρχίσει να διορθώνει και ακολουθίες οι οποίες αντιστοιχούν σε άλλα δείγματα ή challenges. Αυτή η μέγιστη διορθωτική ικανότητα λοιπόν μπορεί να προσδιοριστεί με την σειρά της από το κάτω άκρο των κατανομών inter - class.

Επιστρέφοντας τώρα στο σχήμα 3.17α, υπό ευνοϊκές συνθήκες, το άνω άκρο του ιστογράμματος intra - class και το κάτω άκρο του ιστογράμματος inter - class θα πρέπει να απέχουν προκειμένου να υπάρχει ένα λειτουργικό εύρος διορθωτικών ικανοτήτων για τον κώδικα BCH. Στην αντίθετη περίπτωση όμως όπου οι δύο κατανομές Hamming αλληλεπικαλύπτονται, το λειτουργικό αυτό εύρος παύει να υφίσταται και οποιαδήποτε ικανότητα t οδηγεί αναπόφευκτα σε εσφαλμένες διορθώσεις, είτε προς τη μία είτε προς την άλλη κατεύθυνση (σχήμα 3.17β). Με άλλα λόγια, η παρουσία της εν λόγω αλληλεπικάλυψης υποδηλώνει ότι ακολουθίες από ένα φυσικό αντικείμενο θα αναγνωρίζονται εσφαλμένα ως ακολουθίες ενός άλλου αντικειμένου ή challenge του συστήματος (False Rejection) και αντίθετα οι

ακολουθίες ενός διαφορετικού δείγματος ή challenge θα αντιστοιχίζονται λανθασμένα στο αρχικό αντικείμενο αναφοράς (False Acceptance).

Όπως γίνεται λοιπόν φανερό από τα παραπάνω, η ύπαρξη αλληλοεπικάλυψης μεταξύ των κατανομών intra - class και inter - class εν γένει εκλαμβάνεται ως πλήρως ανεπιθύμητη στο πλαίσιο της παρούσας εργασίας. Εντούτοις, αξίζει να σημειωθεί ότι αναλόγως της στοχευόμενης χρήσης και εφαρμογής, μια PUF μπορεί να θεωρηθεί πλήρως εκμεταλλεύσιμη ακόμη και υπό αυτές τις συνθήκες λειτουργίας, αρκεί η διορθωτική ικανότητα t του κώδικα BCH να οριστεί καταλλήλως. Ειδικότερα για την περίπτωση όπου στα δύο ιστογράμματα υπάρχει αλληλοεπικάλυψη, η επιλογή της βέλτιστης διορθωτικής ικανότητας του BCH (Optimal Identification Threshold) λαμβάνει χώρα υπολογίζοντας το σημείο τομής των περιβαλλουσών των δύο ιστογραμμάτων [70].

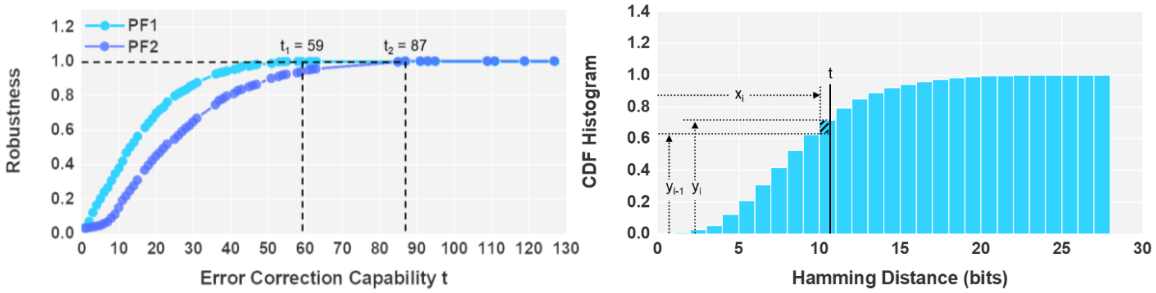
Εν κατακλείδι, η γραφική απεικόνιση των αποστάσεων Hamming σε ζεύγη κατανομών επιτρέπει μια ταχεία αξιολόγηση της απόδοσης που παρουσιάζει το εκάστοτε σύστημα PUF, παρέχοντας πληροφορίες τόσο για τις παραμέτρους του κώδικα BCH που πρέπει να χρησιμοποιηθούν, ώστε η αποκατάσταση των σφαλμάτων να είναι επιτυχημένη, όσο και για το ενδεχόμενο ύπαρξης ψευδώς θετικής ή ψευδώς αρνητικής αυθεντικοποίησης. Ωστόσο, ο ακριβής καθορισμός των προαναφερθέντων παραμέτρων απαιτεί κάποια επιπλέον βήματα υπολογισμών, τα οποία ουσιαστικά αντιστοιχούν στον προσδιορισμό των πιθανοτήτων (3.18), (3.19) και (3.20), χρησιμοποιώντας δύο εναλλακτικές αλλά συμπληρωματικές μεθοδολογίες.

Ειδικότερα, έχοντας ορίσει ένα δεδομένο πλήθος ψηφίων n για τις εξαγόμενες δυαδικές ακολουθίες, το μήκος k των αντίστοιχων μηνυμάτων τους, όπως αυτά κατασκευάζονται με ανεξάρτητο τρόπο κατά το στάδιο της εγγραφής, θα πρέπει να ανήκει σε ένα σύνολο συγκεκριμένων ακεραίων [6], με $k < n$. Όσο λοιπόν το εν λόγω μήκος k ελαττώνεται, τόσο η διορθωτική ικανότητα t του κώδικα BCH ενισχύεται και οι πιθανότητες (3.18) - (3.20) αυξάνονται. Συνεπώς, υπολογίζοντας την πιθανότητα του robustness για κάθε πιθανό t, δύναται να εντοπιστούν όλοι οι κώδικες BCH(n,k,d_{min}) που επιτυγχάνουν την σίγουρη αποκατάσταση των υπεισερχόμενων λαθών. Εξ αυτών των κωδίκων μάλιστα, βέλτιστος θεωρείται ο BCH(n,k,d_{min}) ο οποίος, με την ελάχιστη δυνατή διορθωτική ικανότητα t, είναι σε θέση να επιδείξει πιθανότητα (3.18) ίση με τη μονάδα (σχήμα 3.18α), κάτι που υποδηλώνει την διασφαλισμένη επαληψιμότητα των δυαδικών ακολουθιών. Παράλληλα όμως, λόγω της ελάχιστης αυτής ικανότητας t, η συνολική ασφάλεια του συστήματος δεν διακυβεύεται περισσότερο απ' όσο είναι απολύτως απαραίτητο, αφού οι αντίστοιχες πιθανότητες του unpredictability (3.19) και του unclonability (3.20) συγκρατούνται στο ελάχιστο δυνατό επίπεδο.

Σε αυτό το πλαίσιο λοιπόν, οι ζητούμενες πιθανότητες (3.18), (3.19) και (3.20) δύναται να προσδιοριστούν με δύο διαφορετικές αλλά αλληλοσυμπληρούμενες μεθοδολογίες, εκ των οποίων η πρώτη είναι μια προσεγγιστική μέθοδος υπολογισμού η οποία λαμβάνει χώρα χρησιμοποιώντας την αθροιστική συνάρτηση κατανομής (Cumulative Distribution Function - CDF) των αποστάσεων Hamming [22]. Η προσεγγιστική αυτή μεθοδολογία ουσιωδώς συνοψίζεται από τη σχέση $\Pr[d_H \leq t] = y_{i-1} + (y_{i-1} - y_i)(t - x_i)$, όπου η έκφραση $\Pr[d_H \leq t]$ συμβολίζει την τιμή της ζητούμενης πιθανότητας και το t την διορθωτική ικανότητα t του

[6] Δεν υπάρχει αναλυτικός τύπος που να μπορεί να περιγράψει με απόλυτο τρόπο την συσχέτιση μεταξύ του μήκους k, του μήκους n και της ικανότητας t ενός κώδικα BCH.

χρησιμοποιούμενου BCH. Τέλος, οι παράμετροι x_i, y_i αντιστοιχούν στην τετμημένη και την τεταγμένη τιμή του bin εντός του οποίου εμπίπτει η μελετούμενη διορθωτική ικανότητα t (σχήμα 3.18β).



Σχήμα 3.18: α) Ενδεικτική απεικόνιση της πιθανότητας (3.18) για δύο διαφορετικά συστήματα PUF, PF1 και PF2, ως συνάρτηση της διορθωτικής ικανότητας t όλων των κωδίκων BCH(n, k, d_{min}) που μπορούν να εφαρμοστούν σε ακολουθίες μήκους n = 511 bits. Η ελάχιστη διορθωτική ικανότητα που απαιτείται για την σταθεροποίηση της πιθανότητας αυτής στη μονάδα ανέρχεται σε 59 bits για το PF1 και 87 bits για το PF2 αντιστοίχως, υποδηλώνοντας την μεγαλύτερη σταθερότητα του πρώτου απέναντι στον περιβαλλοντικό θόρυβο. **β)** Προσεγγιστική αποτίμηση της πιθανότητας να προκύψουν πανομοιότυποι έξοδοι και από τα 2 στάδια του fuzzy extractor, χρησιμοποιώντας την CDF των αποστάσεων Hamming.

Στο σημείο αυτό θα πρέπει να υπογραμμιστεί ότι η προσεγγιστική αυτή μεθοδολογία περιορίζεται αυστηρά από τις προκύπτουσες τιμές των αποστάσεων Hamming και δεν λαμβάνει καθόλου υπόψιν ότι μια δυαδική ακολουθία με περισσότερα λάθη από την χρησιμοποιούμενη ικανότητα t του εκάστοτε BCH μπορεί να οδηγήσει τυχαία σε ένα έγκυρο κωδικοποιημένο μήνυμα και συνεπώς να διορθωθεί εσφαλμένα. Επομένως, τα αποτελέσματα της παρουσιαζόμενης προσέγγισης εν γένει προκύπτουν ελαφρώς υποεκτιμημένα σε σχέση με τις πραγματικές τιμές των πιθανοτήτων του συστήματος, οι οποίες προσδιορίζονται από τη δεύτερη αναφερθείσα μέθοδο υπολογισμού, που δεν είναι άλλη από την απλή καταμέτρηση των πανομοιότυπων εξόδων που προκύπτουν και από τα δύο στάδια του fuzzy extractor.

3.2.3 NIST Statistical Test Suite

Το NIST Statistical Test Suite αποτελεί ένα λογισμικό πακέτο 15 ελέγχων (tests), το οποίο αναπτύχθηκε από το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας των Η.Π.Α το 1999 με σκοπό την αξιολόγηση μηχανισμών που γεννούν τυχαίους ή ψευδοτυχαίους αριθμούς. Ουσιαστικά πρόκειται για την εξέταση διαφόρων στατιστικών ιδιοτήτων μιας δυαδικής ακολουθίας, ώστε να εντοπιστούν σε αυτήν συγκεκριμένα μοτίβα συμπεριφοράς τα οποία υποδηλώνουν έλλειψη τυχαιότητας και μπορεί να διακυβεύσουν την συνολική ασφάλεια ενός κρυπτογραφικού συστήματος [71].

3.2.3.1 Γενική Μεθοδολογία

Αρχικά λοιπόν, ορίζεται η μηδενική υπόθεση H_0 (null hypothesis), με την οποία δηλώνεται ως τυχαία η δυαδική ακολουθία εισόδου. Στην συνέχεια, η ισχύς της μηδενικής υπόθεσης H_0 τίθεται υπό αμφισβήτηση και εξετάζεται μέσω των 15 ελέγχων του πακέτου.

Έπειτα, εφαρμόζονται τα διαθέσιμα στατιστικά τεστ επί της δοθείσας ακολουθίας. Κάθε αλγόριθμος εκτελείται σε επίπεδο bit, ελέγχοντας την εμφάνιση ακραίων συμπεριφορών που σε μια πραγματικά τυχαία ακολουθία είναι σπάνιο να παρατηρηθούν. Συνεπώς, αυξημένη πιθανότητα εμφάνισης τέτοιων στατιστικών ανωμαλιών συνηγορούν προς την απόρριψη της αρχικής υπόθεσης.

Κατόπιν, υπολογίζεται το λεγόμενο p-value για κάθε έναν από τους εφαρμοζόμενους ελέγχους. Μέσω αυτού ποσοτικοποιείται και συνοψίζεται η απόκλιση συμπεριφοράς που εμφανίζει η δοθείσα ακολουθία από μια πραγματικά τυχαία πηγή. Ουσιαστικά κάθε p-value αντιστοιχεί σε μια στατιστική τιμή, η οποία αντιπροσωπεύει την πιθανότητα μια γεννήτρια πραγματικά τυχαίων αριθμών να παράξει λιγότερο τυχαίες ακολουθίες από αυτήν που εξετάζεται. Σε αυτό το πλαίσιο λοιπόν, το σύνολο όλων των p-values ορίζεται στο διάστημα [0,1], όπου η τιμή 0 υποδηλώνει μια πλήρως ντετερμινιστική συμπεριφορά, ενώ η τιμή 1 μια συμπεριφορά που φαίνεται να είναι πραγματικά τυχαία.

Ακολούθως, κάθε p-value συγκρίνεται με ένα επίπεδο εμπιστοσύνης $\alpha \in (0.001, 0.01]$, το οποίο αντιστοιχεί στο μέγιστο επιτρεπόμενο ποσοστό απορρίψεων μιας πραγματικά τυχαίας ακολουθίας. Η τιμή του α κατ' ουσίαν αποτελεί το όριο ανοχής για την λανθασμένη απόρριψη της μηδενικής υπόθεσης H_0 και καθορίζεται από τις απαιτήσεις της εκάστοτε κρυπτογραφικής εφαρμογής. Η προεπιλεγμένη τιμή του στο λογισμικό πακέτο ισούται με 0.01, γεγονός που σημαίνει ότι μία ακολουθία από τις εκατό που παράγονται μέσω μια γεννήτριας πλήρως τυχαίων αριθμών αναμένεται τελικά να απορριφθεί.

Εν τέλει, το p-value εκάστου τεστ καθιστά αποδεκτή ή απορριπτέα την αρχική μηδενική υπόθεση H_0 ανάλογα με την τιμή του. Στην περίπτωση που ένας έλεγχος επιστρέφει p-value με τιμή μεγαλύτερη από αυτήν που ορίζει το επιλεγμένο επίπεδο εμπιστοσύνης, τότε το τεστ θεωρείται επιτυχημένο. Αντίθετα, όταν ισχύει η ανισότητα p-value < α, τότε η ακολουθία εισόδου χαρακτηρίζεται μη τυχαία και η υπόθεση H_0 καθίσταται απορριπτέα.

3.2.3.2 Συνοπτική Περιγραφή Διαγνωστικών Ελέγχων

3.2.3.2.1 Frequency (Monobit) Test

Ο πρώτος έλεγχος που εκτελείται από το λογισμικό πακέτο του NIST επικεντρώνεται στο συνολικό πλήθος των μηδενικών και των μονάδων της υπό μελέτη ακολουθίας, το οποίο για μια γεννήτρια πραγματικά τυχαίων αριθμών αναμένεται να είναι ισάριθμο. Ειδικότερα, προσδιορίζονται οι πιθανότητες εμφάνισης των 0 και 1 σε όλο το μήκος της ακολουθίας και εκτιμάται η απόκλισή τους από την αναμενόμενη τιμή 0.5. Σε περίπτωση που η απόκλιση αυτή είναι μεγάλη, η ακολουθία παρουσιάζει σαφή τάση προς μια εκ των δύο δυαδικών τιμών και το τεστ τελικά αποτυγχάνει.

Θα πρέπει να σημειωθεί ότι ακολουθίες που αποτυγχάνουν στο Frequency Monobit Test θεωρούνται de facto μη τυχαίες και οι υπόλοιποι έλεγχοι του λογισμικού δεν χρειάζεται να πραγματοποιηθούν καν.

3.2.3.2.2 Frequency Test within a Block

Το δεύτερο τεστ του πακέτου εξετάζει την αναλογία των μονάδων και των μηδενικών σε ισομήκη υποσύνολα της δοθείσας ακολουθίας. Τα υποσύνολα αυτά αντιστοιχούν σε έναν ακέραιο αριθμό N μη επικαλυπτόμενων τμημάτων με M bits, για κάθε ένα από τα οποία το πλήθος των 1 (ή των 0) θα πρέπει να προσεγγίζει την τιμή M/2, ώστε η ακολουθία στο σύνολο της να χαρακτηριστεί τυχαία.

Ουσιαστικά, ο παρών έλεγχος εξασφαλίζει την ισοκατανομή των 0 και 1 σε όλο το εύρος της δοθείσας ακολουθίας. Για υποακολουθίες μήκους M = 1, ο έλεγχος εκφυλίζεται στο τεστ της προηγούμενης παραγράφου.

3.2.3.2.3 Runs Test

Το τρίτο τεστ του πακέτου NIST εξετάζει τον ρυθμό εναλλαγής των διαδοχικών ροών στο σύνολο της ακολουθίας, όπου ως ροές νοούνται τα τμήματα αυτής που αποτελούνται αποκλειστικά και μόνο από πανομοιότυπα bits. Ουσιαστικά πρόκειται για ένα διαγνωστικό τεστ που ελέγχει αν το πλήθος των ροών της ακολουθίας και η ταχύτητα ταλάντωσής της προσεγγίζουν το αναμενόμενο μιας τυχαίας πηγής.

3.2.3.2.4 Test for the Longest Run of Ones in a Block

Σκοπός του συγκεκριμένου ελέγχου είναι η εύρεση του μεγίστου πλήθους από διαδοχικές μονάδες, σε ισομήκη και μη επικαλυπτόμενα τμήματα της ακολουθίας εισόδου. Με άλλα λόγια, ο παρών αλγόριθμος διαχωρίζει την υπό μελέτη ακολουθία σε επιμέρους blocks, όπως αυτά του 3.2.3.2.2, και εξετάζει αν το μέγιστο μήκος ροών από 1 εντός τους αποκλίνει της τιμής που προκύπτει από την έξοδο μιας γεννήτριας πραγματικά τυχαίων αριθμών.

3.2.3.2.5 Binary Matrix Rank Test

Κατά τον πέμπτο έλεγχο του πακέτου, ερευνάται η ύπαρξη επαναλαμβανόμενων μοτίβων σε όλο το εύρος της δοθείσας ακολουθίας, τα οποία σχετίζονται με την γραμμική εξάρτηση των επιμέρους τμημάτων της. Ο έλεγχος αυτός πραγματοποιείται ακολούθως:

Αρχικά, η υπό μελέτη ακολουθία διαιρείται σε έναν ακέραιο αριθμό μη επικαλυπτόμενων και ισοπληθών υποσυνόλων, τα οποία αναπαρίστανται ως πίνακες M×Q διαστάσεων, με M = Q = 32. Στην συνέχεια, υπολογίζεται η τάξη των παραγόμενων αυτών πινάκων, η οποία αντικατοπτρίζει τον αριθμό των γραμμικά ανεξάρτητων γραμμών ή στηλών τους. Έπειτα, οι πίνακες ταξινομούνται σε τέσσερεις διαφορετικές κατηγορίες, βάσει της τάξης τους. Αν το πλήθος των πινάκων σε κάθε κατηγορία προσεγγίζει το αναμενόμενο, τότε η ακολουθία εισόδου χαρακτηρίζεται τελικά ως τυχαία.

3.2.3.2.6 Discrete Fourier Transform (Spectral) Test

Στα πλαίσια του ελέγχου αυτού, πραγματοποιείται η φασματική ανάλυση της ακολουθίας εισόδου, μέσω της οποίας καθίσταται εφικτή η ανίχνευση περιοδικά επαναλαμβανόμενων προτύπων. Αρχικά εφαρμόζεται ο διακριτός μετασχηματισμός Fourier στην υπό μελέτη ακολουθία και υπολογίζεται το μέτρο των στοιχείων που προκύπτουν από αυτόν. Έπειτα, προσδιορίζεται το πλήθος των φασματικών κορυφών με ύψος που υπερβαίνει ένα προκαθορισμένο κατώτατο όριο. Εάν το πλήθος αυτό ξεπερνά το 5% του συνολικού αριθμού των στοιχείων του φάσματος, τότε το τεστ θεωρείται ανεπιτυχές και η ακολουθία αξιολογείται ως μη τυχαία.

3.2.3.2.7 Non-overlapping Template Matching Test

Με τον έβδομο έλεγχο του λογισμικού πακέτου εξετάζεται το πλήθος των απεριοδικών προτύπων που παρουσιάζονται στο σύνολο της ακολουθίας εισόδου. Για την ακρίβεια, διερευνούνται οι συχνότητες εμφάνισης 148 προεπιλεγμένων προτύπων με μήκος m, οι οποίες υπολογίζονται ξεχωριστά από ισάριθμους επιμέρους ελέγχους.

Σε αυτό το πλαίσιο, κάθε υποελέγχος απαριθμεί τις φορές που απαντάται ένα από τα προαναφερθέντα προκαθορισμένα μοτίβα σε όλο το εύρος της δοθείσας ακολουθίας, επιστρέφοντας μια διακριτή τιμή p-value. Συνεπώς, συνολικά υπολογίζονται 148 p-values, ένα για κάθε πρότυπο.

Η μεθοδολογία ανίχνευσης προτύπων είναι κοινή σε όλους τους επιμέρους ελέγχους και η αναζήτηση εκάστου μοτίβου λαμβάνει χώρα με πανομοιότυπο τρόπο: η ακολουθία σαρώνεται με ένα παράθυρο παρατήρησης από m bits, μέσω του οποίου εξετάζεται η ύπαρξη του προτύπου. Εάν αυτό ανιχνευθεί, τότε το παράθυρο μετατοπίζεται κατά m θέσεις και η αναζήτηση συνεχίζεται. Στην αντίθετη περίπτωση το παράθυρο ολισθαίνει κατά ένα bit μόνο.

3.2.3.2.8 Overlapping Template Matching Test

Από την άλλη πλευρά, το όγδοο τεστ του λογισμικού πακέτου εστιάζει στην συχνότητα εμφάνισης προκαθορισμένων περιοδικών προτύπων μήκους m. Κατ' αντιστοιχία με τον έλεγχο της προηγούμενης παραγράφου, κάθε μοτίβο αναζητείται χρησιμοποιώντας ένα ολισθαίνον παράθυρο παρατήρησης από m bits, το οποίο όμως στην συγκεκριμένη περίπτωση μετατοπίζεται πάντα κατά μία μόνο θέση.

3.2.3.2.9 Maurer's Universal Statistical Test

Το συγκεκριμένο τεστ εξετάζει εάν είναι εφικτή η επαρκής αναπαράσταση της δοθείσας ακολουθίας, από μια ακολουθία σημαντικά μικρότερου μήκους. Με άλλα λόγια, διερευνά την δυνατότητα συμπίεσής της χωρίς απώλεια πληροφορίας.

Αρχικά λοιπόν, η υπό μελέτη ακολουθία διαμερίζεται σε ισομήκη υποσύνολα των L bits, τα οποία στη συνέχεια διαμοιράζονται σε δύο άνισα μέρη: το πρώτο τίθεται ως το τμήμα αρχικοποίησης της διαδικασίας και περιλαμβάνει Q υποσύνολα από L bits, ενώ το δεύτερο ως το τμήμα ελέγχου της, περιέχοντας K υποσύνολα ιδίου μήκους. Κατόπιν, επιλέγεται το πρώτο υποσύνολο του τμήματος ελέγχου και εντοπίζεται το πλησιέστερο υποσύνολο του τμήματος αρχικοποίησης με το οποίο ταυτίζεται, καταγράφοντας την μεταξύ τους απόσταση. Η διαδικασία επαναλαμβάνεται μέχρις ότου χρησιμοποιηθούν όλα τα διαθέσιμα υποσύνολα. Από τις καταγραφείσες αποστάσεις διαπιστώνεται τελικά η δυνατότητα βραχείας περιγραφής της ακολουθίας.

3.2.3.2.10 Linear Complexity Test

Στα πλαίσια του παρόντος ελέγχου, αξιολογείται η γραμμική πολυπλοκότητα ισομηκών τμημάτων της ακολουθίας εισόδου, σε σχέση με ακολουθίες πανομοιότυπου μήκους και πολυπλοκότητας που προκύπτουν από καταχωρητές ολίσθησης γραμμικής ανάδρασης (Linear Feedback Shift Registers - LSFR).

Γενικά, ένας καταχωρητής ολίσθησης με γραμμική ανάδραση συνήθως αποτελείται από μια συστοιχία θέσεων μνήμης (flip-flops), οι οποίες είναι συνδεδεμένες με τέτοιο τρόπο, έτσι ώστε σε κάθε παλμό του ρολογιού το περιεχόμενο τους να μετατοπίζεται κατά μία θέση δεξιά και η είσοδος της πρώτης εξ αυτών να καθορίζεται από τις τιμές κάποιων τυχαία επιλεγμένων θέσεών του. Η πολυπλοκότητα από την οποία χαρακτηρίζεται ένας LSFR είναι ευθέως ανάλογη του μήκους του, δηλαδή με τον αριθμό των θέσεων μνήμης που αυτος περιέχει. Συνεπώς, ένας LSFR μεγάλου μήκους δύναται να παράξει δυαδικές ακολουθίες υψηλής περιπλοκότητας, αποτελώντας μια ιδανική βάση για την υλοποίηση γεννητριών ψευδοτυχαίων αριθμών.

Επί του πρακτέου, προκειμένου να προσδιοριστεί και να αξιολογηθεί η περιπλοκότητα της ζητούμενης ακολουθίας εφαρμόζονται τα εξής βήματα: Η ακολουθία διαμερίζεται σε υποσύνολα των M bits και υπολογίζεται η γραμμική πολυπλοκότητά τους, μέσω του αλγορίθμου Berlekamp - Masse [72]. Ο βαθμός της πολυπλοκότητας ταυτίζεται με το ελάχιστο πλήθος θέσεων που πρέπει να έχει ένας LSFR για να παράξει μια δυαδική ακολουθία ίδιου μήκους. Επομένως, εάν τα

υποσύνολα της ακολουθίας αντιστοιχούν σε εξόδους καταχωρητών βραχέως μήκους τότε ο έλεγχος αποτυγχάνει.

3.2.3.2.11 Serial Test

Το ενδέκατο τεστ του λογισμικού πακέτου NIST εστιάζει στη συχνότητα εμφάνισης όλων των δυνατών 2^m αλληλεπικαλυπτόμενων μοτίβων που μπορούν να παραχθούν από m bits, κατά μήκος ολόκληρης της ακολουθίας. Ειδικότερα, εξετάζεται εάν το ενδεχόμενο εμφάνισης των μοτίβων αυτών είναι ισοπίθανο και εάν το πλήθος τους προσεγγίζει την αναμενόμενη τιμή $n/2^m$ μιας πραγματικά τυχαίας ακολουθίας.

Ουσιαστικά, ο παρών έλεγχος εξασφαλίζει την ομοιόμορφη κατανομή υποσυνόλων από m bits, σε όλο το εύρος της ακολουθίας εισόδου. Για μήκη m = 1, ο έλεγχος εκφυλίζεται στο Frequency Monobit Test της παραγράφου 3.2.3.2.1.

3.2.3.2.12 Approximate Entropy Test

Στα πλαίσια του ελέγχου αυτού αποτιμάται η προσεγγιστική εντροπία της ακολουθίας, χρησιμοποιώντας τις συχνότητες όλων των πιθανών αλληλεπικαλυπτόμενων τμημάτων της. Συγκεκριμένα, υπολογίζονται και αντιπαραβάλλονται οι συχνότητες εμφάνισης δύο ξεχωριστών συνόλων με αλληλεπικαλυπτόμενες υποακολουθίες, μήκους m και m+1 bits αντιστοίχως, από τις οποίες προκύπτει και η ζητούμενη εντροπία.

Εν γένει, καθώς το μέγεθος της εντροπίας αποτελεί ένα μέτρο αβεβαιότητας και αταξίας, η προσεγγιστική εντροπία είναι ευθέως ανάλογη της τυχαιότητας που εμπεριέχεται στην δοθείσα ακολουθία. Συνεπώς, η ευρεθείσα τιμή της θα πρέπει να είναι όσο το δυνατόν μεγαλύτερη ώστε το τεστ να θεωρηθεί επιτυχημένο, προσεγγίζοντας ιδανικά την μέγιστη θεωρητική τιμή ln2.

3.2.3.2.13 Cumulative Sums (Cusum) Test

Το Cumsum τεστ εξετάζει εάν είναι υπερβολικά υψηλό το πλήθος των μηδενικών και των μονάδων στα άκρα της δοθείσας ακολουθίας, αποτελώντας ουσιαστικά άλλον έναν διαγνωστικό έλεγχο που εστιάζει στην ομοιομορφία και την ισοκατανομή των δυαδικών τιμών εντός της. Πρακτικά υλοποιείται εφαρμόζοντας τα παρακάτω βήματα:

Αρχικά, αντικαθίστανται τα μηδενικά σε ολόκληρη την έκταση της ακολουθίας από το -1. Στην συνέχεια, προσδιορίζονται διαδοχικά όλα τα σωρευτικά αθροίσματα των ψηφίων της, προσθέτοντας την τιμή της εκάστοτε τρέχουσας θέσης στο άθροισμα των στοιχείων που έχουν ήδη προηγηθεί. Έπειτα, εντοπίζεται εξ αυτών το άθροισμα με την μέγιστη απόλυτη τιμή, η οποία αντιπαραβάλλεται με το αναμενόμενο αποτέλεσμα ενός απλού τυχαίου περιπάτου[7], καθορίζοντας την τελική έκβαση του τεστ.

Στο σημείο αυτό πρέπει να αναφερθεί ότι η άνωθεν διαδικασία εκτελείται ανατρέχοντας τα ψηφία της ακολουθίας εισόδου από αριστερά προς τα δεξιά.

[7] Ως απλός τυχαίος περίπατος ορίζεται μια τυχαία αλληλουχία ισοπίθανων βημάτων μοναδιαίου μήκους ±1, η οποία ξεκινά και καταλήγει στο μηδέν. Η επιστροφή στην μηδενική τιμή υποδηλώνει έναν πλήρη κύκλο τυχαίου περιπάτου, ενώ η αναμενόμενη μέση τιμή οποιουδήποτε περιπάτου ισούται με το μηδέν.

Όμως ο παρών έλεγχος διενεργείται και με αντίστροφη φορά σάρωσης, επομένως επιστρέφει δύο τιμές από p-values, μία για κάθε κατεύθυνση.

3.2.3.2.14 Random Excursions Test

Ο παρών έλεγχος διερευνά εάν κάθε κύκλος τυχαίου περιπάτου που προκύπτει από τα σωρευτικά αθροίσματα της δοθείσας ακολουθίας, περιλαμβάνει το αναμενόμενο πλήθος επισκέψεων σε 8 προκαθορισμένες καταστάσεις.

Αρχικά, υπολογίζονται τα συσσωρευτικά αθροίσματα της ακολουθίας εισόδου με την μέθοδο της προηγούμενης παραγράφου και συγκεντρώνονται σε ένα διάνυσμα S. Στην αρχή και το πέρας του S προστίθεται ένα μηδενικό. Εν συνεχεία, εντοπίζονται όλες οι μηδενικές τιμές εντός του, με το ευρεθέν πλήθος τους (J-1) να εκφράζει τον αριθμό των κύκλων από τυχαίους περιπάτους που περιλαμβάνει η εν λόγω ακολουθία. Εάν το J βρεθεί μικρότερο του 500, τότε το τεστ θεωρείται ήδη αποτυχές και τερματίζεται. Στην αντίθετη περίπτωση, ο έλεγχος συνεχίζεται ως εξής:

Σε κάθε κύκλο του διανύσματος S, καταμετρούνται οκτώ προκαθορισμένες καταστάσεις x, όπου $x \in \{\pm1,\pm2,\pm3,\pm4\}$. Αυτές αντιπροσωπεύουν τις πιθανότερες απομακρύνσεις από το μηδέν σε έναν απλό τυχαίο περίπατο. Αποστάσεις που ξεπερνούν το |±4| έχουν τόσο μικρό ενδεχόμενο εμφάνισης ώστε συμπεριλαμβάνονται στις καταστάσεις ±4. Ο αριθμός εμφάνισης κάθε μιας κατάστασης σε έναν κύκλο ουσιαστικά αποτελεί και το ζητούμενο πλήθος των προαναφερθέντων επισκέψεων σε αυτήν.

Αφού προσδιοριστούν οι επισκέψεις στις οκτώ προεπιλεγμένες καταστάσεις για κάθε κύκλο, έπειτα υπολογίζεται το πλήθος $v_k(x)$ των κύκλων, στους οποίους μια κατάσταση x εμφανίζεται ακριβώς κ φορές, με $\kappa \in \{0,1,2,3,4,5\}$. Κάθε $v_k(x)$ αντιπαραβάλλεται με το αναμενόμενο αποτέλεσμα μιας τυχαίας ακολουθίας, και ο έλεγχος εν τέλει επιστρέφει 8 διαφορετικές τιμές από p-values, μία για κάθε υπό μελέτη κατάσταση

3.2.3.2.15 Random Excursions Test

Ο τελευταίος έλεγχος του λογισμικού πακέτου NIST εξετάζει εάν όλοι οι κύκλοι από τους τυχαίους περιπάτους που εντοπίστηκαν κατά την διάρκεια του προηγούμενου τεστ, περιλαμβάνουν το αναμενόμενο πλήθος επισκέψεων σε δεκαοκτώ προκαθορισμένες καταστάσεις. Με άλλα λόγια, υπολογίζει την συχνότητα εμφάνισης από 18 διαφορετικά x εντός του διανύσματος S, όπου $x \in \{\pm1,\pm2,\pm3,\pm4,\pm5,\pm6,\pm7,\pm8,\pm9\}$, για κάθε ένα εκ των οποίων επιστρέφει και μια ξεχωριστή τιμή p-value.

3.2.3.3 Εισαγωγή Δεδομένων

Σύμφωνα με το αναθεωρημένο εγχειρίδιο χρήσης που εκδόθηκε από τον οργανισμό NIST το 2010 [71], το ελάχιστο μήκος ακολουθίας που απαιτείται για την ορθή εφαρμογή όλων των διαγνωστικών ελέγχων θα πρέπει να είναι τουλάχιστον 1 Mbit. Από την άλλη πλευρά, το πλήθος των ακολουθιών που εισάγεται προς εξέταση θα πρέπει να είναι ανάλογο του χρησιμοποιούμενου επιπέδου εμπιστοσύνης, το οποίο στην παρούσα μελέτη επιλέχθηκε να είναι ίσο με $\alpha = 0.01$. Συμπερασματικά, προκειμένου να διασφαλιστεί η ορθή χρήση του ομώνυμου πακέτου και η αξιοπιστία των αντίστοιχων αποτελεσμάτων του, το αρχείο δεδομένων που εισάγεται πρέπει να είναι τουλάχιστον 100Mbit για επίπεδο εμπιστοσύνης ίσο με $\alpha = 0.01$, περιέχοντας το λιγότερο 100 ακολουθίες με μήκος 1000000 bits.

3.2.3.4 Ερμηνεία Αποτελεσμάτων και Εξαγωγή Συμπερασμάτων

Τα τελικά αποτελέσματα που προκύπτουν από την εκτέλεση όλων των αλγορίθμων του λογισμικού πακέτου NIST μπορούν να εντοπιστούν συγκεντρωμένα σε ένα αυτόματα παραγόμενο αρχείο, το οποίο ονομάζεται finalAnalysisReport.txt. Χαρακτηριστικό δείγμα ενός τέτοιου αρχείου αποτελεί ο ακόλουθος πίνακας τιμών.

Πίνακας 1: Τμήμα του πίνακα αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα t.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη. Το αρχείο δεδομένων t.txt παράχθηκε μέσω της γεννήτριας Mersenne twister, η οποία αποτελεί την προκαθορισμένη επιλογή αλγορίθμου στο MATLAB.

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\t.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
16	13	12	4	9	9	8	10	11	8	0.38383	0.97	Frequency
10	6	9	17	5	10	14	7	14	8	0.13728	0.99	Block Frequency
16	11	14	9	4	9	7	5	8	17	0.03757	0.99	Cumulative Sums
16	6	10	3	10	8	12	9	17	9	0.06688	0.97	Runs
11	8	13	11	16	11	12	4	7	7	0.27571	0.98	Longest Run
11	9	12	15	8	10	10	7	12	6	0.69931	0.99	Rank
7	9	5	10	17	9	11	7	13	12	0.28967	0.99	FFT
16	13	7	9	8	12	16	8	5	6	0.10879	0.95*	Non-Overlap. Temp
7	8	8	20	7	8	11	14	8	9	0.08559	0.99	Overlapping Temp
8	11	6	7	10	7	12	7	18	4	0.15376	0.99	Universal
8	7	7	8	16	9	10	11	11	12	0.69931	0.99	Entropy
10	3	4	4	8	9	6	4	10	7	0.26446	0.9538*	Random Exc
5	12	7	8	9	5	2	9	4	4	0.11652	0.9692	Random Exc Var
9	11	8	11	10	9	9	9	7	17	0.65793	1.00	Series
14	10	11	9	5	4	9	10	16	12	0.21331	1.00	Linear Complexity

The minimum pass rate for each statistical test except for the random excursion var test is approximately = 0.964130 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion var test is approximately 0.957913 for a sample size = 65 binary sequences.

Σύμφωνα με τον παραπάνω πίνακα, σε κάθε εφαρμοζόμενο τεστ αντιστοιχούν 12 στήλες αποτελεσμάτων.

- Οι στήλες C1 με C10 αντιπροσωπεύουν την ποσοτική κατανομή των p-values που έχουν υπολογιστεί για κάθε μία από τις εξεταζόμενες ακολουθίες, σε δέκα κλάσεις πανομοιότυπου εύρους, οι οποίες καλύπτουν το διάστημα [0,1]. Με άλλα λόγια, περιλαμβάνουν το πλήθος των ακολουθιών, τα p-values των οποίων εμπίπτουν στα υποδιαστήματα (0,0.1], (0.1,0.2],…, (0.9,1] αντιστοίχως.
- Η στήλη με τον τίτλο PROPORTION παρουσιάζει την αναλογία των ακολουθιών, για τις οποίες ισχύει η ανισότητα p-value > α, όπου α = 0.01.
- Τέλος, η στήλη με τον τίτλο P-VALUE περιέχει το συνολικό p-value των p-values (POP). Ουσιαστικά, κάθε στοιχείο της στήλης αυτής αποτελεί μια στατιστική τιμή, η οποία αντικατοπτρίζει πόσο ομοιόμορφη είναι η κατανομή των p-values που έχουν υπολογιστεί για κάθε μία από τις εξεταζόμενες ακολουθίες στα διαστήματα C1 με C10.

Δεδομένου λοιπόν του άνωθεν συνόλου πληροφοριών, η τελική αξιολόγηση της εκάστοτε γεννήτριας αριθμών πραγματοποιείται χρησιμοποιώντας δυο διαφορετικές αλλά αλληλοσυμπληρούμενες προσεγγίσεις.

Η πρώτη εξ αυτών εστιάζει στην στήλη PROPORTION και λαμβάνει χώρα ως εξής. Κάθε προκύπτουσα αναλογία συγκρίνεται με ένα ελάχιστο ποσοστό επιτυχίας, το οποίο παρέχεται από το ίδιο το πακέτο στο τέλος του αρχείου των αποτελεσμάτων. Αν μια αναλογία βρεθεί μικρότερη από το εν λόγω ποσοστό, τότε το αντίστοιχο τεστ θεωρείται αποτυχημένο και δίπλα από την αντίστοιχη τιμή της στήλης εμφανίζεται ένας αστερίσκος.

Η δεύτερη προσέγγιση από την άλλη πλευρά εστιάζει στην στήλη των POP. Σε αυτήν, για να θεωρηθεί ένα τεστ επιτυχές θα πρέπει η αντίστοιχη POP του να ξεπερνά ένα όριο ανοχής, η προεπιλεγμένη τιμή του οποίου ορίζεται από το λογισμικό πακέτο και ισούται με 10^{-4}. Στην αντίθετη περίπτωση, ένας αστερίσκος εμφανίζεται δίπλα από την αντίστοιχη τιμή POP.

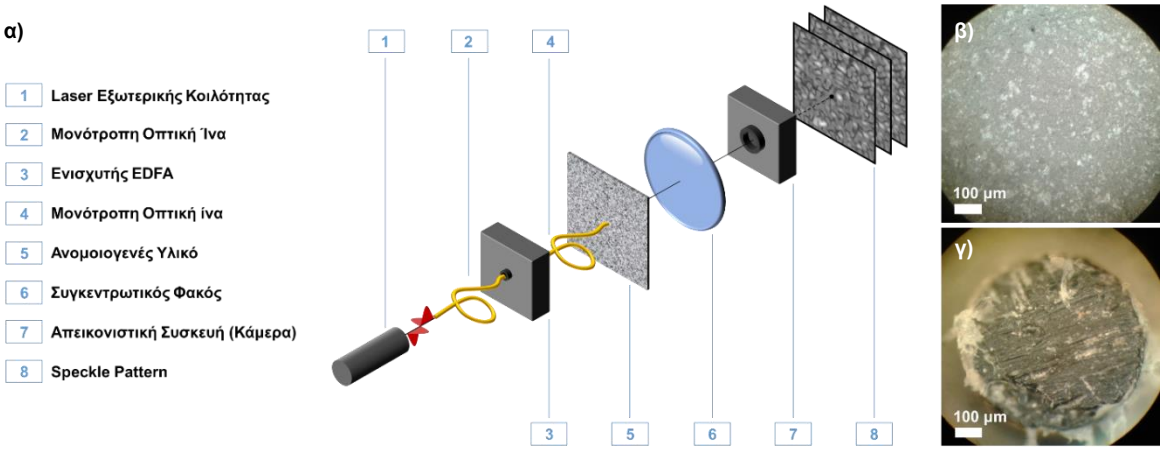
Σε αυτό το πλαίσιο, τα αποτελέσματα που επιδεικνύονται στον πίνακα 1 μπορούν να ερμηνευθούν ακολούθως: από τους 15 παρουσιαζόμενους διαγνωστικούς ελέγχους, δύο τεστ, τα Random Excursions και Non-Overlapping Template τεστ, αρχικά διαφαίνεται ότι αποτυγχάνουν. Όμως, οι αντίστοιχες τιμές αναλογιών τους είναι ελάχιστα μικρότερες από το προβλεπόμενο όριο του 0.964, όπως αυτό έχει ορισθεί από το ομώνυμο πακέτο, και επομένως, οι εν λόγω αποτυχίες να μπορούν να αποδοθούν σε κάποιο στατιστικό λάθος. Το γεγονός αυτό επιβεβαιώθηκε διενεργώντας πέντε επαναληπτικές εφαρμογές όλων των διαθέσιμων ελέγχων, σε μια σειρά αρχείων η οποία προέκυψε από την ίδια γεννήτρια τυχαίων αριθμών μεταβάλλοντας το seed της. Ταυτόχρονα, όλες οι τιμές της στήλης POP ξεπερνούν το όριο ανοχής που έχει τεθεί, το οποίο όπως ήδη αναφέρθηκε άνωθεν ισούται με 0.0001, υποδηλώνοντας ότι η παρατηρούμενη γεννήτρια αριθμών παρουσιάζει αρκετά ομοιόμορφες κατανομές από p-values, σε όλο το εύρος του πεδίου ορισμού τους και για κάθε τεστ.

Συμπερασματικά, η συμπεριφορά της παρουσιαζόμενης γεννήτριας αριθμών προκύπτει αρκούντως τυχαία, με όλους τους ελέγχους του λογισμικού πακέτου NIST να θεωρούνται επιτυχείς.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι ο πίνακας 1 αντιστοιχεί στα αποτελέσματα που προέκυψαν από ένα αρχείο δεδομένων με 100 ακολουθίες, 1Mbit έκαστη, το οποίο παράχθηκε μέσω της γεννήτριας Mersenne twister. Η εν λόγω γεννήτρια αποτελεί την προκαθορισμένη επιλογή αλγορίθμου στο MATLAB. Θα πρέπει επίσης να σημειωθεί, ότι ο πίνακας περιλαμβάνει μόνο ένα τμήμα των εξαγόμενων αποτελεσμάτων, καθώς η πλειοψηφία των επιμέρους υποέλεγχων που εφαρμόζονται στα πλαίσια ορισμένων τεστ έχει παραληφθεί.

4. ΠΕΙΡΑΜΑΤΙΚΗ ΔΙΑΤΑΞΗ ΜΕ ΣΥΝΤΟΝΙΖΟΜΕΝΟ LASER

Η πρώτη πειραματική διάταξη που υλοποιήθηκε στο πλαίσιο της παρούσας διατριβής παρουσιάζεται στο σχήμα 4.1α. Η διάταξη αυτή σχεδιάστηκε προκειμένου να αξιολογηθεί η απόδοση μιας οπτικής PUF, οι εφαρμοζόμενες διεγέρσεις της οποίας προκύπτουν από την ελεγχόμενη και συστηματική μεταβολή του μήκους κύματος της χρησιμοποιούμενης δέσμης ακτινοβολίας.



Σχήμα 4.1: α) Πειραματική υλοποίηση οπτικής PUF με χρήση ενός συντονιζόμενου laser για την παραγωγή διεγέρσεων με διαφορετικό μήκος κύματος. Η ανομοιογενής επιφάνεια εξόδου **β)** του γυάλινου πλακιδίου διάχυσης φωτός και **γ)** της χρησιμοποιούμενης οπτικής ίνας.

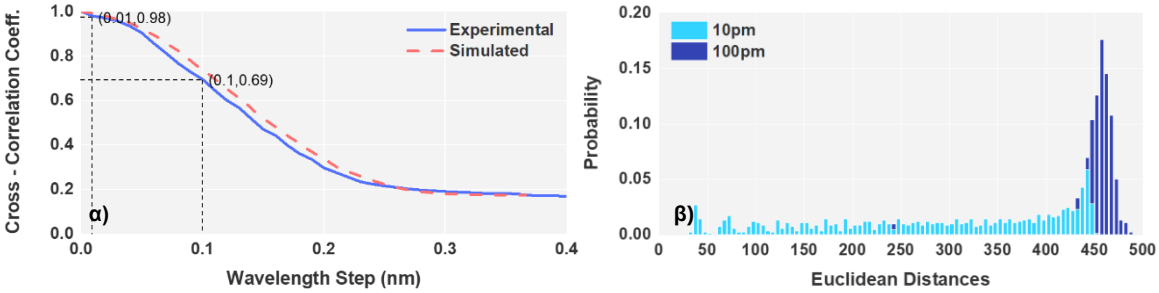
Ειδικότερα, ως πηγή σύμφωνης ακτινοβολίας χρησιμοποιήθηκε ένα διοδικό CW laser εξωτερικής κοιλότητας με συντονιζόμενο μήκος κύματος λ, το οποίο λαμβάνει τιμές στο εγγύς υπέρυθρο από τα 1540nm έως τα 1560nm. Η έξοδος του laser αυτού [1] αρχικά οδηγείται μέσω μίας μονότροπης οπτικής ίνας (Single Mode Fiber - SMF) [2] σε έναν οπτικό ενισχυτή ίνας με προσμίξεις Ερβίου (Erbium Doped Fiber Amplifier - EDFA) [3] και κατόπιν προσπίπτει μέσω μιας δεύτερης SMF [4] στο υπό μελέτη ανομοιογενές μέσο [5]. Εν συνεχεία, η δέσμη που εξέρχεται του μέσου αυτού διέρχεται από έναν αμφίκυρτο φακό εστιακής απόστασης 6mm [6] και συγκεντρώνεται στον αισθητήρα μιας κάμερας vidicon [7] με ανάλυση 340×340 pixels και χρωματικό βάθος 8-bits, μέσω της οποίας λαμβάνεται και η τελική απόκριση του συστήματος [8].

Επομένως, η παραγωγή δυο διαδοχικών διεγέρσεων, όπως αυτές εφαρμόζονται στο πλαίσιο της εικονιζόμενης διάταξης, ισοδυναμεί με την μεταβολή Δλ του μήκους κύματος της δέσμης που προσπίπτει στο εκάστοτε ανομοιογενές υλικό, διατηρώντας όλες τις υπόλοιπες παραμέτρους ακτινοβόλησης σταθερές.

Στο σημείο αυτό θα πρέπει να αναφερθεί ότι ο συνολικός συντονισμός της περιγραφείσας διαδικασίας πραγματοποιήθηκε μέσω του περιβάλλοντος LabVIEW, ενώ δοκιμάστηκαν 2 διαφορετικά ανομοιογενή υλικά ως ενδεχόμενες πηγές πολυπλοκότητας. Συγκεκριμένα, τα δείγματα που επιλέχθηκαν να μελετηθούν ήταν μία πολύτροπη πολυμερική οπτική ίνα βηματικού δείκτη διάθλασης, με πυρήνα 980μm, μήκος 12cm και τυχαίες ανομοιογένειες στις επιφάνειες εισόδου/εξόδου της (unpolished POF), καθώς και ένα γυάλινο πλακίδιο διάχυσης φωτός με τυχαίες αυξομειώσεις στον μιγαδικό δείκτη διάθλασής του (diffuser). Εν προκειμένω, στις φωτογραφίες β και γ του σχήματος 4.1 παρουσιάζονται οι επιφάνειες εξόδου των δύο προαναφερθέντων δειγμάτων, όπως αυτές καταγράφηκαν μέσω ενός συμβατικού εργαστηριακού μικροσκοπίου.

4.1 Επιλογή Δλ Δύο Διαδοχικών Διεγέρσεων

Με χρήση της άνωθεν διάταξης, αρχικά εξετάστηκε η επίδραση του μήκους κύματος λ της χρησιμοποιούμενης ακτινοβολίας πάνω στη συσχέτιση των αποκρίσεων που παράγονται μέσω της POF, προκειμένου να επιλεχθεί μια κατάλληλη τιμή Δλ, η οποία θα οδηγεί σε αρκούντως ανόμοια speckles. Η διερεύνηση αυτή πραγματοποιήθηκε ως εξής: πρώτα καταγράφηκε ένα speckle pattern αναφοράς με λ_0 στα 1548nm και έπειτα λήφθηκαν 40 επαναληπτικές μετρήσεις, αυξάνοντας με διαδοχικό τρόπο το χρησιμοποιούμενο μήκος κύματος κατά Δλ = 10pm κάθε φορά. Με άλλα λόγια, λήφθηκαν 41 συναπτές αποκρίσεις r_i με $0 \leq i \leq 40$ και $\lambda_i =$ (1548 + iΔλ)nm, όπου Δλ = 0.01nm. Έπειτα, υπολογίστηκε ο συντελεστής διασυσχέτισης Pearson μεταξύ της εικόνας αναφοράς και των διαθέσιμων επαναληπτικών μετρήσεων, οι τιμές του οποίου αναπαρίστανται γραφικά ως συνάρτηση της διαφοροποίησης iΔλ από το αρχικό μήκος κύματος λ_0 στο διάγραμμα του σχήματος 4.2α.



Σχήμα 4.2: α) Ο συντελεστής διασυσχέτισης Pearson συναρτήσει της διαφοροποίησης του μήκους κύματος iΔλ της χρησιμοποιούμενης δέσμης ακτινοβολίας. **β)** Οι Ευκλείδειες αποστάσεις μεταξύ 41 πειραματικών speckle patterns που λήφθηκαν με Δλ = 10pm μαζί με τις αντίστοιχες Ευκλείδειες αποστάσεις όπως αυτές υπολογίστηκαν μεταξύ των 41 εικόνων που παράχθηκαν με Δλ = 100 pm.

Όπως φαίνεται λοιπόν και από το αντίστοιχο διάγραμμα, ο συντελεστής διασυσχέτισης Pearson των καταγραφόμενων speckle patterns αρχικά μειώνεται όταν η διαφορά μήκους κύματος μεταξύ των εφαρμοζόμενων challenges αυξάνεται, υποδηλώνοντας την αύξηση της ανομοιότητας των παραγόμενων αποκρίσεων και την ενίσχυση του unpredictability των αντίστοιχων ακολουθιών τους. Κατόπιν όμως, ο συντελεστής αυτός ελαχιστοποιείται στη τιμή 0.2, υποδεικνύοντας ότι τα speckle patterns που προκύπτουν από διεγέρσεις με διαφοροποίηση μεγαλύτερη των 200pm είναι εξίσου ανόμοια. Ως εκ τούτου, η περαιτέρω αύξηση της εν λόγω διαφοράς καθίσταται τελείως ανώφελη, αφού δεν προσφέρει καμία επιπρόσθετη ασφάλεια στο unpredictability του υπό μελέτη συστήματος. Συνεπώς, η ιδανική μεταβολή μεταξύ δύο διαδοχικών διεγέρσεων εντοπίζεται περίπου ίση με Δλ = 200pm. Ωστόσο, καθώς η τιμή αυτή περιορίζει ιδιαιτέρως τον συνολικό αριθμό των εν δυνάμει challenges, αντ' αυτής επιλέχθηκε να χρησιμοποιηθεί τελικά μια μεταβολή ίση με 100pm.

Σε αυτό το πλαίσιο, εν συνεχεία λήφθηκε και ένα δεύτερο σύνολο δεδομένων (dataset) από 41 speckle patterns, ορίζοντας αυτή την φορά τη μεταβολή του μήκους κύματος Δλ ίση με 100pm. Κατόπιν, υπολογίστηκαν οι Ευκλείδειες αποστάσεις μεταξύ όλων των κανονικοποιημένων εικόνων και για τα δύο διαθέσιμα σύνολα δεδομένων ξεχωριστά, προκειμένου να καταστεί εφικτή η ταχεία σύγκριση της επίδοσης που παρουσιάζουν τα αντίστοιχα Δλ τους. Ειδικότερα, στο διάγραμμα β) του σχήματος 4.2 παρουσιάζονται υπό την μορφή ιστογραμμάτων οι κατανομές

πιθανοτήτων για τις $_{41}C_2$ = 820 Ευκλείδειες αποστάσεις που προέκυψαν από την σύγκριση των 41 στιγμιοτύπων εκάστου dataset [8].

Όπως παρατηρείται λοιπόν και από το αντίστοιχο διάγραμμα, η κατανομή για μεταβολή μήκους κύματος ίση με 10pm χαρακτηρίζεται από μια ισχυρότερη αρνητική ασυμμετρία έναντι της κατανομής για μεταβολή ίση με 100pm, αφού η πρώτη παρουσιάζει μια εντονότερη και συνεχή ουρά προς την μηδενική τιμή. Η ουρά αυτή, η οποία υποδηλώνει την αυξημένη ομοιότητα μεταξύ των παραγόμενων πειραματικών αποκρίσεων, βρίσκεται σε πλήρη συμφωνία με τα αποτελέσματα του συντελεστή διασυσχέτισης Pearson, η τιμή του οποίου για δύο διαδοχικές λήψεις με Δλ = 10pm βρέθηκε ίση με 0.98 ενώ με Δλ = 100pm 0.69 αντιστοίχως.

Εν κατακλείδι, από τα διαθέσιμα σύνολα εικόνων, όπως αυτά λήφθηκαν για τις ανάγκες της παρούσας ενότητας, παρατηρήθηκε ότι όταν η διαφοροποίηση του μήκους κύματος μεταξύ δυο διαδοχικών λήψεων αυξάνει, αυξάνει και η αποσυσχέτιση των αντίστοιχων γεωμετρικών γνωρισμάτων τους. Συγκεκριμένα, ως ιδανική διαφοροποίηση εντοπίστηκε η τιμή των 200pm, όμως καθώς η τιμή αυτή περιορίζει ιδιαίτερα τον συνολικό αριθμό των εφαρμοζόμενων challenges στην πράξη επιλέχθηκε να χρησιμοποιηθεί αντ' αυτής μια Δλ ίση με 100pm.

4.2 Σύγκριση Unpredictability Οπτικών Μέσων

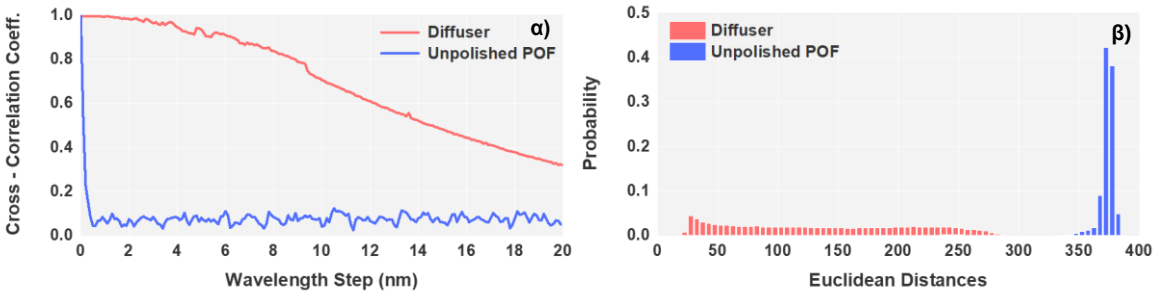
Έχοντας ορίσει το βήμα Δλ μεταξύ δύο διαδοχικών μετρήσεων ίσο με 100pm, εν συνεχεία λήφθηκε ένα επιπρόσθετο σύνολο πειραματικών δεδομένων από 201 speckle patterns, αντικαθιστώντας την χρησιμοποιούμενη οπτική ίνα με το γυάλινο σκεδαστικό μέσο, ώστε να αξιολογηθεί η απόδοση των δύο υλικών ως προς την ιδιότητα του unpredictability τους.

Ακολουθώντας λοιπόν την μεθοδολογία της προηγούμενης παραγράφου, στο διάγραμμα α) του σχήματος 4.3 παρουσιάζεται η εξέλιξη του συντελεστή διασυσχέτισης Pearson για το καινούριο αυτό dataset, συναρτήσει της διαφοροποίησης iΔλ από το μήκος κύματος αναφοράς $λ_0$. Θα πρέπει να σημειωθεί ότι στο εν λόγω διάγραμμα έχει συμπεριληφθεί και μια αντίστοιχη καμπύλη 201 αποκρίσεων από την χρησιμοποιούμενη οπτική ίνα, ούτως ώστε να οπτικοποιηθεί η διαφορετική συμπεριφορά των δύο ανομοιογενών υλικών και να πραγματοποιηθεί ευκολότερα η ζητούμενη συγκριτική τους αξιολόγηση. Από την άλλη μεριά, στο διάγραμμα β) του ίδιου σχήματος επιδεικνύονται υπό τη μορφή ιστογραμμάτων οι κατανομές πιθανοτήτων για τις $_{201}C_2$ = 20100 Ευκλείδειες αποστάσεις που προέκυψαν από τις 201 εικόνες εκάστου dataset.

Όπως ήταν λοιπόν αναμενόμενο και από τα αποτελέσματα της προηγούμενης ενότητας, η πλήρης αποσυσχέτιση των speckle patterns που παράγονται μέσω της οπτικής ίνας εξασφαλίζεται σχεδόν άμεσα, για απόσταση μήκους κύματος από το $λ_0$ αναφοράς ίση με 2Δλ = 200pm. Αντίθετα, η εξέλιξη του συντελεστή διασυσχέτισης για τα speckle patterns από τον diffuser είναι ιδιαιτέρως πιο ομαλή, με την πλήρη αποσυσχέτιση των αποκρίσεων αυτού να επιτυγχάνεται οριακά για μεταβολή 20nm. Επομένως, με χρήση της παρούσας πειραματικής διάταξης, όπου οι εφαρμοζόμενες διεγέρσεις προκύπτουν από τη μεταβολή του μήκους κύματος της προσπίπτουσας δέσμης, η επίδοση του υπό μελέτη σκεδαστικού μέσου αποδεικνύεται σαφώς υποδεέστερη από αυτήν της οπτικής ίνας, καθώς η επαρκής

[8] Το πλήθος των συγκρίσεων που χρειάζεται να πραγματοποιηθούν ούτως ώστε να υπολογιστούν όλες οι Ευκλείδειες αποστάσεις ενός συνόλου δεδομένων μπορεί να προσδιοριστεί εκ των προτέρων μέσω του διωνυμικού συντελεστή $_nC_k = n!/[k!(n-k)!]$.

αποσυσχέτιση των αποκρίσεών του απαιτεί τουλάχιστον δύο τάξεις μεγέθους μεγαλύτερη Δλ.



Σχήμα 4.3: α) Ο συντελεστής διασυσχέτισης Pearson συναρτήσει της διαφοροποίησης του μήκους κύματος iΔλ της χρησιμοποιούμενης δέσμης ακτινοβολίας, όπου Δλ = 100pm. **β)** Οι Ευκλείδειες αποστάσεις των 201 πειραματικών speckle patterns που λήφθηκαν με Δλ = 100pm και για τα δύο υπό μελέτη ανομοιογενή υλικά.

Όσον αφορά τώρα το διάγραμμα του 4.3β, τα ιστογράμματα των Ευκλειδείων αποστάσεων που προέκυψαν από κάθε μελετούμενο υλικό έρχονται σε πλήρη συμφωνία με τα αντίστοιχα αποτελέσματα του συντελεστή διασυσχέτισης Pearson: ενώ η κατανομή της χρησιμοποιούμενης οπτικής ίνας παρουσιάζει την προσδοκώμενη gaussian μορφή της προηγούμενης ενότητας, οι αποκρίσεις του γυάλινου σκεδαστικού μέσου οδηγούν σε ένα σχετικά ομοιόμορφο ιστόγραμμα αποστάσεων με μεγάλο εύρος τιμών και κάτω άκρο που προσεγγίζει το μηδέν, επιβεβαιώνοντας την ιδιαιτέρως αυξημένη ομοιότητα των παραγόμενων speckle patterns του.

Συμπερασματικά, με χρήση της υπό μελέτη διάταξης, όπου οι εφαρμοζόμενες διεγέρσεις προκύπτουν από την μεταβολή του μήκους κύματος της προσπίπτουσας ακτινοβολίας, η επίδοση του χρησιμοποιούμενου diffuser, ως προς την ιδιότητα του unpredictability, αποδεικνύεται κατώτερη από την αντίστοιχη επίδοση μιας πολυμερικής οπτικής ίνας με τυχαίες ανομοιογένειες στις επιφάνειες εισόδου και εξόδου της. Καθώς λοιπόν η εν λόγω οπτική ίνα αποτελεί το πλέον ενδεδειγμένο υλικό που μπορεί να χρησιμοποιηθεί ως πηγή τυχαιότητας στο πλαίσιο της παρούσας διάταξης, οι ενότητες που ακολουθούν εστιάζουν αποκλειστικά στη συνολική αξιολόγηση της απόδοσης αυτής, τόσο στο επίπεδο των παραγόμενων speckle patterns της όσο και στο επίπεδο των δυαδικών ακολουθιών της.

4.3 Ευκλείδειες Αποστάσεις και Συντελεστές Διασυσχέτισης Pearson

Τα σύνολα αποκρίσεων που λήφθηκαν για την συνολική αξιολόγηση της οπτικής ίνας ως κεντρικό στοιχείο της παρούσας διάταξης, μπορούν να συνοψιστούν ως ακολούθως:

- Σύνολο δεδομένων Robustness $D_1 = \{r_i, c_j, p_k \mid 1 \le i \le 60, 1 \le j \le 3, k = 1\}$. Για την κατασκευή του συνόλου D_1 χρησιμοποιήθηκαν τρεις διαφορετικές διεγέρσεις c, οι οποίες εφαρμόστηκαν 60 συναπτές φορές σε μία μόνο οπτική ίνα p. Με άλλα λόγια, το σύνολο δεδομένων D_1 απαρτίζεται από 3 επιμέρους datasets εικόνων, κάθε ένα από τα οποία περιέχει 60 επαναληπτικές λήψεις μίας απόκρισης r που προκύπτουν από την επανειλημμένη εφαρμογή εκάστης διέγερσης στο ίδιο δείγμα.
- Σύνολο δεδομένων Unpredictability $D_2 = \{r_i, c_j, p_k \mid i = 1, 1 \le j \le 201, 1 \le k \le 10\}$. Το συγκεκριμένο σύνολο δεδομένων αποτελείται από 10 επιμέρους datasets με 201 αποκρίσεις r έκαστο, οι οποίες έχουν παραχθεί

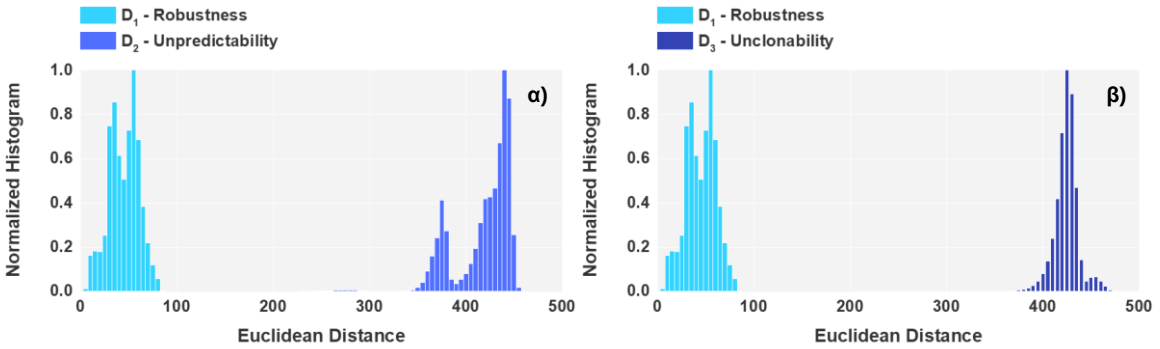
εφαρμόζοντας 201 διαφορετικά challenges c σε 10 οπτικές ίνες p από μία μόνο φορά.

- Σύνολο δεδομένων Unclonability $D_3 = \{r_i, c_j, p_k \mid i = 1,\ 1 \le j \le 11,\ 1 \le k \le 1007\}$. Το εν λόγω σύνολο εικόνων απαρτίζεται από 11 επιμέρους datasets με 1007 αποκρίσεις έκαστο, οι οποίες έχουν κατασκευαστεί εφαρμόζοντας 11 διαφορετικές διεγέρσεις c σε 1007 διαφορετικές οπτικές ίνες p από μία μόνο φορά.

Το πρώτο σκέλος της εν λόγω αξιολόγησης λοιπόν εστιάζει στην προκαταρκτική ανάλυση των άνωθεν πειραματικών δεδομένων μέσω δύο διαφορετικών μετρικών, της Ευκλείδειας απόστασης και του συντελεστή διασυσχέτισης Pearson, με σκοπό την ποσοτικοποίηση της ομοιότητας των διαθέσιμων speckle patterns εκάστου dataset. Η προκαταρκτική αυτή ανάλυση έλαβε χώρα ως ακολούθως: αρχικά όλες οι ληφθείσες πειραματικές μετρήσεις κανονικοποιήθηκαν σύμφωνα με την σχέση (3.8) του προηγούμενου κεφαλαίου. Κατόπιν, υπολογίστηκαν, για κάθε επιμέρους dataset ξεχωριστά, όλες οι Ευκλείδειες αποστάσεις των κανονικοποιημένων εικόνων, παράγοντας 3 ανεξάρτητα sets $_{60}C_2$ αποτελεσμάτων από το σύνολο δεδομένων D_1, 10 ανεξάρτητα sets $_{201}C_2$ αποτελεσμάτων από το σύνολο δεδομένων D_2 και 11 ανεξάρτητα sets $_{1007}C_2$ αποτελεσμάτων από το σύνολο δεδομένων D_3. Έπειτα, τα ανεξάρτητα αυτά sets αποτελεσμάτων ενοποιήθηκαν ανά μελετώμενη ιδιότητα, συγκροτώντας τελικά 3 συγκεντρωτικά σύνολα αποστάσεων, οι κατανομές των οποίων παρουσιάζονται υπό την μορφή κανονικοποιημένων ιστογραμμάτων στα γραφήματα του σχήματος 4.4.

Θα πρέπει να σημειωθεί ότι τα συγκεκριμένα ιστογράμματα επιδεικνύονται σε ζεύγη Robustness - Unpredictability και Robustness - Unclonability, ούτως ώστε να οπτικοποιηθεί η ύπαρξη μιας ενδεχόμενης αλληλοεπικάλυψής τους, η οποία, όπως έχει ήδη αναφερθεί, δύναται να οδηγήσει σε ψευδώς θετική ή αρνητική αυθεντικοποίηση αποκρίσεων. Η παρουσία της αναφερθείσας επικάλυψης, η οποία μάλιστα στην τρέχουσα περίπτωση δεν υφίσταται καν, μπορεί επιπλέον να επιβεβαιωθεί και από τους βασικούς στατιστικούς δείκτες των εν λόγω κατανομών που παρατίθενται στον πίνακα 2.

Ακολούθως, με πανομοιότυπο τρόπο εξήχθησαν και οι αντίστοιχες κατανομές του συντελεστή διασυσχέτισης Pearson, όπως αυτές παρουσιάζονται στα διαγράμματα του σχήματος 4.5, μαζί με τους βασικούς στατιστικούς τους δείκτες, οι οποίοι παρατίθενται στον πίνακα 3.



Σχήμα 4.4: Τα κανονικοποιημένα ζεύγη των συγκεντρωτικών κατανομών **α)** Robustness - Unpredictability και **β)** Robustness - Unclonability για όλες τις Ευκλείδειες αποστάσεις, όπως αυτές εξήχθησαν από έκαστο σύνολο πειραματικών δεδομένων.

Πίνακας 2: Οι στατιστικές τιμές των Ευκλειδείων αποστάσεων, όπως αυτές υπολογίστηκαν για κάθε διαθέσιμο σύνολο πειραματικών δεδομένων.

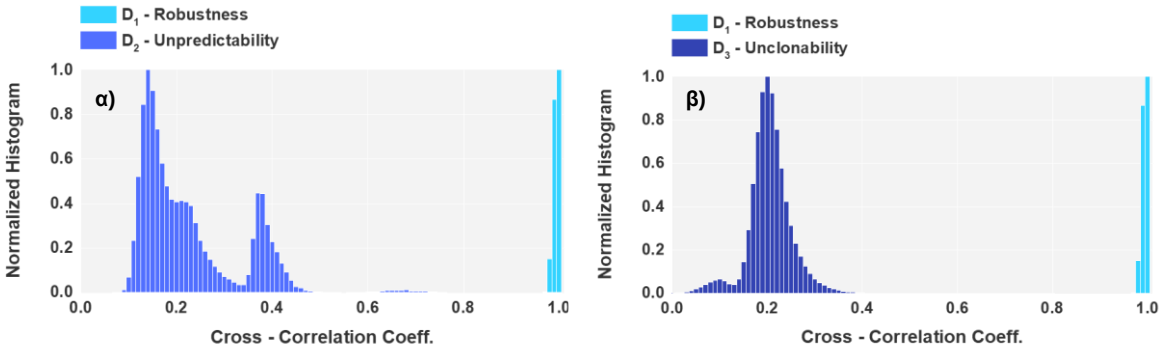
Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	9.57	86.97	47.32	15.41
D_2	231.84	462.81	420.19	30.93
D_3	213.67	509.72	427.22	12.78

Συνοψίζοντας, οι κατανομές του Robustness που επιδεικνύονται στα διαγράμματα των προαναφερθέντων σχημάτων, οι οποίες αντιπροσωπεύουν τις $3\times({}_{60}C_2)$ συγκρίσεις που έλαβαν χώρα κατά την ανάλυση του συνόλου δεδομένων D_1, ουσιαστικά επιτρέπουν την ποσοτικοποίηση της ανομοιότητας μεταξύ των επαναληπτικών λήψεων ενός speckle, προοικονομώντας την αξιοπιστία του υπό μελέτη συστήματος στο επίπεδο των δυαδικών ακολουθιών του. Παρομοίως, τα ιστογράμματα του Unpredictability και του Unclonability, τα οποία παριστάνουν $10\times({}_{201}C_2)$ και $11\times({}_{1007}C_2)$ συγκρίσεις από την ανάλυση των συνόλων D_2 και D_3 αντιστοίχως, ποσοτικοποιούν την ανομοιότητα των speckles που παράγονται υπό διαφορετικές συνθήκες ακτινοβόλησης ή από διαφορετικές οπτικές ίνες, παρέχοντας πληροφορίες για το επίπεδο ασφαλείας που δύναται να επιτευχθεί μετά την εφαρμογή της εκάστοτε συνάρτησης κατακερματισμού εικόνων.

Βάσει των παραπάνω αποτελεσμάτων λοιπόν μπορεί να εξαχθεί το εξής ακόλουθο τελικό συμπέρασμα: καθώς και τα 4 ζεύγη κατανομών που προέκυψαν από την εφαρμογή των δύο χρησιμοποιούμενων μετρικών δεν εμφανίζουν οποιαδήποτε επικάλυψη τιμών, τα speckle patterns που παράγονται υπό διαφορετικά challenges ή από διαφορετικές ίνες προκύπτουν επαρκώς ανόμοια ώστε η πιθανότητα να αναγνωριστούν εσφαλμένα ως τα θορυβικά ανάλογα μίας και μόνο απόκρισης να αναμένεται αμελητέα.

Πίνακας 3: Οι στατιστικές τιμές των συντελεστών διασυσχέτισης Pearson, όπως αυτές υπολογίστηκαν για κάθε διαθέσιμο σύνολο πειραματικών δεδομένων.

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	+0.9673	+0.9996	+0.9893	0.0063
D_2	+0.0736	+0.7675	+0.2322	0.1060
D_3	-0.1238	+0.8025	+0.2098	0.0472



Σχήμα 4.5: Τα κανονικοποιημένα ζεύγη των συγκεντρωτικών κατανομών **α)** Robustness - Unpredictability και **β)** Robustness - Unclonability για όλες τις τιμές των συντελεστών διασυσχέτισης Pearson, όπως αυτές εξήχθησαν από έκαστο σύνολο πειραματικών δεδομένων

4.4 Αποστάσεις Hamming και Πιθανότητες Ιδιοτήτων

Το δεύτερο και τελευταίο σκέλος της τρέχουσας αξιολόγησης εστιάζει στην ανάλυση των δυαδικών ακολουθιών που προέκυψαν από τα διαθέσιμα σύνολα δεδομένων D_1, D_2 και D_3 μέσω της τεχνικής RBM, η οποία αποτελεί και την βασική συνάρτηση κατακερματισμού εικόνων στο πλαίσιο της παρούσας εργασίας, λόγω

των μειωμένων υπολογιστικών της απαιτήσεων. Στις παραγράφους που ακολουθούν λοιπόν, παρουσιάζονται εν συντομία τόσο τα βήματα που εφαρμόστηκαν για την εξαγωγή των εν λόγω δυαδικών ακολουθιών όσο και τα κύρια αποτελέσματα που προέκυψαν από την στατιστική ανάλυσή τους.

Εν προκειμένω, αρχικά κατασκευάστηκαν 60 δυαδικές ακολουθίες μήκους 511 bits μέσω της τεχνικής RBM από κάθε ανεξάρτητο dataset του συνόλου δεδομένων D_1, θέτοντας μία εκ των διαθέσιμων πειραματικών αποκρίσεων ως εικόνα εγγραφής και θεωρώντας τις υπόλοιπες 59 ως εισόδους του σταδίου αυθεντικοποίησης. Η διαδικασία αυτή επαναλήφθηκε μέχρις ότου χρησιμοποιηθούν όλα τα speckles του εκάστοτε dataset ως εικόνα αναφοράς μια φορά, οδηγώντας σε 60 διαφορετικά σύνολα 60 δυαδικών ακολουθιών, κάθε ένα από τα οποία αντιστοιχεί και σε ένα μοναδικό σετ βοηθητικών δεδομένων.

Έπειτα για κάθε ένα από αυτά τα (3×60) sets των 60 ακολουθιών, προσδιορίστηκαν ξεχωριστά όλες οι αποστάσεις Hamming τους, οι οποίες κατόπιν συγκεντρώθηκαν σε ένα ενιαίο σύνολο αποτελεσμάτων που περιλαμβάνει συνολικά $(3\times60)\times({}_{60}C_2)$ τιμές.

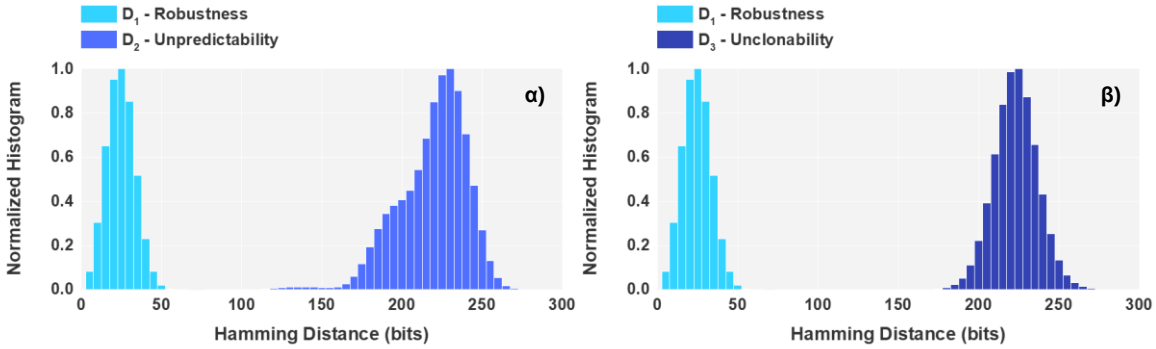
Εν συνεχεία, υπολογίστηκαν οι πιθανότητες του να προκύψουν πανομοιότυπες έξοδοι και από τα δύο στάδια του εφαρμοζόμενου fuzzy extractor και για κάθε δυνατή διορθωτική ικανότητα t του χρησιμοποιούμενου BCH, η οποία για μήκος δυαδικών ακολουθιών ίσο με n = 511 bits μπορεί να λάβει 57 διαφορετικές τιμές. Τέλος, προσδιορίστηκαν οι μέσοι όροι των (3×60) πιθανοτήτων που προέκυψαν ανά δυνατή τιμή διορθωτικής ικανότητας t, οδηγώντας στην ζητούμενη ποσοτικοποίηση της ιδιότητας του Robustness. Θα πρέπει να σημειωθεί ότι οι συγκεκριμένες πιθανότητες υπολογίστηκαν και με τους δύο εναλλακτικούς τρόπους που αναφέρονται στην υποενότητα 3.2.2: είτε με την απευθείας καταμέτρηση των δυαδικών εξόδων που προκύπτουν πανομοιότυπες και από τα δύο στάδια του fuzzy extractor, είτε προσεγγιστικά από τις CDF των αποστάσεων Hamming που παράχθηκαν από το εκάστοτε set ακολουθιών.

Στην συνέχεια εξήχθησαν οι δυαδικές ακολουθίες των εικόνων που απαρτίζουν τα σύνολα δεδομένων D_2 και D_3, ακολουθώντας ακριβώς την ίδια μεθοδολογία που εφαρμόστηκε επί του συνόλου D_1, προσδιορίστηκαν ομοίως όλες οι αποστάσεις Hamming μεταξύ των εν λόγω ακολουθιών και υπολογίστηκαν οι μέσοι όροι των αντίστοιχων πιθανοτήτων τους, οι οποίοι εν τέλει οδήγησαν και στην ποσοτικοποίηση των δύο εναπομεινάντων ιδιοτήτων, αυτές του Unpredictability και του Unclonability.

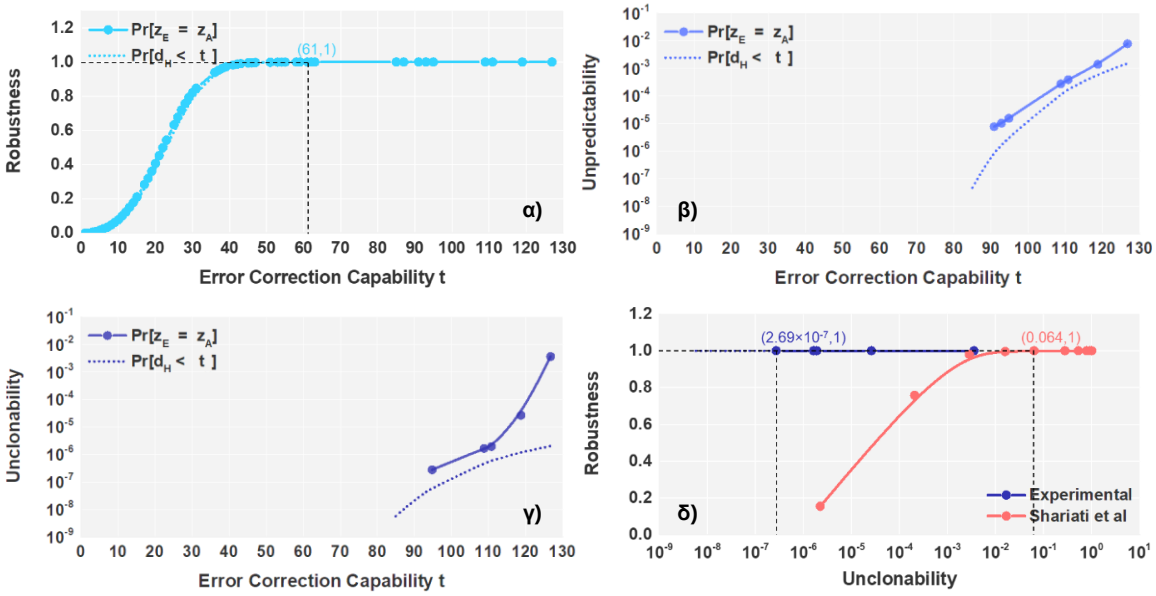
Πίνακας 4: Οι στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών μήκους 511 bits, οι οποίες εξήχθησαν μέσω της τεχνικής RBM από έκαστο σύνολο πειραματικών δεδομένων

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	0	61	23	7
D_2	80	298	217	15
D_3	72	321	221	14

Σε αυτό το πλαίσιο, στα διαγράμματα του σχήματος 4.6 παρουσιάζονται υπό την μορφή κανονικοποιημένων ιστογραμμάτων όλες οι συγκεντρωτικές κατανομές των αποστάσεων Hamming, όπως αυτές προέκυψαν από τις συγκρίσεις που πραγματοποιήθηκαν μεταξύ των ακολουθιών εκάστου συνόλου δεδομένων, ενώ στον πίνακα 4 παρατίθενται και οι αντίστοιχοι στατιστικοί τους δείκτες. Ακολούθως, στα γραφήματα α-γ του σχήματος 4.7 επιδεικνύονται οι μέσοι όροι των προαναφερθεισών πιθανοτήτων, ως συνάρτηση της διορθωτικής ικανότητας t.



Σχήμα 4.6: Τα κανονικοποιημένα ζεύγη των συγκεντρωτικών κατανομών **α)** Robustness - Unpredictability και **β)** Robustness - Unclonability για όλες τις αποστάσεις Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών μήκους 511 bits, οι οποίες εξήχθησαν μέσω της τεχνικής RBM από έκαστο σύνολο πειραματικών δεδομένων.



Σχήμα 4.7: Η μέση πιθανότητα του να προκύψουν πανομοιότυπες έξοδοι και από τα δύο στάδια του fuzzy extractor συναρτήσει της διορθωτικής ικανότητας t με δεδομένο μήκος δυαδικών ακολουθιών n= 511bits για **α)** τα δεδομένα του Robustness, **β)** τα δεδομένα του Unpredictability, **γ)** τα δεδομένα του Unclonability. Σε κάθε περίπτωση οι εν λόγω πιθανότητες προσδιορίστηκαν με δύο εναλλακτικούς τρόπους: είτε με την απευθείας καταμέτρηση των εξόδων που προκύπτουν πανομοιότυπες (συνεχής γραμμή με σημεία), είτε προσεγγιστικά από τις CDF των αποστάσεων Hamming (διακεκομμένη γραμμή). **δ)** Οι πιθανότητες του Robustness ως συνάρτηση των αντίστοιχων πιθανοτήτων Unclonability, όπως αυτές προέκυψαν από τα δεδομένα της παρούσας εργασίας μαζί με τα αντίστοιχα βιβλιογραφικά αποτελέσματα της [22]

Όπως μπορεί να παρατηρηθεί λοιπόν από τα αποτελέσματα της τρέχουσας ενότητας, η μέγιστη απόσταση Hamming που προέκυψε από το σύνολο δεδομένων D_1 ισούται με 61 bits. Η απόσταση αυτή, η οποία ουσιαστικά αντιπροσωπεύει και τον μέγιστο αριθμό των σφαλμάτων που παρουσιάζουν οι παραγόμενες ακολουθίες, λόγω του υπεισερχόμενου πειραματικού θορύβου, υποδεικνύει την ελάχιστη διορθωτική ικανότητα t του κώδικα BCH που πρέπει να εφαρμοστεί, προκειμένου να διασφαλιστεί η ζητούμενη επαναληψιμότητα του συστήματος. Καθώς μάλιστα η εν λόγω απόσταση έρχεται σε πλήρη αντιστοιχία με την τιμή της t, για την οποία η πιθανότητα του Robustness γίνεται ίση με την μονάδα στο σχήμα 4.7α, επιβεβαιώνεται εις διπλούν ότι, η σίγουρη αποκατάσταση των λαθών και η ορθή ανακατασκευή οποιασδήποτε ακολουθίας, επιτυγχάνεται μόνο όταν $t \geq 61$.

Στο σημείο αυτό κρίνεται σκόπιμο να υπογραμμιστεί ότι σύμφωνα με τον πίνακα 4, η ελάχιστη απόσταση Hamming του συνόλου δεδομένων D_1 δεν ξεπερνά τις

μέγιστες τιμές αποστάσεων που προέκυψαν από τα σύνολα D_2 και D_3. Συνεπώς, τα αντίστοιχα ζεύγη κατανομών τους, όπως αυτά παρουσιάζονται στα διαγράμματα του σχήματος 4.6, δεν εμφανίζουν οποιαδήποτε επικάλυψη τιμών καθιστώντας το προαναφερθέν ενδεχόμενο των ψευδώς θετικών ή αρνητικών αυθεντικοποιήσεων εξαιρετικά απίθανο. Το γεγονός αυτό επαληθεύεται και από τις γραφικές παραστάσεις 4.7β και 4.7γ, στις οποίες γίνεται εμφανές ότι ο κώδικας BCH με t = 61 αδυνατεί να διορθώσει τις διαφοροποιήσεις των ακολουθιών που παράχθηκαν από διαφορετικά challenges ή οπτικές ίνες, οδηγώντας σε μηδενικές τιμές πιθανοτήτων Unpredictability και Unclonability.

Όσον αφορά τώρα τις δύο εναλλακτικές μεθοδολογίες που χρησιμοποιήθηκαν για τον υπολογισμό των εν λόγω πιθανοτήτων, τα αποτελέσματα της προσεγγιστικής μεθόδου εμφανίζονται ελαφρώς υποεκτιμημένα σε σχέση με τις τιμές που προκύπτουν από την καταμέτρηση των πανομοιότυπων εξόδων, όπως αυτό ήταν άλλωστε αναμενόμενο. Η απόκλιση αυτή οφείλεται στο γεγονός ότι μια δυαδική ακολουθία με περισσότερα λάθη από την επιλεγμένη ικανότητα t του χρησιμοποιούμενου BCH μπορεί να οδηγήσει τυχαία σε ένα έγκυρο κωδικοποιημένο μήνυμα και συνεπώς να διορθωθεί εσφαλμένα.

Εν κατακλείδι, η συνολική απόδοση της παρούσας υλοποίησης αποδεικνύεται άκρως ικανοποιητική και ως προς τις 3 ιδιότητες μιας PUF. Εντούτοις, λόγω του περιορισμένου αριθμού από διαθέσιμα challenges, η εν λόγω υλοποίηση καθίσταται ιδιαιτέρως ευάλωτη απέναντι σε υπολογιστικές επιθέσεις εξάντλησης διεγέρσεων και επομένως η λειτουργία της ως γεννήτρια τυχαίων αριθμών δεν ενδείκνυται. Η λύση λοιπόν που προτείνεται για την συγκεκριμένη διάταξη είναι η χρησιμοποίηση της ως ένα σύστημα αυθεντικοποίησης μοναδιαίας απόκρισης, η απόδοση του οποίου εξαρτάται αποκλειστικά από τις ιδιότητες του Robustness και του Unclonability.

Σε αυτό το πλαίσιο, στην γραφική παράσταση 4.7δ παρουσιάζονται οι πιθανότητες του Robustness συναρτήσει των πιθανοτήτων Unclonability, όπως αυτές υπολογίστηκαν για κάθε δυνατή διορθωτική ικανότητα t του χρησιμοποιούμενου BCH. Στο ίδιο διάγραμμα έχει επίσης συμπεριληφθεί και η αντίστοιχη καμπύλη αποτελεσμάτων μιας παρεμφερούς οπτικής PUF, όπως αυτή μελετήθηκε με πανομοιότυπη μεθοδολογία από την Shalooma Shariati [22].

Όπως φαίνεται λοιπόν από και από το διάγραμμα 4.7δ, για πιθανότητα Robustness ίση με την μονάδα, δηλαδή με εξασφαλισμένη την ζητούμενη επαναληψιμότητα του εκάστοτε συστήματος, η πιθανότητα Unclonability που προέκυψε από τα δεδομένα της παρούσας εργασίας ισούται με 2.69×10^{-7}, ενώ η αντίστοιχη βιβλιογραφική πιθανότητα βρέθηκε ίση με 0.064. Με άλλα λόγια, η πιθανότητα να προκύψουν οι έξοδοι δύο διαφορετικών ινών ίδιες και από τα δύο στάδια του fuzzy extractor, προκύπτει 5 τάξεις μεγέθους μικρότερη από την αντίστοιχη πιθανότητα του συστήματος που εξετάζεται στην [22], καθιστώντας το παρόν σύστημα ιδιαιτέρως πιο ασφαλές .

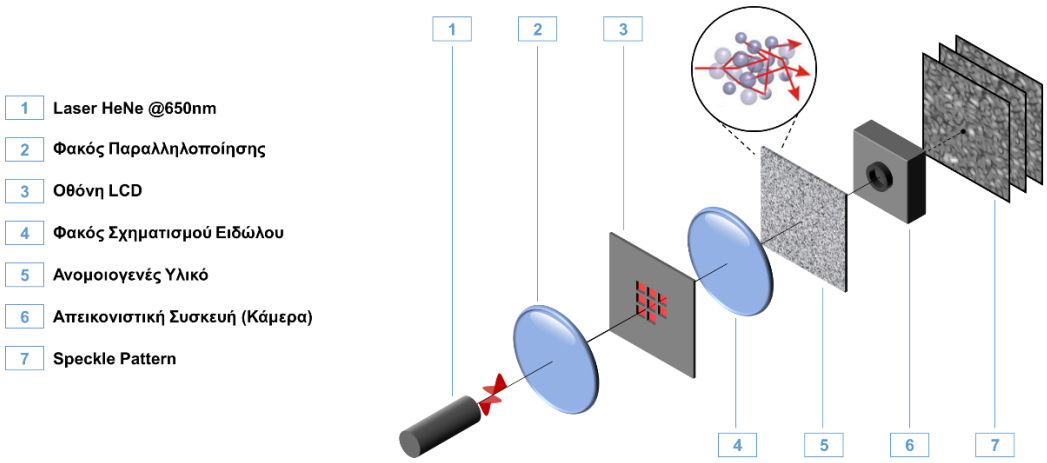
4.5 Συμπεράσματα

Ανακεφαλαιώνοντας τα περιεχόμενα του εν λόγω κεφαλαίου, η πρώτη υλοποίηση που πραγματοποιήθηκε στο πλαίσιο της παρούσας διδακτορικής εργασίας, σχεδιάστηκε ώστε να μελετηθεί εάν η μεταβολή Δλ του μήκους κύματος της χρησιμοποιούμενης δέσμης ακτινοβολίας αποτελεί την καταλληλότερη μέθοδο για την παραγωγή των απαιτούμενων διεγέρσεων ενός οπτικού συστήματος PUF. Τα κύρια ευρήματα της μελέτης αυτής συνοψίζονται ως εξής:

- Με τη τρέχουσα μέθοδο παραγωγής διεγέρσεων, το Unpredictability μιας POF με τυχαίες ανομοιογένειες στις επιφάνειες εισόδου και εξόδου της προκύπτει σαφώς ανώτερο από το αντίστοιχο Unpredictability ενός γυάλινου πλακιδίου διάχυσης φωτός, καθιστώντας το πρώτο εκ των δύο υλικών ως το καταλληλότερο οπτικό μέσο που μπορεί να χρησιμοποιηθεί στο πλαίσιο της παρούσας υλοποίησης.
- Η αύξηση της διαφοροποίησης Δλ μεταξύ δύο διαδοχικών challenges οδηγεί στην γρηγορότερη αποσυσχέτιση των καταγραφόμενων speckle patterns, ενισχύοντας το Unpredictability του μελετούμενου συστήματος, ανεξαρτήτως οπτικού μέσου. Ταυτοχρόνως όμως, η αύξηση αυτή περιορίζει σημαντικά τον συνολικό αριθμό των δυνατών διεγέρσεων, καθιστώντας το εν λόγω σύστημα ιδιαίτερα ευάλωτο σε υπολογιστικές επιθέσεις. Επομένως, η υλοποίηση του παρόντος κεφαλαίου μπορεί να χρησιμοποιηθεί με ασφάλεια μόνο ως σύστημα αυθεντικοποίησης μοναδιαίας απόκρισης, καθώς η λειτουργία της ως γεννήτρια τυχαίων αριθμών κρίνεται εν τέλει αρκετά επισφαλής, αφού η συγκεκριμένη μέθοδος παραγωγής διεγέρσεων δεν δύναται να οδηγήσει σε έναν επαρκή αριθμό από ασυσχέτιστες εξόδους.
- Με δεδομένη την στοχευόμενη χρήση της παρούσας οπτικής υλοποίησης ως ένα σύστημα αυθεντικοποίησης μοναδιαίας απόκρισης, η συνδυαστική απόδοση της POF, ως προς τις ιδιότητες του Robustness και του Unclonability της, βρέθηκε ότι υπερτερεί έναντι της αποδόσεως παρεμφερούς μελετηθέντος συστήματος, όπως αυτό εξετάστηκε στη σχετική βιβλιογραφία με πανομοιότυπο τρόπο [22].

5. ΠΕΙΡΑΜΑΤΙΚΗ ΔΙΑΤΑΞΗ ΜΕ ΟΘΟΝΗ LCD

Η δεύτερη πειραματική διάταξη που υλοποιήθηκε στο πλαίσιο της παρούσας διατριβής παρουσιάζεται στο σχήμα 5.1. Η διάταξη αυτή σχεδιάστηκε προκειμένου να δοκιμαστεί μια εναλλακτική μέθοδος ακτινοβόλησης των χρησιμοποιούμενων οπτικών μέσων και να διερευνηθεί η δυνατότητα επαύξησης του αριθμού των challenges μέσω αυτής.



Σχήμα 5.1: Πειραματική υλοποίηση οπτικής PUF με χρήση μιας οθόνης LCD για την παραγωγή των διεγέρσεων.

Εν συντομία, ως πηγή σύμφωνης ακτινοβολίας για την εν λόγω διάταξη χρησιμοποιείται ένα laser HeNe χωρίς σταθεροποιητή πόλωσης, το οποίο εκπέμπει στα 650nm. Η δέσμη εξόδου του [1] αρχικά διέρχεται μέσω ενός επιπεδόκυρτου φακού παραλληλοποίησης [2] και προσπίπτει σε μια οθόνη TFT LCD, διαστάσεων 34×56 mm, ανάλυσης 128×160 εικονοστοιχείων και χρωματικού βάθους 18 bits [3], από την οποία ακτινοβολείται μόνο ένα τετραγωνικό πλέγμα οκτώ εικονοστοιχείων. Οι 255 δυνατοί συνδυασμοί ενεργών και ανενεργών pixels από το πλέγμα αυτό, οι οποίοι αντιστοιχούν και στις απαιτούμενες διεγέρσεις του υπό μελέτη συστήματος, διαμορφώνουν το προφίλ έντασης της δέσμης, σχηματίζοντας ένα μοναδικό οπτικό μοτίβο. Το είδωλο του οπτικού μοτίβου εν συνεχεία προβάλλεται μέσω ενός αμφίκυρτου φακού [4] στην επιφάνεια του χρησιμοποιούμενου ανομοιογενούς μέσου [5], ουσιαστικά τροποποιώντας τα σημεία πρόσπτωσης του φωτός επί αυτού. Κατόπιν, το κεντρικό τμήμα της δέσμης που εξέρχεται από το ανομοιογενές μέσο προσπίπτει στον αισθητήρα μιας τυπικής CMOS web-camera [6], με πραγματική ανάλυση 480×640 pixels και μεγάλη διάσταση ~0.8cm, μέσω της οποίας καταγράφεται η ζητούμενη απόκριση του συστήματος, τελικής ανάλυσης 960×1280 pixels και χρωματικού βάθους 8 bits [7].

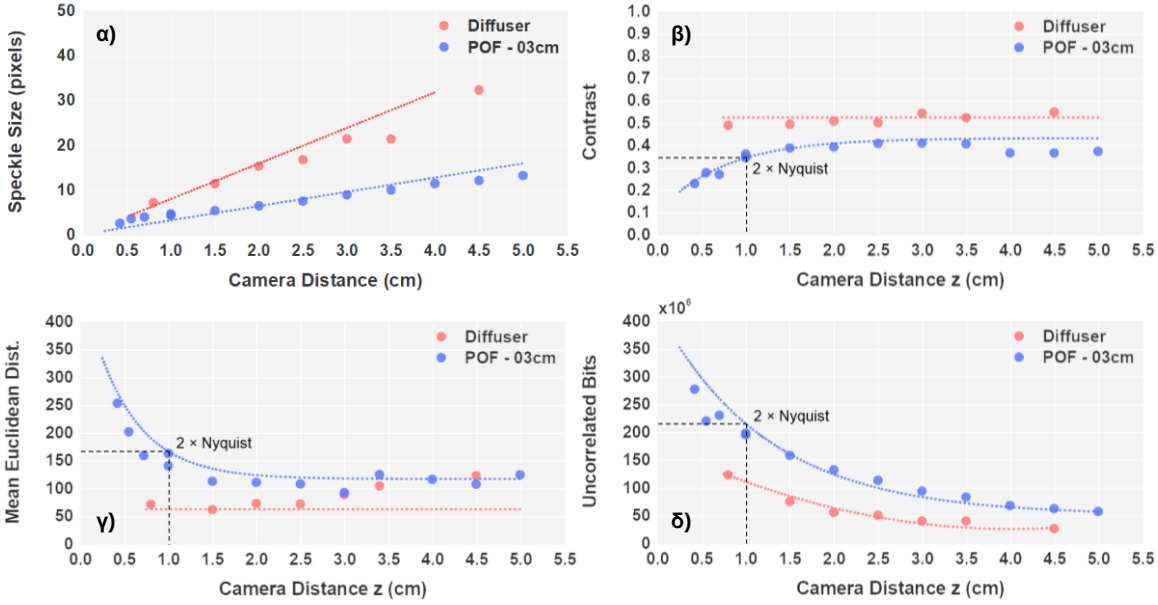
Θα πρέπει να σημειωθεί ότι στο πλαίσιο της παρούσας διάταξης ο έλεγχος της οθόνης LCD πραγματοποιήθηκε με έναν μικροελεγκτή Arduino, ενώ ο συντονισμός της συνολικής πειραματικής διαδικασίας διεξήχθη μέσω του περιβάλλοντος Matlab. Τα υπό μελέτη υλικά και σε αυτή την περίπτωση ήταν μία πολύτροπη πολυμερική οπτική ίνα βηματικού δείκτη διάθλασης, με πυρήνα 980μm, μήκος 3cm και τυχαίες ανομοιογένειες στις δύο επιφάνειες εισόδου/εξόδου της (unpolished POF), καθώς και ένα γυάλινο πλακίδιο διάχυσης φωτός με τυχαίες αυξομειώσεις στον μιγαδικό δείκτη διάθλασής του (diffuser).

5.1 Επίδραση του Μεγέθους των Speckles

Με χρήση της άνωθεν διάταξης αρχικά εξετάστηκε η επίδραση του μεγέθους των κηλίδων από τα speckles πάνω στην επαναληψιμότητα και την πολυπλοκότητα

των παραγόμενων μετρήσεων. Για τον σκοπό αυτό εφαρμόστηκε σε κάθε χρησιμοποιούμενο ανομοιογενές υλικό ένα και μοναδικό challenge 60 διαδοχικές φορές, μέσω του οποίου καταγράφηκε ένα ισοπληθές σύνολο από 60 όμοιες αποκρίσεις σε διάρκεια 10min. Η διαδικασία αυτή επαναλήφθηκε για διαφορετικές αποστάσεις της κάμερας από το εκάστοτε ανομοιογενές μέσο, διατηρώντας όλες τις υπόλοιπες πειραματικές συνθήκες σταθερές.

Στα ακόλουθα διαγράμματα λοιπόν, αποτυπώνονται τα σημαντικότερα αποτελέσματα που προέκυψαν από τις μετρήσεις αυτές. Συγκεκριμένα, στο διάγραμμα του σχήματος 5.2α παρουσιάζεται το μέγεθος των κηλίδων ενός speckle ως συνάρτηση της απόστασης που χωρίζει την κάμερα από το εκάστοτε ανομοιογενές υλικό, ενώ στη γραφική παράσταση 5.2β επιδεικνύεται η φωτοαντίθεση των speckles αυτών συναρτήσει της ίδιας απόστασης. Ακολούθως στο γράφημα του σχήματος 5.2γ αναπαριστάται η μέση τιμή των Ευκλειδείων αποστάσεων, όπως αυτές προσδιορίστηκαν μεταξύ των 60 διαθέσιμων πειραματικών εικόνων για κάθε απόσταση z ξεχωριστά, ενώ στο σχήμα 5.2δ παρουσιάζεται ο αριθμός των ασυσχέτιστων ψηφίων που περιέχει εκάστη εικόνα. Θα πρέπει να αναφερθεί ότι στα εν λόγω διαγράμματα έχουν συμπεριληφθεί με διακεκομμένες γραμμές και οι αντίστοιχες θεωρητικές καμπύλες που παράχθηκαν από ένα σύνολο κατάλληλων προσομοιώσεων, για την διεξαγωγή των οποίων θεωρήθηκε μια απόλωτη δέσμη φωτός με μήκος κύματος 650nm. Σε κάθε περίπτωση, το μέγεθος των κόκκων από τα speckles προσδιορίστηκε μέσω του FWHM της συνάρτησης αυτοσυσχετίσεως τους.



Σχήμα 5.2: α) Μέγεθος κηλίδων και **β)** φωτοαντίθεση των speckle patterns ως συνάρτηση της απόστασης που διαχωρίζει την απεικονιστική κάμερα από το υπό μελέτη οπτικό μέσο. **γ)** Μέση τιμή των Ευκλειδείων αποστάσεων, όπως αυτές υπολογίστηκαν μεταξύ των εξήντα εικόνων που λήφθηκαν υπό πανομοιότυπες πειραματικές συνθήκες για κάθε απόσταση. **δ)** Πλήθος ασυσχέτιστων ψηφίων των speckle patterns ως συνάρτηση της ίδιας απόστασης. Σε κάθε περίπτωση, τα σημεία των παρουσιαζόμενων διαγραμμάτων αντιστοιχούν σε πειραματικά αποτελέσματα, ενώ οι διακεκομμένες γραμμές στα θεωρητικά που προέκυψαν με χρήση του αριθμητικού μοντέλου.

Όπως φαίνεται λοιπόν και από το διάγραμμα 5.2α, όσο η κάμερα απομακρύνεται από το χρησιμοποιούμενο υλικό το μέγεθος των κόκκων των speckles αυξάνεται, εμφανίζοντας μια γραμμική εξάρτηση από την απόσταση z όπως ήταν άλλωστε αναμενόμενο. Από την άλλη πλευρά, η διαφορά των κλίσεων που παρατηρείται μεταξύ των δύο δειγμάτων μπορεί να αποδοθεί στη διαφορετική διάμετρο της δέσμης κατά την έξοδό της από αυτά, καθώς κατά την διάδοσή της εντός του

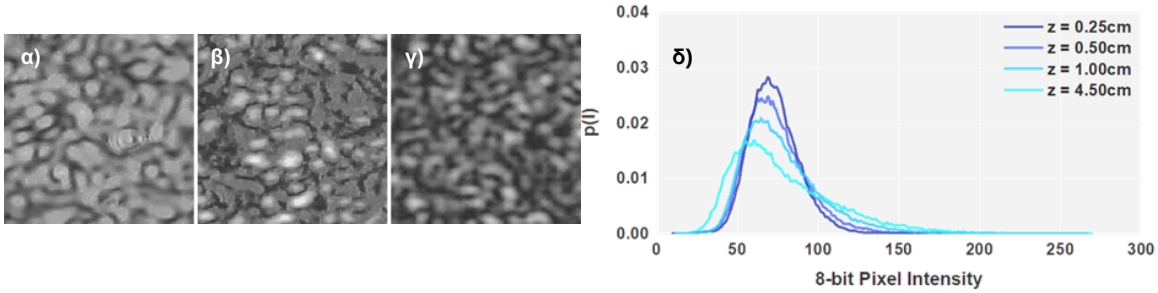
diffuser αυτή διευρύνεται σημαντικά. Στο γεγονός αυτό οφείλονται και οι μεγαλύτερες κηλίδες που σχηματίζονται με χρήση του diffuser, σε σχέση με αυτές που παράγονται από την POF ακόμη και για πανομοιότυπες αποστάσεις της κάμερας. Εντούτοις, όλες οι εικόνες ανεξαιρέτως ξεπερνούν το όριο δειγματοληψίας κατά Nyquist, παρουσιάζοντας πάντα μέγεθος κηλίδων μεγαλύτερο από 2 εικονοστοιχεία ανά διάσταση.

Όσον αφορά τώρα το σχήμα 5.2β, τα speckle patterns που παράγονται από την POF για αποστάσεις εγγύτερες του 1cm, εμφανίζουν κόκκο μικρότερο των 4 pixels (2×Nyquist) και χαρακτηρίζονται από μια γραμμικά αυξανόμενη φωτοαντίθεση, η οποία στην συνέχεια σταθεροποιείται γύρω από την τιμή 0.39. Η συμπεριφορά αυτή συμφωνεί πλήρως με τα αποτελέσματα που προέκυψαν από το χρησιμοποιούμενο αριθμητικό μοντέλο, αλλά και με τα ανάλογα ευρήματα της αντίστοιχης βιβλιογραφίας [73]. Αντιθέτως, τα speckles που προέρχονται από τον diffuser είναι όλα μεγαλύτερα από τέσσερα pixels ανά διάσταση, με την τιμή της φωτοαντίθεσής τους να παραμένει σταθερή και ίση με 0.52 για όλο το εύρος των εξεταζόμενων αποστάσεων.

Στο σημείο αυτό θα πρέπει να υπενθυμιστεί ότι καθώς η φωτοαντίθεση ενός speckle είναι αντιστρόφως ανάλογη του αντίστοιχου SNR της, η απόκλιση αυτής από την αναμενόμενη θεωρητική τιμή $1/\sqrt{2}$ υποδηλώνει την ύπαρξη αυξημένου μετρητικού θορύβου, ο οποίος υποβιβάζει την ποιότητα των καταγραφόμενων εικόνων και υποβαθμίζει την συνολική επαναληψιμότητα του υπό μελέτη συστήματος. Συνεπώς, βάσει των ανωτέρω γραφικών συνεπάγεται ότι η μεγιστοποιημένη καταστολή του θορύβου παρατήρησης επιτυγχάνεται όταν η απόσταση μεταξύ της απεικονιστικής συσκευής και του εκάστοτε ανομοιογενούς μέσου είναι τέτοια, ώστε το μέγεθος των ληφθέντων speckles να είναι το λιγότερο ίσο με 4 pixels ανά διάσταση. Τέλος, οι μέγιστες τιμές φωτοαντίθεσης εκάστου δείγματος, οι οποίες ισούνται με 0.52 για τον diffuser και 0.39 για την POF αντιστοίχως, υποδεικνύουν ότι οι μετρήσεις που προέρχονται από τον γυάλινο σκεδαστή έχουν μεγαλύτερο SNR έναντι των εικόνων που προκύπτουν από την οπτική ίνα, υποδηλώνοντας την αυξημένη ευκρίνεια των αποκρίσεών του, τη μεγαλύτερη σταθερότητά του συναρτήσει του χρόνου και γενικά την ανώτερη επίδοση αυτού από άποψη robustness.

Εν γένει, τα άνωθεν συμπεράσματα, όπως αυτά εξήχθησαν από την ερμηνεία των τιμών φωτοαντίθεσης, βρίσκονται σε καλή συμφωνία με τα αποτελέσματα που προέκυψαν και από την συμπεριφορά των αντιστοίχων Ευκλειδείων αποστάσεων. Ωστόσο, από την σύγκριση των δύο διαγραμμάτων ανακύπτουν ορισμένες διαφοροποιήσεις, οι οποίες μπορούν να συνοψιστούν ακολούθως: οι Ευκλείδειες αποστάσεις των εικόνων που παράγονται από την POF αρχικά ελαττώνονται όσο η κάμερα απομακρύνεται από την έξοδο αυτής. Εντούτοις, οι τιμές τους παγιώνονται για αποστάσεις μεγαλύτερες του 1.5cm έναντι του 1cm που προέκυψε από την αντίστοιχη ανάλυση της φωτοαντίθεσης και για μέγεθος κηλίδων, το οποίο ξεπερνά τα 6 pixels ανά διάσταση (3×Nyquist). Από την άλλη πλευρά, ο diffuser παρουσιάζει μια απροσδόκητη αύξηση Ευκλειδείων αποστάσεων για $z > 3$cm και μεγέθη κόκκων άνω των 16 εικονοστοιχείων (8×Nyquist), η οποία μπορεί να αποδοθεί στη μείωση της έντασης της προσπίπτουσας ακτινοβολίας επί του χρησιμοποιούμενου αισθητήρα, γεγονός που οδηγεί στην αυτόματη αύξηση του bias από το ίδιο το firmware της webcam και, συνακολούθως, στην αύξηση του παραγόμενου θορύβου στις καταγραφόμενες λήψεις. Το φαινόμενο αυτό, καθώς δεν έχει ληφθεί καθόλου υπόψιν στην υλοποίηση του αριθμητικού μοντέλου, δεν κατέστη εφικτό και να προβλεφθεί.

Τέλος, στο διάγραμμα του σχήματος 5.2δ όπως έχει ήδη αναφερθεί, αναπαριστάται ο αριθμός των ασυσχέτιστων bits ενός speckle ως συνάρτηση της απόστασης z, ο οποίος υπολογίζεται από την σχέση $N_{bits} = N \times H/S$, όπου S το μέγεθος των κηλίδων του speckle, H η εντροπία Shannon του speckle και N ο συνολικός αριθμός από τα pixels του speckle [74]. Όταν λοιπόν το μέγεθος των κόκκων αυξάνει, η εντροπία Shannon ενός speckle pattern ενισχύεται, αφού η p(I) των εντάσεών του διευρύνεται (σχήμα 5.3γ). Ταυτόχρονα όμως, η πληροφορία που εμπεριέχεται σε αυτό φθίνει, καθώς ολοένα και περισσότερα pixels ομαδοποιούνται σε μικρότερο αριθμό κηλίδων, οδηγώντας στην ελάττωση του πλήθους των ασυσχέτιστων ψηφίων του. Με άλλα λόγια, όσο η απεικονιστική κάμερα απομακρύνεται από την έξοδο του χρησιμοποιούμενου μέσου και το μέγεθος των κηλίδων ενός speckle ελαττώνεται, ο όγκος της ασυσχέτιστης πληροφορίας που μπορεί να εξαχθεί από αυτό μειώνεται. Για να αποφευχθεί λοιπόν η εν λόγω μείωση, το μέγεθος των κόκκων ενός speckle πρέπει να τίθεται όσο το δυνατόν μικρότερο.



Σχήμα 5.3: Πειραματικές αποκρίσεις προερχόμενες από **α)** την POF για z = 5.00cm και από **β)** τον diffuser για z = 1.50cm μαζί με **γ)** το αντίστοιχο υπολογιστικό αποτέλεσμα του δεύτερου, όπως αυτό προέκυψε από το χρησιμοποιούμενο αριθμητικό μοντέλο. Όλα τα παρουσιαζόμενα speckles χαρακτηρίζονται από κηλίδες 12 εικονοστοιχείων ανά διάσταση. **δ)** Συνάρτηση πυκνότητας πιθανότητας των εντάσεων από υπολογιστικά speckles, τα οποία έχουν κατασκευαστεί για διάφορες αποστάσεις z της κάμερας από την έξοδο της POF.

Εν κατακλείδι, βάσει των ανωτέρω αποτελεσμάτων εξάγεται το συμπέρασμα ότι για να ελαχιστοποιηθεί η επίδραση του θορύβου και να ενισχυθεί το robustness οποιουδήποτε συστήματος PUF με την ελάχιστη δυνατή απώλεια πληροφορίας, το μέγεθος των κηλίδων από τα speckles που παράγονται θα πρέπει να καταλαμβάνει περίπου 6 εικονοστοιχεία ανά διάσταση.

5.2 Σύγκριση Απόδοσης Οπτικών Μέσων

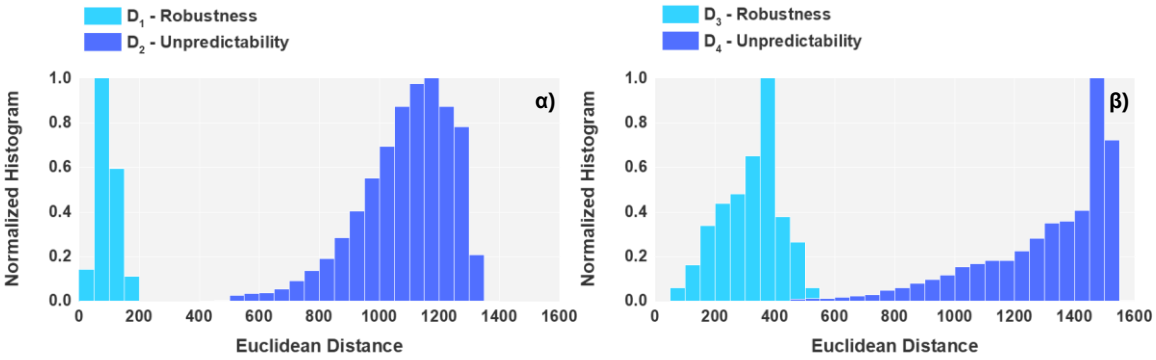
Το δεύτερο σκέλος της παρούσας διερεύνησης εστιάζεται στην αξιολόγηση της επίδοσης που επιδεικνύει η περιγραφείσα διάταξη ως ένα ολοκληρωμένο σύστημα PUF και στον εντοπισμό του πλέον ενδεδειγμένου υλικού, το οποίο παρουσιάζει τη βέλτιστη απόδοση robustness και unpredictability ταυτοχρόνως. Σε αυτό το πλαίσιο λοιπόν, λήφθηκαν 4 διαφορετικά σύνολα από speckle patterns, οι κηλίδες των οποίων καλύπτουν περίπου 36 εικονοστοιχεία των καταγραφόμενων εικόνων, όπως αυτό επιβάλλεται από τα ευρήματα της προηγούμενης ενότητας.

Αναλυτικότερα, το πρώτο σύνολο δεδομένων D_1 περιλαμβάνει 60 διαδοχικές λήψεις της ίδιας απόκρισης r, οι οποίες προέκυψαν εφαρμόζοντας μία και μοναδική διέγερση c σε έναν μόνο diffuser p για 10min: $D_1 = \{r_i, c_j, p_k \mid 1 \leq i \leq 60, j = 1, k = 1\}$, όπου $r_i \in \mathbb{R}^{N1 \times N2}$ με $N_1 = 960$ και $N_2 = 1280$. Το εν λόγω σύνολο ουσιαστικά περιέχει όλες τις μετρήσεις που χρειάζονται από τον diffuser για να ποσοτικοποιηθεί η επίδραση του θορύβου επί των speckles αυτού και να μελετηθεί η επαναληψιμότητα των δυαδικών ακολουθιών του. Από την άλλη μεριά, το δεύτερο σύνολο δεδομένων D_2 περιέχει 255 διαφορετικές αποκρίσεις r, οι οποίες παράχθηκαν εφαρμόζοντας κάθε διαθέσιμο challenge c μία μόνο φορά σε ένα και

μοναδικό diffuser p: $D_2 = \{r_i, c_j, p_k \mid i = 1, \leq j \leq 255, k = 1\}$. Το σύνολο αυτό περιλαμβάνει όλες τις εικόνες των speckles που απαιτούνται από τον diffuser, ώστε να αξιολογηθεί η χρησιμοποιούμενη μέθοδος για την παραγωγή των διεγέρσεων και να ποσοτικοποιηθεί η μοναδικότητα των δυαδικών ακολουθιών που προκύπτουν από αυτή. Ομοίως ορίζονται και τα δύο υπόλοιπα σύνολα δεδομένων D_3 και D_4, τα οποία λήφθηκαν με πανομοιότυπο τρόπο αντικαθιστώντας απλά τον diffuser με την POF.

5.2.1 Ευκλείδειες Αποστάσεις και Συντελεστές Διασυσχέτισης Pearson

Στα ιστογράμματα του σχήματος 5.4 αναπαριστώνται γραφικά οι Ευκλείδειες αποστάσεις μεταξύ όλων των κανονικοποιημένων μετρήσεων εκάστου dataset, με τις αντίστοιχες κατανομές τους να έχουν ομαδοποιηθεί ανά ζεύγη για κάθε οπτικό μέσο. Ειδικότερα, οι κατανομές robustness αντιπροσωπεύουν $_{60}C_2 = 1770$ συγκρίσεις, όπως αυτές πραγματοποιήθηκαν μεταξύ των επαναλήψεων που απαρτίζουν τα σύνολα D_1 και D_3, ενώ οι κατανομές unpredictability παριστάνουν $_{255}C_2 = 32385$ συγκρίσεις από τις 255 διαφορετικές αποκρίσεις των συνόλων D_2 και D_4. Στο πίνακα 5 συνοψίζονται και τα βασικά στατιστικά μέτρα των κατανομών αυτών.



Σχήμα 5.4: Οι κατανομές των Ευκλειδείων αποστάσεων για **α)** το ανομοιογενές σκεδαστικό μέσο και **β)** την POF, όπως αυτές εξήχθησαν από τα 60 speckle patterns που λήφθηκαν υπό πανομοιότυπες συνθήκες ακτινοβόλησης (robustness) και τα 255 speckle patterns που προέκυψαν εφαρμόζοντας όλες τις διαθέσιμες πειραματικές διεγέρσεις (unpredictability).

Όπως φαίνεται λοιπόν και από τα εν λόγω διαγράμματα, οι αποκρίσεις του συνόλου D_3, οι οποίες έχουν παραχθεί από την POF, παρουσιάζουν αυξημένη ανομοιότητα έναντι των speckles που προέρχονται από τον γυάλινο σκεδαστή, αφού η κατανομή των αντιστοίχων Ευκλειδείων αποστάσεών τους χαρακτηρίζεται από μεγαλύτερη μέση τιμή και πλατύτερο εύρος. Η αυξημένη αυτή ανομοιότητα υποδηλώνει την μικρότερη ανοχή της ίνας απέναντι στον περιβαλλοντικό θόρυβο, η οποία ενισχύει αναλόγως και τη μοναδικότητα των εικόνων που προκύπτουν από τις διαφορετικές εφαρμοζόμενες διεγέρσεις. Εντούτοις, λόγω της ιδιαιτέρως χαμηλής σταθερότητας, τα δύο ιστογράμματα της POF αλληλεπικαλύπτονται, γεγονός που καθιστά πιθανή την ύπαρξη ψευδά αρνητικών ή θετικών αποτελεσμάτων. Με άλλα λόγια, αποκρίσεις οι οποίες παράγονται από δύο διαφορετικές διεγέρσεις και εμπίπτουν εντός της αναφερθείσας επικάλυψης, οδηγούν σε τόσο συναφείς ακολουθίες που μετά τη διόρθωση των λιγοστών διαφορών τους, αντιστοιχίζονται εσφαλμένα στην ίδια τελική δυαδική έξοδο. Ομοίως, οι επαναλαμβανόμενες λήψεις του ίδιου speckle που ανήκουν σε αυτή την επικάλυψη οδηγούν σε δυαδικές ακολουθίες οι οποίες εμπεριέχουν τόσα πολλά λάθη, ώστε να εκλαμβάνονται ως αποκρίσεις δύο διαφορετικών διεγέρσεων.

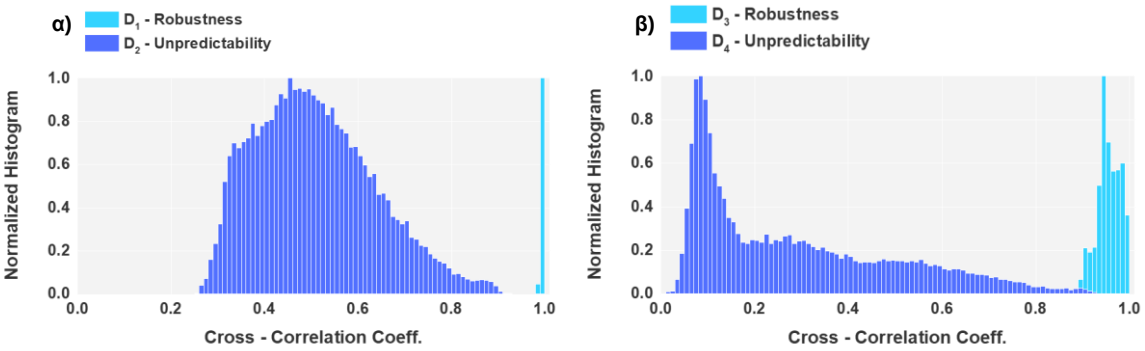
Αντίθετα, οι κατανομές των robustness και unpredictability για τον diffuser είναι ξεκάθαρα διακριτές και σαφώς διαχωρισμένες, γεγονός που καθιστά τον γυάλινο σκεδαστή το πιο κατάλληλο οπτικό μέσο για την υπό μελέτη διάταξη.

Πίνακας 5: Στατιστικές τιμές των Ευκλειδείων αποστάσεων, όπως αυτές υπολογίστηκαν μεταξύ των αποκρίσεων του diffuser και της POF.

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	32.8	195.7	92.0	34.0
D_2	432.1	1352.4	1087.1	154.7
D_3	67.2	533.9	318.1	98.6
D_4	395.0	1720.3	1306.3	220.6

Κατόπιν, στα γραφήματα του σχήματος 5.5 απεικονίζονται οι συντελεστές διασυσχέτισης Pearson μεταξύ των ίδιων μετρήσεων, ενώ στον πίνακα 6 συνοψίζονται οι αντίστοιχες στατιστικές τους τιμές, από τις οποίες εξάγονται πανομοιότυπα συμπεράσματα με αυτά των Ευκλειδείων αποστάσεων.

Σε αυτό το σημείο κρίνεται σκόπιμο να αναφερθεί ότι κατά την διεξαγωγή των εν λόγω πειραμάτων παρατηρήθηκε πως όταν το ποσοστό των κοινών εικονοστοιχείων μεταξύ δυο διεγέρσεων μεγαλώνει, ο συντελεστής διασυσχέτισης των αντιστοίχων speckles τους αυξάνεται. Για παράδειγμα μία απόκριση που σχηματίζεται από δύο ενεργά pixels επί της LCD παρουσιάζει ένα ικανό πλήθος αμοιβαίων κηλίδων με τα speckles που προέρχονται από έκαστο μεμονωμένο pixel ξεχωριστά. Ταυτόχρονα όμως όσο το ποσοστό των κοινών εικονοστοιχείων μειούται με την επιφάνεια ακτινοβόλησης να ελαττώνεται, τόσο αυξάνεται και η επίδραση του μετρητικού θορύβου, η οποία εντείνεται ιδιαιτέρως στην περίπτωση της οπτικής ίνας λόγω της μεγαλύτερης μηχανικής αστάθειάς της. Σε αυτή την μεγαλύτερη μηχανική αστάθεια οφείλεται και η έντονη ασυμμετρία του ιστογράμματος D_4, η οποία χαμηλώνει μεν τον μέσο όρο και την επικρατούσα τιμή της αντίστοιχης κατανομής αλλά δεν κατορθώνει να αντισταθμίσει την υψηλή ομοιότητα των αποκρίσεων που παράγονται από διεγέρσεις με μεγάλο ποσοστό κοινών pixels.



Σχήμα 5.5: Οι κατανομές των συντελεστών διασυσχέτισης Pearson για α) το ανομοιογενές σκεδαστικό μέσο και β) την POF, όπως αυτές εξήχθησαν από τα 60 speckles που λήφθηκαν υπό πανομοιότυπες συνθήκες ακτινοβόλησης (robustness) και τα 255 speckle patterns που προέκυψαν εφαρμόζοντας όλες τις διαθέσιμες πειραματικές διεγέρσεις (unpredictability).

Πίνακας 6: Στατιστικές τιμές των συντελεστών διασυσχέτισης Pearson, όπως αυτές υπολογίστηκαν μεταξύ των αποκρίσεων της POF και του σκεδαστικού μέσου

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	+0.9844	+0.9996	+0.9961	0.0029
D_2	+0.2568	+0.9240	+0.5094	0.1287
D_3	+0.8840	+0.9982	+0.9549	0.0247
D_4	-0.2042	+0.9365	+0.2859	0.2117

Συνεπώς, βάσει των άνωθεν παρατηρήσεων μπορεί να εξαχθεί το ακόλουθο πρωταρχικό συμπέρασμα: η παρούσα τεχνική ακτινοβόλησης εκ πρώτης όψεως

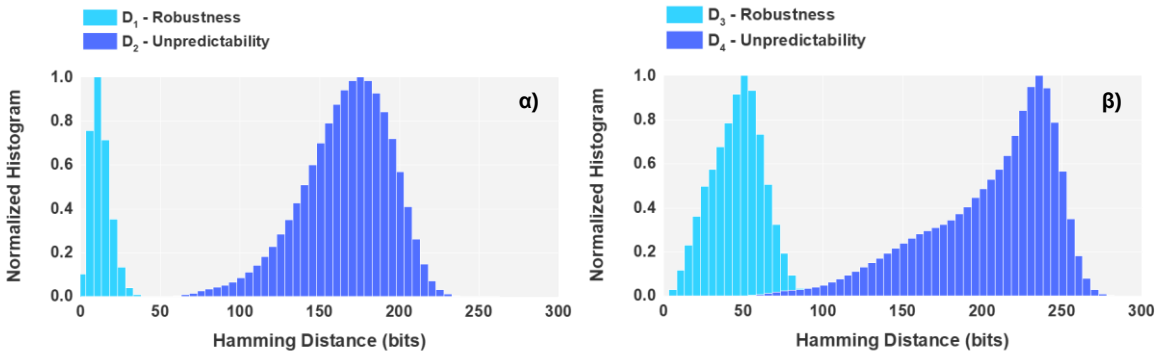
θεωρείται πλήρως ακατάλληλη για την παραγωγή των ζητούμενων διεγέρσεων μιας PUF καθώς, ως έχει, αδυνατεί να οδηγήσει σε αρκούντως ασυσχέτιστα speckles, ανεξαρτήτως οπτικού μέσου. Η αύξηση όμως της επιφάνειας του γυάλινου σκεδαστή [24] σε συνδυασμό με την χρήση μεγαλύτερου πλέγματος από pixels κατά την κατασκευή των challenges ενδέχεται να επιτρέψει την μείωση του ποσοστού των κοινών ενεργών εικονοστοιχείων, χωρίς την ανεπανόρθωτη υποβάθμιση της επαναληψιμότητας. Εντούτοις, η εναλλακτική αυτή λύση μπορεί να εφαρμοστεί ικανοποιητικά μόνο για την περίπτωση του diffuser, καθώς η επιφάνεια ακτινοβόλησης της ίνας περιορίζεται από το εκάστοτε μέγεθος του πυρήνα της.

5.2.2 Αποστάσεις Hamming και Πιθανότητες Ιδιοτήτων

Για την ολοκληρωμένη αξιολόγηση της παρούσας διάταξης, εν συνεχεία διερευνήθηκε η ποιότητα των δυαδικών ακολουθιών, όπως αυτές εξάγονται από τα 4 προαναφερθέντα σύνολα δεδομένων, μέσω της τεχνικής RBM.

Συγκεκριμένα, από το σύνολο δεδομένων D_1 κατασκευάστηκαν 60 δυαδικές ακολουθίες μήκους 511 bits, θέτοντας μία εκ των διαθέσιμων πειραματικών αποκρίσεων ως εικόνα εγγραφής και θεωρώντας τις υπόλοιπες 59 ως εισόδους του σταδίου αυθεντικοποίησης. Η διαδικασία αυτή επαναλήφθηκε μέχρις ότου χρησιμοποιηθούν όλα τα speckles ως εικόνα αναφοράς μια φορά, οδηγώντας σε 60 διαφορετικά σύνολα δυαδικών ακολουθιών, κάθε ένα από τα οποία αντιστοιχεί και σε ένα μοναδικό σετ βοηθητικών δεδομένων. Έπειτα, προσδιορίστηκαν οι αποστάσεις Hamming μεταξύ των δυαδικών ακολουθιών για κάθε σύνολο ξεχωριστά και υπολογίστηκαν οι πιθανότητες να προκύψουν πανομοιότυποι έξοδοι και από τα δύο στάδια του fuzzy extractor. Με τον ίδιο ακριβώς τρόπο παράχθηκαν 60 σύνολα 60 δυαδικών ακολουθιών από το dataset D_3, και 255 διαφορετικά σύνολα 255 δυαδικών ακολουθιών από τα datasets D_2 και D_4 αντιστοίχως.

Εν προκειμένω στα γραφήματα του σχήματος 5.6 παρουσιάζονται συγκεντρωμένες όλες οι αποστάσεις Hamming που υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών εκάστου συνόλου, με τις αντίστοιχες κατανομές τους να έχουν ομαδοποιηθεί ανά ζεύγη για κάθε δείγμα. Αναλυτικότερα, οι κατανομές του robustness απεικονίζουν ($60 \times {}_{60}C_2$) συγκρίσεις, όπως αυτές πραγματοποιήθηκαν μεταξύ των δυαδικών ακολουθιών που παράχθηκαν από τα σύνολα D_1 και D_3, ενώ οι κατανομές του unpredictability αντιπροσωπεύουν ($255 \times {}_{255}C_2$) συγκρίσεις από τις ακολουθίες των συνόλων D_2 και D_4 αντιστοίχως. Στον πίνακα 7 συνοψίζονται και οι βασικές στατιστικές τιμές αυτών των κατανομών.



Σχήμα 5.6: Οι κατανομές των αποστάσεων Hamming μεταξύ όλων των δυαδικών ακολουθιών, μήκους 511 bits, όπως αυτές προέκυψαν μέσω της τεχνικής RBM για τα δεδομένα **α)** του γυάλινου σκεδαστικού μέσου και **β)** της POF αντιστοίχως.

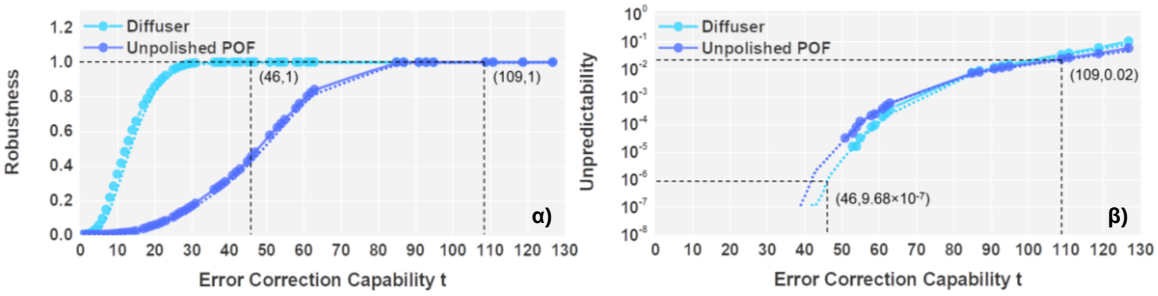
Ακολούθως, στα διαγράμματα του σχήματος 5.7 αναπαριστώνται οι πιθανότητες του να προκύψουν οι ίδιες δυαδικές έξοδοι και από τα δύο στάδια του fuzzy extractor. Θα πρέπει να σημειωθεί ότι οι πιθανότητες αυτές, οι οποίες

ποσοτικοποιούν τις ζητούμενες ιδιότητες του robustness και του unpredictability, υπολογίστηκαν για κάθε δυνατή διορθωτική ικανότητα t του BCH κώδικα με δύο διαφορετικούς τρόπους: είτε με απευθείας σύγκριση των παραγόμενων εξόδων, είτε προσεγγιστικά από το ιστόγραμμα των προαναφερθέντων αποστάσεων Hamming.

Πίνακας 7: Στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών της POF και του σκεδαστικού μέσου που παράχθηκαν μέσω της τεχνικής RBM.

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	0	45	13.7	6.2
D_2	41	263	167.7	27.8
D_3	2	104	47.5	16.1
D_4	38	320	206.6	40.2

Εν συντομία, τα ιστογράμματα των αποστάσεων hamming, όπως αυτά αποτυπώνονται στα διαγράμματα του σχήματος 5.6, βρίσκονται σε καλή συμφωνία με τα αποτελέσματα που προέκυψαν από την ανάλυση των αντίστοιχων εικόνων τους: και οι δύο κατανομές του γυάλινου σκεδαστή έχουν μικρότερη μέση τιμή και μικρότερη τυπική απόκλιση σε σύγκριση με τις αντίστοιχες κατανομές της POF, αντανακλώντας την αυξημένη ομοιότητα των speckle patterns που παράγονται από αυτόν. Ωστόσο, από τις τιμές του πίνακα 7 αποδεικνύεται ότι τα ζεύγη ιστογραμμάτων εμφανίζουν μια μερική αλληλεπικάλυψη και για τα δύο υλικά, η οποία μπορεί να οδηγήσει σε ψευδώς αρνητική ή ψευδώς θετική αυθεντικοποίηση. Το γεγονός αυτό επιβεβαιώνει την ανεπάρκεια της χρησιμοποιούμενης τεχνικής ως μέθοδο παραγωγής διεγέρσεων, καθιστώντας αναγκαία τη λήψη επιπρόσθετων επανορθωτικών μέτρων, τα οποία θα επιτρέψουν τον διαχωρισμό των εν λόγω ιστογραμμάτων, είτε με πειραματικό είτε με υπολογιστικό τρόπο.



Σχήμα 5.7: Η πιθανότητα να προκύψουν πανομοιότυπες δυαδικές έξοδοι και από τα δύο στάδια του fuzzy extractor, συναρτήσει της διορθωτικής ικανότητας t του BCH κώδικα για **α)** τα δεδομένα που λήφθηκαν υπό τις ίδιες συνθήκες ακτινοβόλησης και για **β)** τα δεδομένα που λήφθηκαν εφαρμόζοντας όλες τις διαθέσιμες πειραματικές διεγέρσεις. Σε κάθε περίπτωση, οι διακεκομμένες γραμμές αντιστοιχούν στις προσεγγιστικές καμπύλες που προέκυψαν μέσω των αποστάσεων Hamming.

Όσον αφορά τώρα το διάγραμμα του σχήματος 5.7α, η πιθανότητα να ανακύψουν οι ίδιες δυαδικές έξοδοι και από τα δύο στάδια του fuzzy extractor αρχικά αυξάνει όσο μεγαλώνει η διορθωτική ικανότητα t του χρησιμοποιούμενου BCH. Εν συνεχεία όμως, η τιμή αυτής της πιθανότητας μεγιστοποιείται στην μονάδα, γεγονός που υποδηλώνει ότι ο εν λόγω κώδικας μπορεί πλέον να διορθώσει τουλάχιστον ίσο αριθμό σφαλμάτων με αυτόν που υπεισέρχεται στις δυαδικές ακολουθίες λόγω του μετρητικού θορύβου. Συνεπώς, για την αξιόπιστη λειτουργία του υπό μελέτη συστήματος η ελάχιστη αποδεκτή τιμή t για την περίπτωση του diffuser είναι ίση με 46 bits. Από την άλλη πλευρά, η αυξημένη ευαισθησία της POF απέναντι στον περιβαλλοντικό θόρυβο καθιστά αναγκαία την χρήση υψηλότερης διορθωτικής ικανότητας t, με την ελάχιστη αποδεκτή τιμή της να ορίζεται ίση με 109 bits.

Ταυτόχρονα όμως, οι αντίστοιχες πιθανότητες της γραφικής αναπαράστασης 5.7β, όπως αυτές προέκυψαν από τα σύνολα δεδομένων D_2 και D_4, αυξάνονται αδιαλείπτως όσο η διορθωτική ικανότητα t μεγαλώνει, με τον αριθμό των διαφορετικών δυαδικών εξόδων να μειώνεται. Για να αποφευχθεί λοιπόν η ανεπιθύμητη αυτή μείωση, η οποία καθιστά το σύστημα συστηματικά πιο ευάλωτο σε ενδεχόμενες υπολογιστικές επιθέσεις, η ικανότητα t του χρησιμοποιούμενου BCH πρέπει να τεθεί όσο το δυνατόν μικρότερη.

Συμπερασματικά, από τις γραφικές αναπαραστάσεις της παρούσας ενότητας δύναται να εξαχθεί το ακόλουθο τελικό συμπέρασμα: τα δύο υπό μελέτη υλικά παρουσιάζουν μια ιδιαιτέρως παρεμφερή απόδοση ως προς το unpredictability των δυαδικών εξόδων τους. Εντούτοις, λαμβάνοντας υπόψιν την ελάχιστη αποδεκτή τιμή t εκάστου μέσου, η πιθανότητα του να προκύψουν πανομοιότυπα αποτελέσματα και από τα δύο στάδια του fuzzy extractor είναι 0.02 για την οπτική ίνα και 9.68×10^{-7} για τον γυάλινο σκεδαστή, γεγονός που καθιστά το δεύτερο καταλληλότερο προς χρήση.

5.3 Συγκριτική Αξιολόγηση Τεχνικών Hashing για POF

Όπως έχει ήδη αποδειχθεί από τις προηγούμενες υποενότητες, η ανεπαρκής απόδοση του παρόντος συστήματος καθιστά αναγκαία την τροποποίηση της χρησιμοποιούμενης πειραματικής διάταξης, ώστε να επιτευχθεί ο ζητούμενος διαχωρισμός των υπό μελέτη κατανομών. Η τροποποίηση αυτή, όμως, στην περίπτωση της οπτικής ίνας είναι ιδιαίτερα δυσχερής, καθώς οι περιορισμένες διαστάσεις της επιφάνειας εισόδου της αποτρέπουν την προαναφερθείσα διεύρυνση της προσπίπτουσας δέσμης. Συνεπώς, η μοναδική λύση που μπορεί να προταθεί για την βελτίωση των εν λόγω αποτελεσμάτων είναι η αναζήτηση μιας καταλληλότερης τεχνικής hashing, η εφαρμογή της οποίας στα υπάρχοντα speckles θα οδηγήσει σε δυαδικές ακολουθίες με κατανομές που δεν επικαλύπτονται. Με αυτό τον σκοπό λοιπόν, δοκιμάστηκαν οι υπόλοιπες μέθοδοι εξαγωγής ακολουθιών, προκειμένου να εντοπιστεί αυτή που ενισχύει την ανομοιότητα των εικόνων σε δυαδικό επίπεδο, αλλά ταυτοχρόνως διατηρεί την επαναληψιμότητά τους εντός αποδεκτών ορίων.

5.3.1 Εύρεση Βέλτιστων Παραμέτρων

5.3.1.1 Τεχνική SVD

Στο πλαίσιο της παρούσας ενότητας, αρχικά διερευνήθηκε η επίδραση των παραμέτρων εκάστης τεχνικής πάνω στις εξαγόμενες δυαδικές ακολουθίες. Στην περίπτωση της SVD, οι βασικές αυτές παράμετροι είναι οι ακόλουθες:

- Το πλήθος q_1, το μέγεθος k_1, και η προκύπτουσα επικάλυψη d_1 των τμημάτων στα οποία διαχωρίζεται το υπό μελέτη πειραματικό speckle. Από αυτά τα τμήματα προέρχονται και τα ιδιάζοντα διανύσματα που συνθέτουν την πρώτη ενδιάμεση εικόνα της εν λόγω τεχνικής Γ_1.
- Το πλήθος q_2, το μέγεθος k_2, και η προκύπτουσα επικάλυψη d_2 των τετραγωνικών τμημάτων στα οποία διαχωρίζεται η προαναφερθείσα ενδιάμεση εικόνα Γ_1. Από τα τμήματα αυτά προέρχονται και τα ιδιάζοντα διανύσματα που απαρτίζουν την δεύτερη και τελευταία εικόνα της εν λόγω τεχνικής Γ_2.

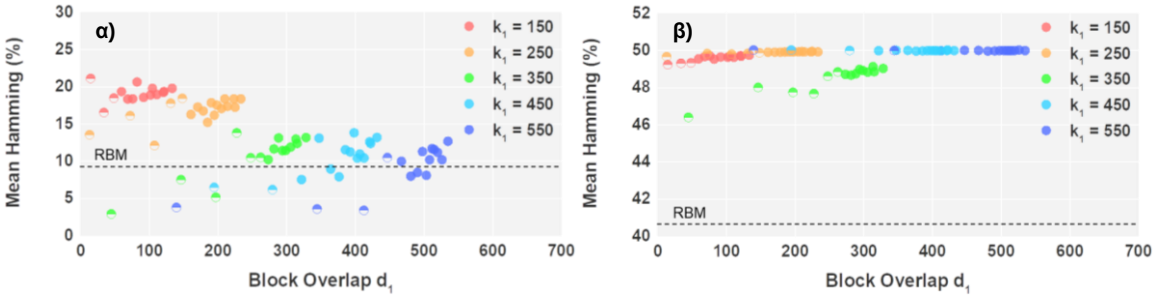
Το πρώτο σκέλος του παρόντος υποκεφαλαίου λοιπόν εστιάζει στην μελέτη της επιρροής των παραμέτρων q_1 και k_1 πάνω στις παραγόμενες δυαδικές ακολουθίες. Η διεξαγωγή της μελέτης αυτής έλαβε χώρα ως εξής. Πρώτα, όλες οι διαθέσιμες πειραματικές αποκρίσεις περικόπηκαν με πανομοιότυπο τρόπο, ώστε οι

διαστάσεις τους να γίνουν τετραγωνικές και ίσες με 960 × 960 pixels χάριν ευκολίας. Έπειτα, πραγματοποιήθηκε η διαίρεση των αποκρίσεων στα ζητούμενα τετραγωνικά τμήματα, από τα οποία εξήχθησαν και τα ιδιάζοντα διανύσματα που αποτελούν τις ενδιάμεσες εικόνες $Γ_1$. Ύστερα, οι προκύπτουσες εικόνες $Γ_1$ μετατράπηκαν απευθείας στις ζητούμενες δυαδικές ακολουθίες της παρούσας μελέτης, παραλείποντας εντελώς τη δεύτερη εφαρμογή της ανάλυσης SVD επί αυτών. Η άνωθεν διαδικασία επαναλήφθηκε μεταβάλλοντας τις τιμές q_1 και k_1 του ολισθαίνοντος παραθύρου τμηματοποίησης και για τα δύο σύνολα δεδομένων. Συνεπώς, για έκαστο ζεύγος τιμών q_1 και k_1 παράχθηκαν δύο σετ δυαδικών ακολουθιών, μήκους $k_1×(2q_1)$ bits, από τα οποία προέκυψαν δύο αντίστοιχες κατανομές αποστάσεων Hamming. Μέσω των κατανομών αυτών εντοπίστηκε και το βέλτιστο σημείο λειτουργίας της μονής εφαρμογής SVD επί των υπαρχόντων πειραματικών αποκρίσεων, το οποίο ουσιαστικά πρέπει να οδηγεί σε δύο επαρκώς διαχωρισμένα ιστογράμματα robustness και unpredictability με το ελάχιστο υπολογιστικό κόστος.

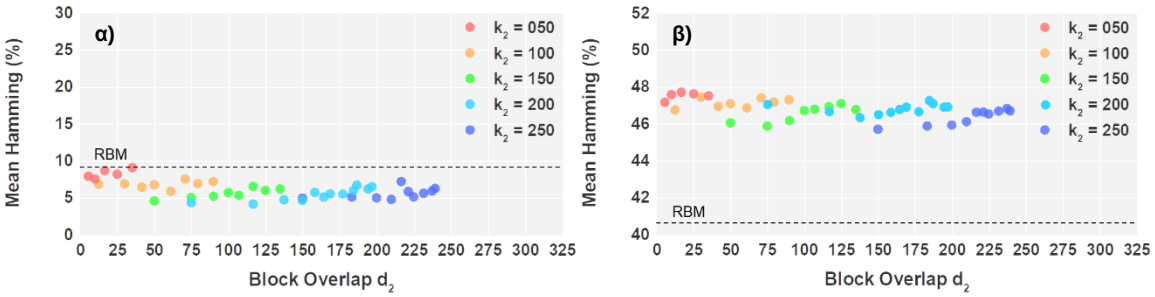
Σε αυτό το πλαίσιο λοιπόν στα διαγράμματα του σχήματος 5.8 αναπαριστώνται γραφικά οι μέσοι όροι των ποσοστιαίων αποστάσεων Hamming που προσδιορίστηκαν για κάθε σετ δυαδικών ακολουθιών, ως συνάρτηση της επικάλυψης των τμημάτων d_1, όπως αυτή διαμορφώνεται από τις επιλεγμένες τιμές των υπό μελέτη παραμέτρων. Συγκεκριμένα, κάθε σημείο του διαγράμματος 5.8α αντιστοιχεί στον μέσο όρο ${}_{60}C_2 = 1770$ αποστάσεων, οι οποίες υπολογίστηκαν από τις δυαδικές ακολουθίες του συνόλου D_3 (robustness), ενώ κάθε σημείο του γραφήματος 5.8β συμβολίζει τον μέσο όρο ${}_{255}C_2 = 32385$ αποστάσεων, οι οποίες προέκυψαν από τις αντίστοιχες ακολουθίες του συνόλου D_4 (unpredictability). Στο σημείο αυτό θα πρέπει να υπογραμμιστεί ότι τα ζεύγη κατανομών που προέκυψαν από κάθε σύνολο τιμών (q_1, k_1, d_1) ελέγχθηκαν και σε επίπεδο επικάλυψης, προκειμένου να απορριφθούν οι παράμετροι τμηματοποίησης οι οποίες αποτυγχάνουν να οδηγήσουν σε επαρκώς διαχωρισμένα ιστογράμματα. Οι απορριφθέντες αυτοί συνδυασμοί έχουν συμπεριληφθεί στα εν λόγω διαγράμματα του σχήματος 5.8 και αναπαριστώνται από τα σημεία που είναι κατά το ήμισυ κενά.

Αναλυτικότερα, ο μέσος όρος των ποσοστιαίων αποστάσεων Hamming, όπως αυτός προέκυψε από το σύνολο δεδομένων D_3, αρχικά παρουσιάζει μια αντιστρόφως ανάλογη σχέση με το μέγεθος k_1 του χρησιμοποιούμενου παραθύρου, αλλά για $k_1 \geq 450$ φαίνεται ότι σταθεροποιείται. Αντίθετα, ο αντίστοιχος μέσος όρος του συνόλου D_4 πρώτα εμφανίζει μια ελαφρώς ανοδική πορεία, η οποία εν συνεχεία σταθεροποιείται γύρω από την βέλτιστη δυνατή τιμή του 50%. Συνεπώς, η μονή εφαρμογή της SVD σε τμήματα μεγαλύτερων διαστάσεων διαχωρίζει με σχετικά αυξανόμενη επιτυχία τα σημαντικότερα γεωμετρικά γνωρίσματα των διαθέσιμων αποκρίσεων, φιλτράροντας τις μικρότερες και πιο θορυβικές λεπτομέρειές τους. Με άλλα λόγια, όσο περιορίζονται οι διαστάσεις του χρησιμοποιούμενου παραθύρου, το ιδιάζον διάνυσμα που εξάγεται από αυτό εμπεριέχει μεγαλύτερο όγκο από ασήμαντες αλλά θορυβικές χωρικές πληροφορίες, οι οποίες δεν επηρεάζουν ιδιαίτερα την μοναδικότητα των δυαδικών ακολουθιών, αλλά υποβαθμίζουν αισθητά την επαναληψιμότητά τους.

Όσον αφορά τώρα το πλήθος q_1 των υπό μελέτη τμημάτων και την κοινή επιφάνεια d_1 που αυτό το πλήθος υποδηλώνει, εν γένει παρατηρείται το ότι όσο διευρύνεται η επικάλυψη του ολισθαίνοντος παραθύρου, τόσο αυξάνεται η μέση ποσοστιαία απόσταση Hamming και για τα δύο σύνολα δεδομένων. Ταυτοχρόνως όμως, ελαττώνεται και η τυπική απόκλιση των αποστάσεων αυτών, με αποτέλεσμα να απαλείφεται και η προαναφερθείσα ανεπιθύμητη επικάλυψη των δύο αντίστοιχων κατανομών τους.



Σχήμα 5.8: Μέση τιμή αποστάσεων Hamming για τις δυαδικές ακολουθίες που προέκυψαν από τα speckles του **α)** συνόλου δεδομένων D_3 (robustness) και του **β)** συνόλου δεδομένων D_4 (unpredictability), από μόνο μία εφαρμογή SVD με μεταβαλλόμενες τις παραμέτρους k_1 και q_1.



Σχήμα 5.9: Μέση τιμή αποστάσεων Hamming για τις δυαδικές ακολουθίες που προέκυψαν από τα speckles του **α)** robustness και του **β)** unpredictability, από την διπλή εφαρμογή της SVD, για σταθερές παραμέτρους $k_1 = 450$ και $q_1 = 225$, αλλά μεταβαλλόμενες παραμέτρους k_2 και q_2.

Ως εκ τούτου, η μονή εφαρμογή της SVD επί των διαθέσιμων πειραματικών αποκρίσεων αποδεικνύεται επαρκής για την αποφυγή εσφαλμένων αυθεντικοποιήσεων, καθώς στην πλειοψηφία των περιπτώσεων επιτυγχάνει την ενίσχυση της ιδιομορφίας των ακολουθιών από διαφορετικά challenges κατά ~10% σε σχέση με την τεχνική RBM, οδηγώντας σε κατανομές αποστάσεων Hamming εμφανώς διαχωρισμένες. Η απόδοση της μάλιστα βελτιώνεται όσο το μέγεθος και η επικάλυψη του παραθύρου αυξάνει, υποδεικνύοντας ως καταλληλότερα τα σύνολα παραμέτρων με $k_1 \geq 450$ pixels. Σε αυτό το πλαίσιο λοιπόν, το σύνολο των παραμέτρων που επιλέχθηκε να χρησιμοποιηθεί για την πρώτη εφαρμογή της SVD αντιστοιχεί σε $k_1 = 450$ pixels, $q_1 = 225$ τμήματα και $d_1 \approx 414$ pixels.

Με δεδομένες τις παραπάνω τιμές των k_1 και q_1, στην συνέχεια διεξήχθη μια αντίστοιχη διερεύνηση για τις παραμέτρους k_2 και q_2, ακολουθώντας ακριβώς την ίδια μεθοδολογία: οι ενδιάμεσες εικόνες Γ_1, όπως αυτές προκύπτουν από την πρώτη εφαρμογή της SVD και πριν το βήμα της δυαδικοποίησης, διαχωρίζονται σε q_2 τετραγωνικά τμήματα με μέγεθος k_2. Κατόπιν, από την ανάλυση SVD εκάστου τμήματος εξάγονται τα ιδιάζοντα διανύσματα που συνθέτουν τις ενδιάμεσες εικόνες Γ_2, οι οποίες εν τέλει δυαδικοποιούνται, οδηγώντας στις ζητούμενες δυαδικές ακολουθίες της παρούσας μελέτης, με μήκος $k_2 \times (2q_2)$ bits.

Εν προκειμένω, στα γραφήματα του σχήματος 5.9 παρουσιάζονται τα αποτελέσματα των μέσων ποσοστιαίων αποστάσεων Hamming, όπως αυτά προέκυψαν μεταβάλλοντας τις τιμές q_2 και k_2 του ολισθαίνοντος παραθύρου τμηματοποίησης και για τα δύο σύνολα δεδομένων.

Όπως φαίνεται λοιπόν από τα αντίστοιχα διαγράμματα, οι τρέχουσες τιμές αποστάσεων Hamming είναι εν γένει χαμηλότερες από αυτές της μονής εφαρμογής SVD, εμφανίζοντας μια παρεμφερή συμπεριφορά και για τα 2 datasets: ο αριθμός των ψηφίων που διαφέρει μεταξύ των δυαδικών ακολουθιών φθίνει όταν το μέγεθος k_2 των χρησιμοποιούμενων τμημάτων αυξάνεται και όταν η επικάλυψη d_2 αυτών ελαττώνεται. Τα ευρεθέντα αυτά αποτελέσματα δύναται να ερμηνευθούν

ακολούθως: τα κύρια γεωμετρικά χαρακτηριστικά των ενδιάμεσων εικόνων Γ_1, στις οποίες εφαρμόζεται για δεύτερη φορά η ανάλυση SVD, ουσιαστικά αντιστοιχούν στις λωρίδες που σχηματίζονται από τα ιδιάζοντα διανύσματα των πειραματικών speckle patterns˙ όσο λοιπόν το μέγεθος και το πλήθος των τμημάτων αυξάνει, οι λωρίδες αυτές οριοθετούνται καλύτερα, με τις μικρές αυξομειώσεις εντός τους να εκλαμβάνονται ως θόρυβος και εν τέλει να απαλείφονται.

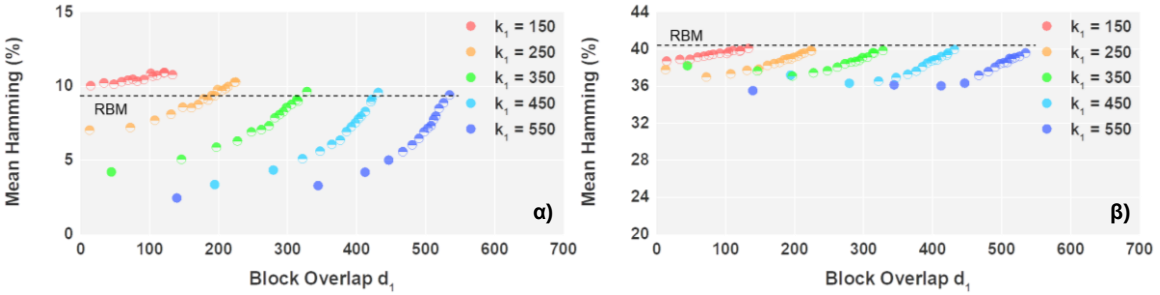
Συμπερασματικά, με δεδομένες τις επιλεγμένες τιμές $k_1 = 450$ και $q_1 = 225$, η επίδοση της διπλής εφαρμογής SVD βρέθηκε να υπερτερεί έναντι αυτής που προέκυψε από την τεχνική RBM, καθώς για κάθε δοκιμαζόμενο συνδυασμό (k_2, q_2, d_2) επιτυγχάνεται η βελτίωση των αποστάσεων Hamming, τόσο των ακολουθιών του robustness όσο και των ακολουθιών του unpredictability. Η ταυτόχρονη αυτή βελτίωση οδηγεί με την σειρά της στον ζητούμενο διαχωρισμό των δύο αντίστοιχων κατανομών, οι οποίες μάλιστα παραμένουν και σχετικά ανεπηρεάστες από τη μεταβολή των μελετούμενων παραμέτρων. Συνεπώς, οποιοδήποτε σύνολο (k_2, q_2, d_2) αποδεικνύεται κατάλληλο για την δεύτερη εφαρμογή της SVD, με τις επιλεγμένες τελικές τιμές να ισούνται με $k_2 = 200$ pixels, $q_2 = 144$ τμήματα και $d_2 \approx 177$ pixels αντιστοίχως.

5.3.1.2 Τεχνική NMF

Στην παρούσα ενότητα παρατίθενται συνοπτικά τα αποτελέσματα που προέκυψαν από μια ανάλογη διερεύνηση με αυτήν της προηγούμενης παραγράφου, η οποία διεξήχθη για τις παραμέτρους της τεχνικής NMF, (k_1, q_1, d_1) και (k_2, q_2, d_2), ακολουθώντας ακριβώς την ίδια μεθοδολογία. Και σε αυτή την περίπτωση, οι μεταβλητές k_1, q_1 και d_1 συμβολίζουν τις διαστάσεις, το πλήθος και την επικάλυψη των τμημάτων, επί των οποίων λαμβάνει χώρα η πρώτη εφαρμογή της ανάλυσης NMF, ενώ οι μεταβλητές k_2, q_2 και d_2 αντιπροσωπεύουν τις αντίστοιχες παραμέτρους τμηματοποίησης για την δεύτερη εφαρμογή αυτής.

Σε αυτό το πλαίσιο, στα διαγράμματα του σχήματος 5.10 επιδεικνύονται οι μέσοι όροι των ποσοστιαίων αποστάσεων Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών που παράχθηκαν από τα datasets D_3 και D_4, ως συνάρτηση της επικάλυψης των τμημάτων d_1. Θα πρέπει να σημειωθεί ότι και σε αυτές τις γραφικές παραστάσεις, οι αποστάσεις από τα ζεύγη κατανομών που εμφανίζουν ακόμα την ανεπιθύμητη επικάλυψη που αποπειράθηκε να απαλειφθεί, συμβολίζονται από τα σημεία που είναι κατά το ήμισυ κενά, ούτως ώστε να εντοπιστούν οι απορριφθέντες συνδυασμοί παραμέτρων, οι οποίοι αδυνατούν να αποτρέψουν την ψευδώς θετική ή ψευδώς αρνητική αυθεντικοποίηση αποτελεσμάτων.

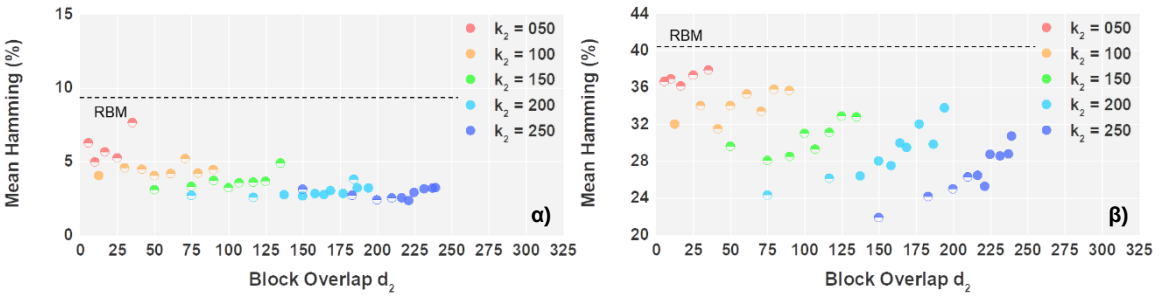
Όπως αποδεικνύεται λοιπόν από τις δυο αναφερθείσες γραφικές, η μονή εφαρμογή της ανάλυσης NMF δεν κατορθώνει εν γένει να απομακρύνει τις κατανομές των Robustness και Unpredictability που παράγονται μέσω της unpolished POF. Ο διαχωρισμός μάλιστα των μη επικαλυπτόμενων ζευγών προκύπτει τόσο οριακός, ώστε η συνολική επίδοση της μονής NMF να χαρακτηρίζεται ως τελείως ανεπαρκής. Επομένως, οι τελικές τιμές των παραμέτρων που επιλέχθηκαν να χρησιμοποιηθούν για την πρώτη εφαρμογή της NMF συμπίπτουν με αυτές της προηγούμενης ενότητας, κυρίως για λόγους σύγκρισης, με το μέγεθος του ολισθαίνοντος παραθύρου τμηματοποίησης να ορίζεται ίσο με $k_1 = 450$ pixels και το πλήθος των εξαγόμενων blocks να τίθεται ίσο με $q_1 = 225$ τμήματα.



Σχήμα 5.10: Μέση τιμή ποσοστιαίων αποστάσεων Hamming για τις δυαδικές ακολουθίες που προέκυψαν από τα speckles του **α)** δεδομένων D_3 (robustness) και του **β)** συνόλου δεδομένων D_4 (unpredictability), από μόνο μία εφαρμογή MNF με μεταβαλλόμενες τις παραμέτρους k_1 και q_1.

Ακολούθως, στα γραφήματα του σχήματος 5.11 παρουσιάζονται οι αντίστοιχοι μέσοι όροι των ποσοστιαίων αποστάσεων Hamming ως συνάρτηση της επικάλυψης d_2, όπως αυτοί προέκυψαν από την διπλή εφαρμογή της ανάλυσης NMF επί των συνόλων D_3 και D_4, για σταθερές παραμέτρους $k_1 = 450$ και $q_1 = 225$, αλλά μεταβαλλόμενες παραμέτρους k_2 και q_2.

Όπως φαίνεται λοιπόν από τα παρακάτω διαγράμματα, ούτε η διπλή εφαρμογή της NMF κατορθώνει να απομακρύνει τις κατανομές του Robustness και του Unpredictability, ειδικά για μέγεθος τμημάτων k_2 μικρότερο των 200 pixels. Εντούτοις για $k_2 \geq 200$, παρατηρείται ότι επιτυγχάνεται γενικά ο επιθυμητός διαχωρισμός των εξαγόμενων κατανομών, ο οποίος όμως είναι και πάλι τόσο οριακός, ώστε η μελετούμενη τεχνική να κρίνεται τελικά πλήρως ακατάλληλη για τις ανάγκες της παρούσας εργασίας.



Σχήμα 5.11: Μέση τιμή αποστάσεων Hamming για τις δυαδικές ακολουθίες που προέκυψαν από τα speckles του **α)** robustness και του **β)** unpredictability, από την εφαρμογή και των δύο NMF, για σταθερές παραμέτρους $k_1 = 450$ και $q_1 = 225$, αλλά μεταβαλλόμενες παραμέτρους k_2 και q_2.

Συμπερασματικά, από τις ποσοστιαίες αποστάσεις Hamming των δυαδικών ακολουθιών που παράγονται μέσω της τεχνικής NMF, γίνεται εμφανές ότι η διπλή εφαρμογή της ομώνυμης ανάλυσης δεν εξασφαλίζει την απουσία εσφαλμένων αυθεντικοποιήσεων, αφού οποιοσδήποτε συνδυασμός παραμέτρων αδυνατεί να απομακρύνει επαρκώς τις δύο στοχευόμενες κατανομές, όπως αυτές προκύπτουν από τα speckles των datasets D_3 και D_4. Η συνολική επίδοση μάλιστα της εν λόγω τεχνικής βρέθηκε ότι μειονεκτεί σε σχέση με αυτήν της τεχνικής RBM, αφού ο πολλαπλασιαστικός ευρεστικός αλγόριθμος που χρησιμοποιήθηκε για την υλοποίηση της οδηγεί σε ακολουθίες με ψηφία, η πλειοψηφία των οποίων συνήθως καταλήγει να λαμβάνει την τιμή μηδέν. Με άλλα λόγια, τα ψηφία των δυαδικών ακολουθιών που παράγονται μέσω της τεχνικής NMF παρουσιάζουν μια συστηματική τάση προς την μηδενική τιμή, γεγονός που τις καθιστά πιο προβλέψιμες από τις αντίστοιχες ακολουθίες των υπολοίπων τεχνικών. Σε αυτή την τάση της τεχνικής NMF να παράγει ακολουθίες με μεγάλο αριθμό μηδενικών μπορούν να αποδοθούν και οι χαμηλότερες αποστάσεις Hamming που προκύπτουν από την εν λόγω τεχνική σε σχέση αυτές της προαναφερθείσας RBM.

Από το σύνολο λοιπόν των παραμέτρων (k_1, q_1, d_1) και (k_2, q_2, d_2) της υπό μελέτη τεχνικής με την διπλή εφαρμογή της ανάλυσης NMF, εντοπίσθηκαν ελάχιστοι συνδυασμοί τιμών που οδηγούν σε αποδεκτά αποτελέσματα αποστάσεων Hamming. Ως εκ τούτου, τελικά οι τιμές παραμέτρων που επιλέχθηκαν για την τελική εφαρμογή της εν λόγω τεχνικής είναι ίδιες με αυτές της προαναφερθείσας τεχνικής SVD, κυρίως για λόγους διευκόλυνσης, καθώς τα αποτελέσματα από αυτές είναι από τα βέλτιστα που μπορούν να επιτευχθούν.

Συνεπώς, οι τελικές τιμές παραμέτρων που χρησιμοποιήθηκαν για την πρώτη εφαρμογή της NMF ισούνται με $k_1 = 450$ pixels, $q_1 = 225$ τμήματα και $d_1 \approx 414$ pixels, ενώ για την δεύτερη εφαρμογή αυτής με $k_2 = 200$ pixels, $q_2 = 144$ τμήματα και $d_2 \approx 177$ pixels αντιστοίχως.

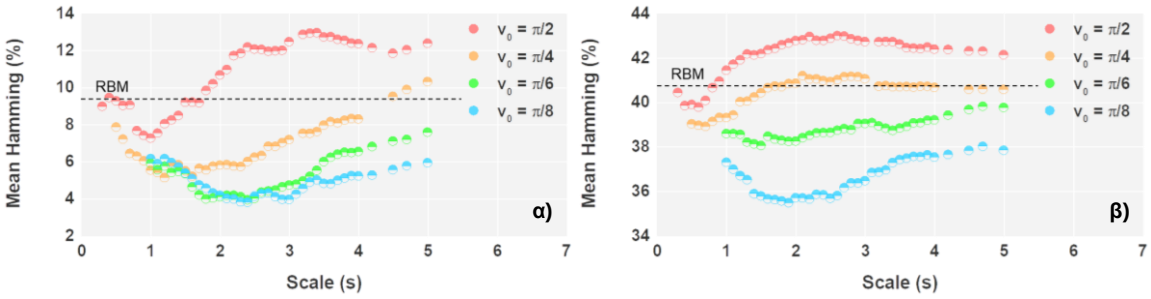
5.3.1.3 Τεχνική GBM

Στην ενότητα τούτη παρουσιάζεται η επιρροή των παραμέτρων της τελευταίας τεχνικής που χρησιμοποιήθηκε στο πλαίσιο της παρούσας διατριβής για την εξαγωγή δυαδικών ακολουθιών από τα datasets D_3 και D_4, της τεχνικής GBM. Οι παράμετροι αυτές είναι:

- Το μέγεθος g×g των φίλτρων Gabor, το οποίο συμπίπτει με τις διαστάσεις των μη επικαλυπτόμενων τμημάτων που διαχωρίζεται κάθε μελετούμενη εικόνα.
- Το χωρικό εύρος (scale) των φίλτρων Gabor, το οποίο καθορίζεται από τη τυπική απόκλιση s της δισδιάστατης Gaussian συνάρτησης αυτού.
- Η χωρική συχνότητα (spatial frequency) των φίλτρων Gabor, η οποία προσδιορίζεται από τον κυματάριθμο v_0 του χρησιμοποιούμενου κυματανύσματος.
- Οι χωρικές κατευθύνσεις (orientation) των φίλτρων, οι οποίες προκύπτουν από την φάση θ του προαναφερθέντος κυματανύσματος.

Στο σημείο αυτό κρίνεται σκόπιμο να υπενθυμιστεί ότι η GBM ουσιαστικά αντιστοιχεί στην εφαρμογή μιας συστοιχίας φίλτρων Gabor, τα οποία παράγονται διατηρώντας σταθερές τις παραμέτρους g, s και v_0, αλλά μεταβάλλοντας την χωρική κατεύθυνσή τους θ. Σε αυτό το πλαίσιο, δοκιμάστηκαν 720 εναλλακτικές συστοιχίες φίλτρων με οκτώ διαφορετικούς προσανατολισμούς $\theta = (i-1)/8\pi$, όπου $0 \le i \le 7$, οι οποίες κατασκευάστηκαν από τους ακόλουθους συνδυασμούς τιμών: $g = 30j$ με $1 \le j \le 4$, $s = 0.1k + 0.5$ με $0 \le k \le 45$ και $v_0 = (\pi/2)/\ell$ με $1 \le \ell \le 4$ αντιστοίχως.

Στα ενδεικτικά διαγράμματα του παρακάτω σχήματος λοιπόν επιδεικνύονται οι μέσοι όροι των ποσοστιαίων αποστάσεων Hamming που προέκυψαν για μέγεθος φίλτρων ίσο με g = 30, συναρτήσει του χωρικού τους εύρους s. Συγκεκριμένα, κάθε σημείο του γραφήματος 5.12α αντιστοιχεί στον μέσο όρο ${}_{60}C_2 = 1770$ αποστάσεων, οι οποίες υπολογίστηκαν από τις δυαδικές ακολουθίες του συνόλου D_3 (robustness), ενώ κάθε σημείο του γραφήματος 5.12β συμβολίζει τον μέσο όρο ${}_{255}C_2 = 32385$ αποστάσεων, οι οποίες προέκυψαν από τις αντίστοιχες ακολουθίες του συνόλου D_4 (unpredictability). Θα πρέπει να σημειωθεί ότι και σε αυτές τις γραφικές παραστάσεις, οι αποστάσεις από τα ζεύγη κατανομών που εμφανίζουν ακόμα την ανεπιθύμητη επικάλυψη που αποπειράθηκε να απαλειφθεί, συμβολίζονται από τα σημεία που είναι κατά το ήμισυ κενά.



Σχήμα 5.12: Μέση τιμή ποσοστιαίων αποστάσεων Hamming για τις δυαδικές ακολουθίες που προέκυψαν από τα speckle patterns του **α)** robustness και του **β)** unpredictability, μέσω της τεχνικής GBM. Οι τράπεζες φίλτρων που χρησιμοποιήθηκαν αποτελούνται από οκτώ διαφορετικά φίλτρα Gabor σταθερού μεγέθους, ίσου με g = 30 pixels ανά διάσταση, τα οποία παράχθηκαν από ισάριθμες τιμές προσανατολισμών θ = (i-1)/8π, όπου 0 ≤ i ≤ 7.

5.3.2 Αποστάσεις Hamming και Πιθανότητες Ιδιοτήτων

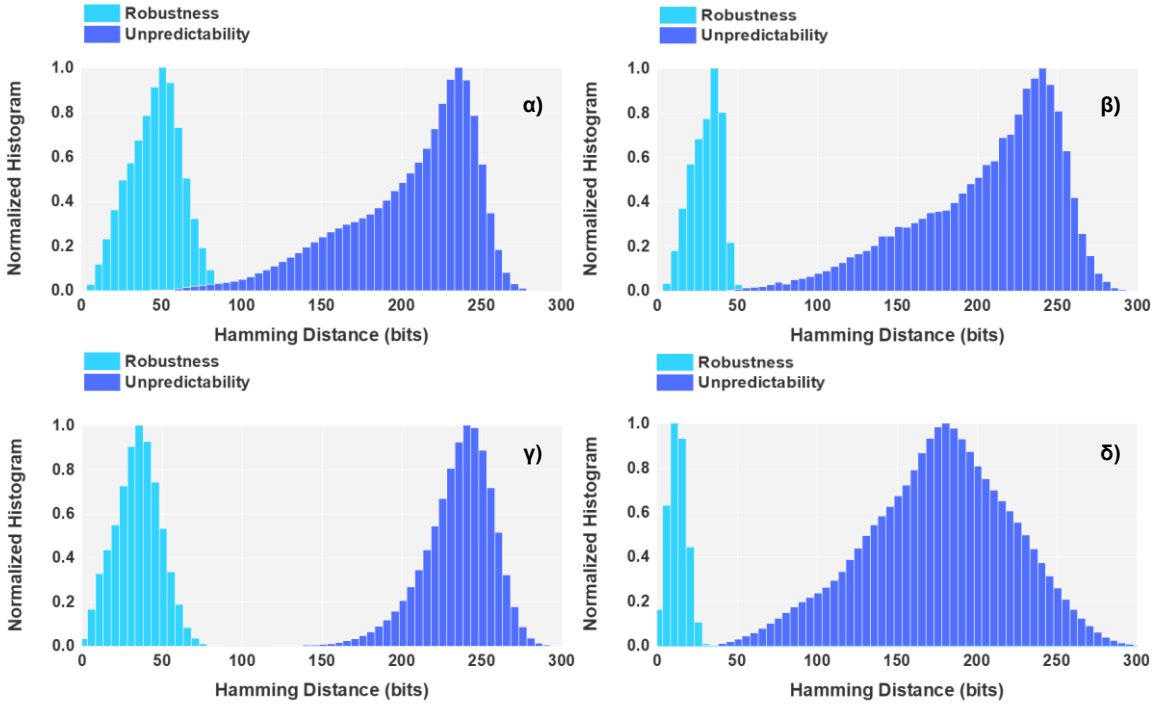
Έχοντας διερευνήσει λοιπόν την επίδραση των παραμέτρων εκάστης τεχνικής πάνω στις εξαγόμενες δυαδικές ακολουθίες και έχοντας εντοπίσει τους κατάλληλους συνδυασμούς τιμών, οι οποίοι οδηγούν στο βέλτιστο σημείο λειτουργίας του συστήματος με την POF, εν συνεχεία θεωρήθηκε σκόπιμο να πραγματοποιηθεί μια επιπλέον συγκριτική μελέτη της απόδοσης που παρουσιάζει η κάθε τεχνική, εφαρμόζοντας την κυκλική μεθοδολογία της παραγράφου 5.2.2.

Εν προκειμένω, στα γραφήματα του σχήματος 5.13 παρουσιάζονται συγκεντρωμένα όλα τα ζεύγη κατανομών από τις αποστάσεις Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών που προέκυψαν από κάθε εφαρμοζόμενη τεχνική, ενώ στους πίνακες 8, 9 και 10 συνοψίζονται τα αντίστοιχα στατιστικά τους μέτρα. Ακολούθως, στα γραφήματα του σχήματος 5.14 αναπαριστώνται οι πιθανότητες να προκύψουν οι ίδιες δυαδικές έξοδοι και από τα δύο στάδια του fuzzy extractor, οι οποίες προσδιορίστηκαν με δύο διαφορετικές προσεγγίσεις κατά τα γνωστά. Σε αυτό το σημείο κρίνεται αναγκαίο να αναφερθεί ότι στις γραφικές αναπαραστάσεις της παρούσας ενότητας έχουν επιπλέον συμπεριληφθεί και τα ήδη παρουσιασμένα αποτελέσματα της τεχνικής RBM, για λόγους πληρότητας.

Σύμφωνα λοιπόν με τα παρακάτω ιστογράμματα, τα οποία αντιπροσωπεύουν $(60 \times {}_{60}C_2)$ συγκρίσεις στην περίπτωση του robustness και $(255 \times {}_{255}C_2)$ συγκρίσεις στην περίπτωση του unpredictability, από τις 4 διαφορετικές τεχνικές που δοκιμάστηκαν για την εξαγωγή των ζητούμενων ακολουθιών, μόνο η SVD επιτυγχάνει τον στοχευόμενο διαχωρισμό των υπό μελέτη κατανομών. Εντούτοις, οι επιδόσεις όλων των τεχνικών ως προς την ιδιότητα του robustness εμφανίζονται εμφανώς βελτιωμένες σε σχέση με αυτήν της RBM, καθώς η μέση τιμή και το εύρος των αντίστοιχων κατανομών τους περιορίζεται σημαντικά. Το εν λόγω γεγονός επιβεβαιώνεται και από τις καμπύλες του διαγράμματος 5.14α, μέσω των οποίων διαπιστώνεται ότι για τις τεχνικές NMF, GBM και SVD η διορθωτική ικανότητα t που χρειάζεται ούτως ώστε να λάβει η πιθανότητα του robustness τους μοναδιαία τιμή είναι $t_{NMF} = 42$, $t_{GBM} = 51$ και $t_{SVD} = 91$ bits, ενώ για την τεχνική RBM απαιτούνται $t_{RBM} = 109$ bits διόρθωσης αντιστοίχως.

Όσον αφορά τώρα το unpredictability του υπό μελέτη συστήματος, όπως αποδεικνύεται από τα κάτωθι αποτελέσματα, η SVD υπερτερεί ξεκάθαρα έναντι των άλλων 3 τεχνικών, οι οποίες μάλιστα παρουσιάζουν ιδιαίτερα παρεμφερή επίδοση, σύμφωνα με το σχήμα 5.14β. Ωστόσο, λαμβάνοντας υπόψιν τις τιμές διορθωτικής ικανότητας t που απαιτούνται για να διασφαλιστεί η επαναληψιμότητα των δυαδικών εξόδων από εκάστη τεχνική, η πιθανότητα του να προκύψουν

πανομοιότυπα αποτελέσματα και από τα δύο στάδια του fuzzy extractor είναι 0.02 για την RBM, 5.09×10^{-4} για την NMF και 3.09×10^{-4} για την GBM, γεγονός που καθιστά την τελευταία την βέλτιστη εναλλακτική επιλογή.



Σχήμα 5.13: Οι κατανομές των αποστάσεων Hamming μεταξύ όλων των δυαδικών ακολουθιών, μήκους 511 bits, όπως αυτές προέκυψαν μέσω των **α)** RBM **β)** GBM, **γ)** SVD και **δ)** NMF τεχνικών από τα δεδομένα της POF.

Πίνακας 8: Στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών που παράχθηκαν μέσω της GBM τεχνικής

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_3	1	47	26.5	9.3
D_4	47	400	207.7	44.2

Πίνακας 9: Στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών που παράχθηκαν μέσω της SVD τεχνικής

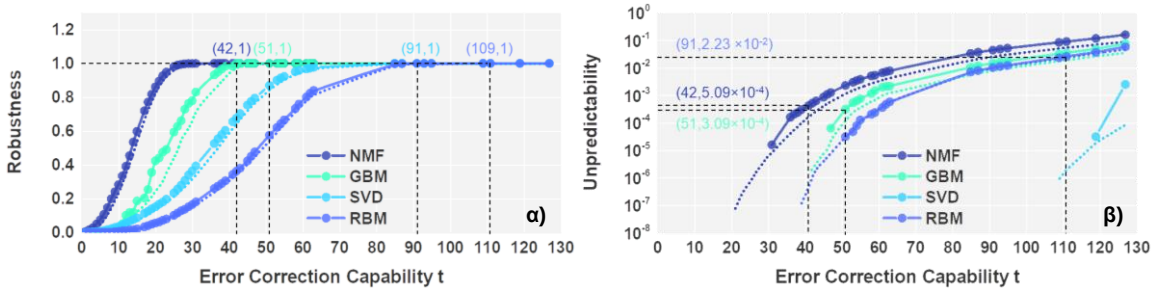
Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_3	0	89	36.0	14.0
D_4	99	320	236.5	21.7

Πίνακας 10: Στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν μεταξύ των δυαδικών ακολουθιών που παράχθηκαν μέσω της NMF τεχνικής .

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_3	0	37	13.85	5.8
D_4	20	341	177.3	45.3

Συμπερασματικά, εκ των 4 τεχνικών που δοκιμάστηκαν για την εξαγωγή των ζητούμενων δυαδικών ακολουθιών, μόνο η τεχνική SVD διαχωρίζει με επιτυχία τις κατανομές των αποστάσεων Hamming για το robustness και το unpredictability της POF. Επομένως η SVD είναι και η μόνη προσέγγιση που ελαχιστοποιεί το ενδεχόμενο ύπαρξης εσφαλμένων αυθεντικοποίησεων, αποτελώντας την

καταλληλότερη μέθοδο παραγωγής ακολουθιών με χρήση της παρούσας διάταξης.



Σχήμα 5.14: Η πιθανότητα να προκύψουν πανομοιότυπες δυαδικές έξοδοι και από τα δύο στάδια του fuzzy extractor, συναρτήσει της διορθωτικής ικανότητας t του BCH κώδικα για **α)** τα δεδομένα που λήφθηκαν υπό τις ίδιες συνθήκες ακτινοβόλησης και για **β)** τα δεδομένα που λήφθηκαν εφαρμόζοντας όλες τις διαθέσιμες πειραματικές διεγέρσεις.

Θα πρέπει να σημειωθεί όμως ότι καθώς οι δυαδικές εκδοχές των ενδιάμεσων εικόνων που προκύπτουν από την τεχνική αυτή εμφανίζουν μια ξεκάθαρη ραβδωτή μορφολογία, όπως παρουσιάζεται και στο σχήμα 3.13δ, επιβάλλεται ένα επιπλέον βήμα πριν την ψευδοτυχαία επιλογή των ψηφίων που απαρτίζουν την τελική ακολουθία, προκειμένου να ενισχυθεί η συνολική ασφάλεια του συστήματος. Το επιπλέον αυτό βήμα θα μπορούσε να αντιστοιχεί στην εφαρμογή μιας μη γραμμικής δισδιάστατης απεικόνισης στην εν λόγω εικόνα, όπως είναι η απεικόνιση Henon, η οποία αναδιατάσσει με χαοτικό τρόπο τα στοιχεία αυτής, απαλείφοντας οποιοδήποτε επαναλαμβανόμενο και γεωμετρικό της μοτίβο [75].

5.4 Συμπεράσματα

Συνοψίζοντας τα περιεχόμενα του εν λόγω κεφαλαίου, η δεύτερη υλοποίηση οπτικής PUF που κατασκευάστηκε στο πλαίσιο της παρούσας διατριβής, σχεδιάστηκε για να μελετηθεί ως μέθοδος παραγωγής διεγέρσεων η μεταβολή των σημείων πρόσπτωσης του φωτός επί του εκάστοτε ανομοιογενούς μέσου. Η μεταβολή αυτή ουσιαστικά πραγματοποιήθηκε αναβοσβήνοντας 8 εικονοστοιχεία μιας οθόνης LCD, η οποία παρεμβλήθηκε στην οπτική διαδρομή της χρησιμοποιούμενης δέσμης, οδηγώντας σε 255 συνδυασμούς ενεργών και ανενεργών pixels που τροποποιούν το προφίλ εντάσεως αυτής με μοναδικό τρόπο. Τα κύρια ευρήματα της εν λόγω μελέτης λοιπόν συνοψίζονται ως εξής:

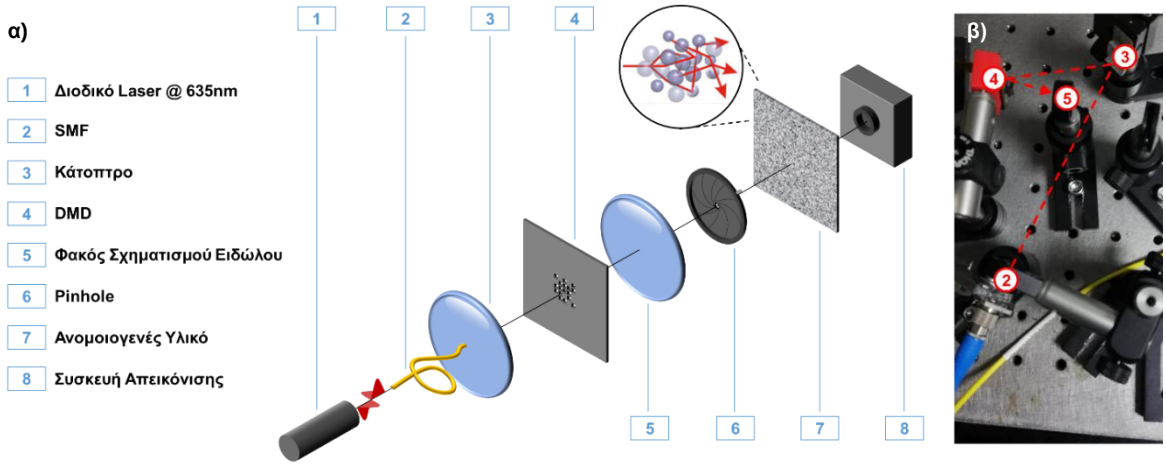
- Για να ελαχιστοποιηθεί η επίδραση του πειραματικού θορύβου και να ενισχυθεί το robustness οποιουδήποτε συστήματος PUF με την ελάχιστη δυνατή απώλεια πληροφορίας, οι κηλίδες από τα speckle patterns που καταγράφονται πρέπει να καταλαμβάνουν περίπου 6 pixels ανά διάσταση επί του αισθητήρα.
- Οι απλοϊκοί δυαδικοί συνδυασμοί και ο μικρός αριθμός των χρησιμοποιούμενων pixels από τα οποία συγκροτούνται οι εφαρμοζόμενες διεγέρσεις καθιστούν την παρούσα μέθοδο ακτινοβόλησης των υλικών μη ικανοποιητική, καθώς αδυνατεί να οδηγήσει σε αρκούντως ασυσχέτιστα speckles και αποτυγχάνει να εξαλείψει το ενδεχόμενο εσφαλμένων αυθεντικοποιήσεων. Συνεπώς για την επίλυση των προβλημάτων αυτών χρήζεται αναγκαία η τροποποίηση της χρησιμοποιούμενης πειραματικής διάταξης, η οποία όμως θεωρήθηκε εφικτή μόνο για την περίπτωση του diffuser.
- Για την περίπτωση της οπτικής ίνας η αντιμετώπιση των άνωθεν αναφερθέντων ζητημάτων επιδιώχθηκε υπολογιστικά, αντικαθιστώντας την χρησιμοποιούμενη τεχνική εξαγωγής RBM με την καταλληλότερη τεχνική SVD, η οποία διαχωρίζει αποτελεσματικότερα τα γεωμετρικά γνωρίσματα

των διαθέσιμων αποκρίσεων, ελαχιστοποιώντας τη πιθανότητα να πραγματοποιηθούν ψευδά θετικές ή ψευδά αρνητικές αυθεντικοποίησεις.

6. ΠΕΙΡΑΜΑΤΙΚΗ ΔΙΑΤΑΞΗ ΜΕ ΟΘΟΝΗ DMD

Η τρίτη πειραματική διάταξη που χρησιμοποιήθηκε στο πλαίσιο της παρούσας διατριβής ουσιαστικά αποτελεί μια βελτιωμένη παραλλαγή της προαναφερθείσας υλοποίησης με την LCD, στην οποία εφαρμόστηκαν ορισμένες κατάλληλες τροποποιήσεις, προκειμένου να αντιμετωπιστούν τα κύρια ζητήματα που προέκυψαν κατά την χρήση της. Τα ζητήματα αυτά είναι: η αύξηση της ανάλυσης των εφαρμοζόμενων challenges, η μείωση των κοινών εικονοστοιχείων μεταξύ τους και η μεγέθυνση των προβαλλόμενων ειδώλων τους πάνω στην επιφάνεια εισόδου του χρησιμοποιούμενου diffuser. Ταυτόχρονα, λήφθηκαν κάποια επιπλέον μέτρα για τον έλεγχο και την καταστολή του μετρητικού θορύβου, ώστε το τελικό εργαστηριακό πρωτότυπο να οδηγεί σε αποκρίσεις με καλύτερη επαναληψιμότητα και μεγαλύτερη αξιοπιστία.

Σε αυτό το πλαίσιο λοιπόν, στην ακόλουθη σχηματική αναπαράσταση παρουσιάζεται η εναλλακτική υλοποίηση της οπτικής PUF που διερευνήθηκε στο προηγούμενο κεφάλαιο, όπως αυτή προσαρμόστηκε για την επιτυχή αντιμετώπιση των άνωθεν προβλημάτων.



Σχήμα 6.1: α) Σχηματικό διάγραμμα οπτικής PUF με χρήση μιας συσκευής ψηφιακών μικρο-κατόπτρων για την παραγωγή των διεγέρσεων. **β)** Φωτογραφία τμήματος από το πείραμα που επιδεικνύει την ακριβή τοποθέτηση των χρησιμοποιούμενων οπτικών στοιχείων για την οδήγηση της δέσμης.

Όπως φαίνεται λοιπόν και από το παραπάνω σχήμα, ως πηγή σύμφωνης ακτινοβολίας στη παρούσα περίπτωση επιλέχθηκε ένα διοδικό CW laser με γραμμικά πολωμένη έξοδο και μήκος κύματος στα 635nm. Η δέσμη του laser αυτού 1 αρχικά οδηγείται μέσω μιας συμβατικής μονότροπης οπτικής ίνας 2 σε ένα κάτοπτρο 3, η ανάκλαση από το οποίο εν συνεχεία προσπίπτει σε μια συσκευή ψηφιακών μικρο-κατόπτρων (Digital Micromirror Device - DMD) 4, με ανάλυση 640×340 micromirrors, pitch 7.56μm και δυνατότητα γωνιακής κίνησης καθρεφτών στις ±10°. Στην εν λόγω συσκευή προβάλλεται μια δυαδική εικόνα αντίστοιχης ανάλυσης, οι μοναδιαίες εντάσεις της οποίας στρέφουν ένα μοναδικό συνδυασμό από micromirrors στις +10°, εκτρέποντας και ένα τμήμα της διαδιδόμενης δέσμης αναλόγως. Το εκτρεπόμενο αυτό τμήμα, αφού διέλθει μέσω ενός συγκεντρωτικού φακού 5 και μιας ίριδας (pinhole) 6, κατόπιν προσπίπτει στην επιφάνεια του γυάλινου σκεδαστή 7, η έξοδος του οποίου καταγράφεται από μια επιστημονική κάμερα CMOS 8με ανάλυση 1200×800 pixels και χρωματικό βάθος 16bits.

Στο σημείο αυτό κρίνεται σκόπιμο να διασαφηνιστεί ότι η δυαδική εικόνα που προβάλλεται στην συσκευή DMD ουσιαστικά αποτελεί και την εφαρμοζόμενη διέγερση του υπό μελέτη συστήματος, η οποία, ακριβώς όπως και στην περίπτωση

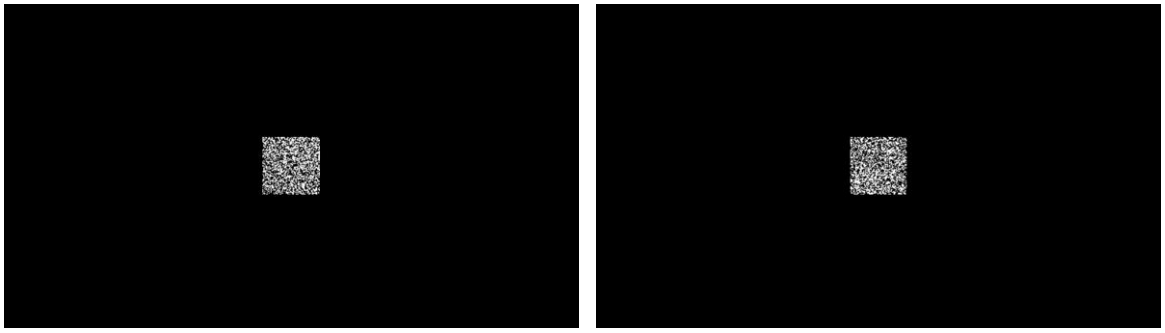
της οθόνης LCD, επιτρέπει την ελεγχόμενη μεταβολή των σημείων πρόσπτωσης του φωτός επί του χρησιμοποιούμενου οπτικού μέσου. Ωστόσο η συσκευή DMD, λόγω των περιορισμένων διαστάσεων και της μεγαλύτερης ανάλυσής της, διευκολύνει την επίλυση των προαναφερθέντων ζητημάτων, προσφέροντας μεγαλύτερη ευελιξία κατά την παραγωγή των απαιτούμενων challenges. Επιπροσθέτως, λόγω του διαφορετικού τρόπου λειτουργίας της, παρουσιάζει λιγότερες απώλειες σε σύγκριση με την οθόνη LCD, ελαττώνοντας και το επίπεδο του εισερχόμενου θορύβου[9].

Θα πρέπει επίσης να σημειωθεί ότι η απεικονιστική κάμερα με την οποία καταγράφονται οι παραγόμενες πειραματικές αποκρίσεις διαθέτει ένα ενσωματωμένο σύστημα ψύξης με Peltier, το οποίο καθιστά δυνατό τόσο τον έλεγχο όσο και την μείωση της θερμοκρασίας σε πραγματικό χρόνο. Συγκεκριμένα, η θερμοκρασία λειτουργίας της κάμερας καθόλη την διάρκεια των πειραματικών μετρήσεων διατηρήθηκε ίση με 10^oC, γεγονός που επέτρεψε την αισθητή καταστολή του θορύβου dark current.

6.1 Προκαταρκτική Αξιολόγηση Διάταξης

Το πρώτο σκέλος της παρούσας διερεύνησης εστιάζει στην προκαταρκτική αξιολόγηση της επίδοσης που παρουσιάζει η εικονιζόμενη πειραματική διάταξη ως προς τις 3 βασικές ιδιότητες μιας PUF.

Για τον σκοπό αυτόν λοιπόν αρχικά κατασκευάστηκε ένα σύνολο από 10000 διαφορετικές διεγέρσεις, κάθε μία από τις οποίες αντιστοιχεί και σε μια δυαδική εικόνα, όπως αυτές των φωτογραφιών του σχήματος 6.2.



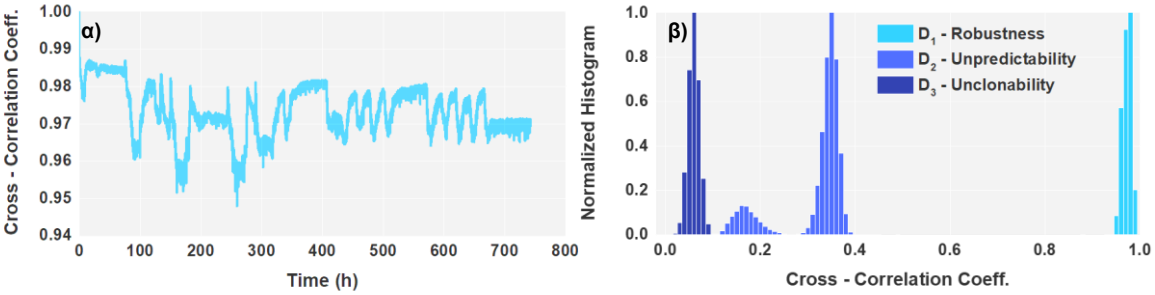
Σχήμα 6.2: Ενδεικτικά παραδείγματα διεγέρσεων με ανάλυση 64x64 micromirrors, εκ των οποίων μόνο το 1/2 του συνολικού πλήθους τους συνεισφέρει στην τελική ακτινοβόληση του diffuser.

Αναλυτικότερα, κάθε εφαρμοζόμενη διέγερση είναι ένα μοναδικό ασπρόμαυρο μοτίβο 64×64 εικονοστοιχείων, το οποίο τοποθετείται στο κέντρο μιας δυαδικής εικόνας με συνολική ανάλυση 640×340 pixels. Οι δύο πιθανές τιμές φωτεινότητας εντός του μοτίβου αυτού είναι πάντα ισοπληθείς και κατανεμημένες έτσι, ώστε τα παραγόμενα challenges να προκύπτουν ανά δύο ασυσχέτιστα. Η περιβάλλουσα περιοχή του εν λόγω μοτίβου από την άλλη πλευρά παραμένει πάντοτε μηδενική. Με άλλα λόγια, οι μοναδιαίες τιμές από την δυαδική εικόνα εκάστου challenge στρέφουν κατά 10^o έναν μοναδικό συνδυασμό από $64^2/2 = 2048$ micromirrors, τα οποία ανήκουν σε ένα σταθερό πλέγμα 64×64 μικροκατόπτρων της χρησιμοποιούμενης DMD. Ο εν λόγω συνδυασμός μικροκατόπτρων είναι και αυτός που συνεισφέρει στην τελική ακτινοβόληση του diffuser.

[9] Η οθόνη LCD εμφανίζει αυξημένα επίπεδα θορύβου και απωλειών σε σχέση με την συσκευή DMD λόγω των επιπλέον πολωτών, κρυστάλλων, φίλτρων Bayer κλπ που περιέχει.

Έπειτα λήφθηκαν τρία διαφορετικά σύνολα από speckle patterns, οι κηλίδες των οποίων καλύπτουν ~36 εικονοστοιχεία των καταγραφόμενων εικόνων, όπως αυτό επιβάλλεται από τα αποτελέσματα του προηγούμενου κεφαλαίου. Συγκεκριμένα, το πρώτο σύνολο δεδομένων D_1 περιέχει 15374 επαναληπτικές λήψεις της ίδιας απόκρισης r, οι οποίες παράχθηκαν εφαρμόζοντας μία μόνο διέγερση c σε έναν και μοναδικό diffuser p για έναν περίπου μήνα: $D_1 = \{r_i,c_j,p_k \mid 1 \leq i \leq 15374, j = 1, k = 1\}$, όπου $r_i \in \mathbb{R}^{N1 \times N2}$ με $N_1 = 1200$ και $N_2 = 800$. Το εν λόγω σύνολο περιλαμβάνει όλες τις μετρήσεις που χρειάζονται για να μελετηθεί η επίδραση του θορύβου πάνω στην επαναληψιμότητα των παραγόμενων αποκρίσεων και να αξιολογηθεί η επίδοση της χρησιμοποιούμενης διάταξης ως προς την ιδιότητα του Robustness. Από την άλλη μεριά, το δεύτερο σύνολο δεδομένων D_2 περιέχει 10000 διαφορετικές αποκρίσεις r, οι οποίες παράχθηκαν εφαρμόζοντας κάθε διαθέσιμο challenge c μία μόνο φορά σε έναν και μοναδικό diffuser p: $D_2 = \{r_i,c_j,p_k \mid i = 1, 1 \leq j \leq 10000, k = 1\}$. Το σύνολο αυτό περιλαμβάνει όλες τις μετρήσεις που απαιτούνται, ώστε να αξιολογηθεί η επίδοση της διάταξης ως προς την ιδιότητα του Unpredictability. Τέλος, το τρίτο σύνολο δεδομένων D_3 περιλαμβάνει 10000 διαφορετικές αποκρίσεις r, οι οποίες παράχθηκαν εφαρμόζοντας μία και μοναδική διέγερση c σε 10000 διαφορετικούς diffuser p από μία μόνο φορά: $D_3 = \{r_i,c_j,p_k \mid i = 1, j = 1, 1 \leq k \leq 10000\}$. Το σύνολο αυτό περιέχει τις μετρήσεις που καθιστούν εφικτή την διερεύνηση της τελευταίας ιδιότητας, αυτής του Unclonability.

Κατόπιν, προσδιορίστηκαν, κατά τα γνωστά, όλοι οι συντελεστές διασυσχέτισης Pearson μεταξύ των κανονικοποιημένων πειραματικών αποκρίσεων εκάστου dataset ξεχωριστά. Εν προκειμένω, στο γράφημα α) του σχήματος 6.3 επιδεικνύεται η χρονική εξέλιξη του εν λόγω συντελεστή, όπως αυτός υπολογίστηκε μεταξύ του πρώτου speckle pattern από το dataset D_1 και των 15373 επαναληπτικών λήψεών του. Αντίστοιχα, στο γράφημα β) του ίδιου σχήματος παρουσιάζονται οι συγκεντρωτικές κατανομές των συντελεστών και από τα τρία σύνολα δεδομένων, υπό την μορφή κανονικοποιημένων ιστογραμμάτων, ενώ στον πίνακα 11 ακολούθως συνοψίζονται και τα βασικά στατιστικά τους μέτρα.



Σχήμα 6.3: α) Συντελεστής διασυσχέτισης Pearson, όπως αυτός υπολογίστηκε μεταξύ της πρώτης εικόνας του dataset D_1 και των 15373 επαναληπτικών λήψεων του, ως συνάρτηση του χρόνου. **β)** Οι κατανομές των συντελεστών διασυσχέτισης Pearson, όπως αυτές εξήχθησαν από τα 15374 speckles που λήφθηκαν υπό πανομοιότυπες συνθήκες ακτινοβόλησης (Robustness), τα 10000 speckles που προέκυψαν από την εφαρμογή όλων των πειραματικών διεγέρσεων σε έναν diffuser (Unpredictability) και τα 10000 speckles που παράχθηκαν εφαρμόζοντας ένα μόνο challenge σε 10000 διαφορετικούς diffuser (Unclonability).

Πίνακας 11: Στατιστικές τιμές των συντελεστών διασυσχέτισης Pearson, όπως αυτές υπολογίστηκαν για κάθε σύνολο δεδομένων.

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_1	+0.9324	+0.9943	+0.9771	0.0091
D_2	-0.0115	+0.4848	+0.3099	0.0711
D_3	-0.0307	+0.0934	+0.0303	0.0115

Όπως φαίνεται λοιπόν και από το διάγραμμα 6.3α, η τιμή του συντελεστή διασυσχέτισης Pearson καταδεικνύει μια συστηματική εναλλαγή συμπεριφοράς συναρτήσει του χρόνου, παρουσιάζοντας τέσσερα διαστήματα ~4.5 ημερών με έντονες διακυμάνσεις και πέντε περιοχές ~2 ημερών με υψηλότερη ευστάθεια. Η παρατηρούμενη αυτή εναλλαγή που έχει εβδομαδιαία βάση, μπορεί να αποδοθεί στην αύξηση του περιβαλλοντικού θορύβου κατά την διάρκεια των εργάσιμων ημερών, όπου οι εργαστηριακές συνθήκες είναι περισσότερο ευμετάβλητες και το υπό μελέτη σύστημα λιγότερο απομονωμένο. Εντούτοις, καθόλη την διάρκεια των πειραματικών μετρήσεων ο εν λόγω συντελεστής διατηρείται σε ένα άκρως ικανοποιητικό επίπεδο, το οποίο παλινδρομεί γύρω από το 0.97 και δεν υποχωρεί κάτω του 0.94. Το εν λόγω γεγονός τεκμηριώνει μια σαφή και σταθερή ομοιότητα μεταξύ των καταγραφόμενων αποκρίσεων, η οποία εκτιμάται ότι εξασφαλίζει την επαναληψιμότητα των εξαγόμενων δυαδικών ακολουθιών σε μακροπρόθεσμο μάλιστα ορίζοντα.

Όσον αφορά τώρα το διάγραμμα του σχήματος 6.3β, όπως μπορεί να παρατηρηθεί, τα δύο ζεύγη των εικονιζόμενων κατανομών, Robustness - Unpredictability και Robustness - Unclonability, δεν παρουσιάζουν οποιαδήποτε επικάλυψη στα αντίστοιχα ιστογράμματά τους, ελαχιστοποιώντας τη πιθανότητα να προκύψουν ψευδώς θετικά ή ψευδώς αρνητικά αποτελέσματα. Συνεπώς, η σημαντικότερη ανεπάρκεια της προηγούμενης διάταξης έχει ήδη αντιμετωπιστεί με επιτυχία. Εντούτοις όμως, ενώ η κατανομή από τα δεδομένα του Unclonability αντιστοιχεί σε αποκρίσεις, οι οποίες θεωρούνται πλήρως ασυσχέτιστες, το ιστόγραμμα του unpredictability εμφανίζει υψηλό μέσο όρο τιμών, υποδηλώνοντας ότι η πλειοψηφία των speckles που παράγονται από διαφορετικές διεγέρσεις συνεχίζουν να προκύπτουν αρκετά όμοιες.

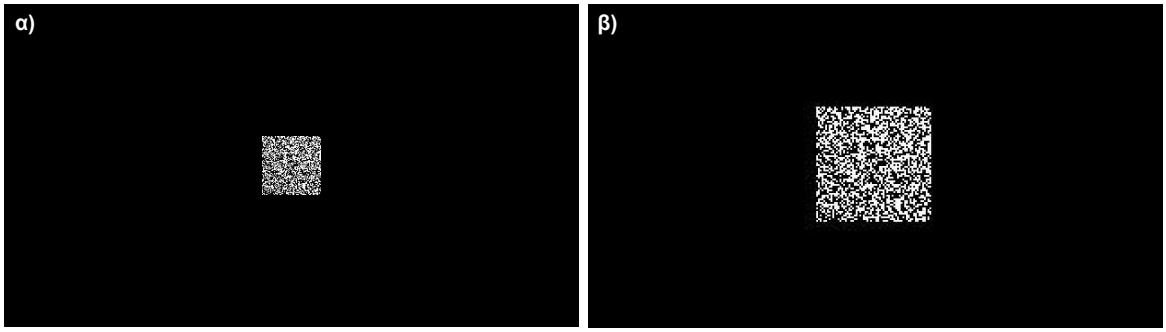
Σε αυτό το πλαίσιο λοιπόν, εν συνεχεία αποπειράθηκε η ενίσχυση της ανομοιότητας των παραγόμενων αποκρίσεων, μέσω της αύξησης της ανάλυσης των εφαρμοζόμενων challenges και της μεγέθυνσης του προβαλλόμενου ειδώλου τους πάνω στο υπό μελέτη ανομοιογενές υλικό.

6.2 Επίδραση Διαστάσεων Διέγερσης

Εν συντομία, η περαιτέρω ενίσχυση της ασφάλειας του συστήματος ως προς την ιδιότητα του unpredictability επετεύχθη με την εφαρμογή ενός εναλλακτικού συνόλου από 10000 διαφορετικές διεγέρσεις με συνολική ανάλυση 640×340 pixels και κεντρικά μοτίβα, τα οποία έχουν πανομοιότυπα γεωμετρικά γνωρίσματα με αυτά της προηγούμενης ενότητας αλλά διπλάσια ανάλυση. Τα καινούρια αυτά challenges, τα οποία ουσιαστικά καλύπτουν ένα σταθερό πλέγμα 128×128 micromirrors επί της χρησιμοποιούμενης συσκευής DMD, επιτρέπουν τον τετραπλασιασμό της επιφάνειας ακτινοβόλησης του δείγματος, χωρίς να καταστεί ουδεμία τροποποίηση της εικονιζόμενης πειραματικής διάταξης απαραίτητη.

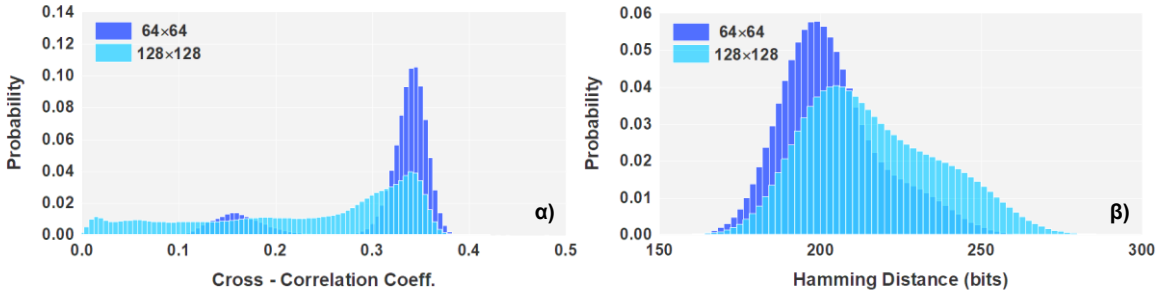
Για τις ανάγκες της τρέχουσας ενότητας λοιπόν, αρχικά παράχθηκαν τα προαναφερθέντα δυαδικά challenges, μετατρέποντας έκαστο μεμονωμένο εικονοστοιχείο από το μοτίβο κάθε υπάρχουσας διέγερσης σε ένα υπερ-pixel διαστάσεων 2×2. Εν συνεχεία, λήφθησαν οι αντίστοιχες πειραματικές αποκρίσεις των διεγέρσεων αυτών, απομακρύνοντας την κάμερα απεικόνισης από την έξοδο του diffuser, ώστε το μέγεθος των καταγραφόμενων speckles να διατηρηθεί ίσο με ~6 pixels ανά διάσταση. Κατόπιν, προσδιορίστηκαν οι συντελεστές διασυσχέτισης Pearson μεταξύ όλων των ληφθέντων πειραματικών speckles, η συγκεντρωτική κατανομή των οποίων επιδεικνύεται στο διάγραμμα α) του σχήματος 6.5. Στο ίδιο γράφημα έχει επίσης συμπεριληφθεί και το ιστόγραμμα των συντελεστών που

προέκυψαν από τις αποκρίσεις της προηγούμενης ενότητας, όπως αυτές παράχθηκαν μέσω των challenges με μοτίβα διαστάσεων 64×64.



Σχήμα 6.4: Ενδεικτικά παραδείγματα διεγέρσεων με ανάλυση **α)** 64x64 και **β)** 128x128 micromirrors, εκ των οποίων μόνο το 1/2 του συνολικού πλήθους τους συνεισφέρει στην τελική ακτινοβόληση του diffuser. Τα γεωμετρικά χαρακτηριστικά και των δύο δυαδικών μοτίβων είναι πανομοιότυπα.

Έπειτα, από τις 10000 πειραματικές αποκρίσεις που καταγράφηκαν υπό την εφαρμογή των καινούριων αυτών διεγέρσεων επιλέχθηκε ένα αντιπροσωπευτικό υποσύνολο 2000 εικόνων, από τις οποίες εξήχθησαν μέσω της τεχνικής RBM 2000 σύνολα 2000 δυαδικών ακολουθιών μήκους 511 bits. Ύστερα, υπολογίστηκαν όλες οι αποστάσεις Hamming για κάθε σύνολο ακολουθιών ξεχωριστά και κατασκευάστηκε ένα συγκεντρωτικό ιστόγραμμα, το οποίο παρουσιάζεται στο διάγραμμα του σχήματος 6.5β. Να σημειωθεί ότι η διαδικασία αυτή επαναλήφθηκε και για το σύνολο των αποκρίσεων που προήλθαν από τις διεγέρσεις με ανάλυση 64×64 μικροκατόπτρων, η κατανομή των οποίων επιδεικνύεται στο ίδιο διάγραμμα.



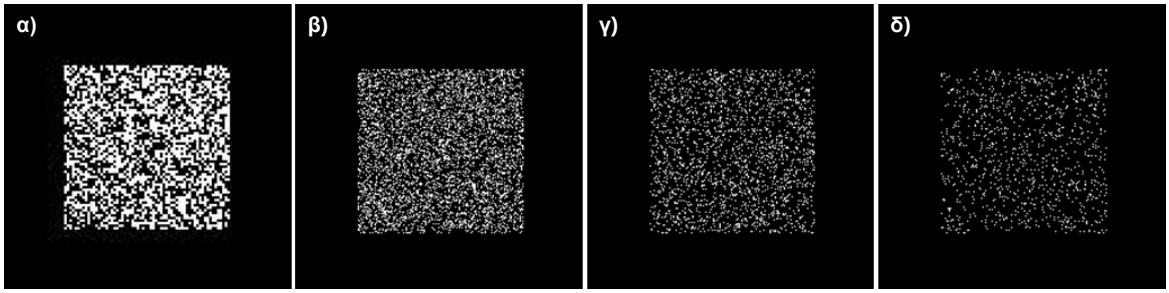
Σχήμα 6.5: α) Οι κατανομές των συντελεστών διασυσχέτισης Pearson, όπως αυτές εξήχθησαν για τα δύο dataset αποκρίσεων που λήφθηκαν υπό την εφαρμογή όλων των διαθέσιμων διεγέρσεων, οι οποίες αντιστοιχούν σε μοτίβα διαστάσεων 64×64 και 128×128 micromirrors. **β)** Οι αντίστοιχες αποστάσεις Hamming μεταξύ των δυαδικών ακολουθιών, μήκους 511 bits, που εξήχθησαν από ένα υποσύνολο 2000 speckles για κάθε dataset αποκρίσεων.

Όπως φαίνεται λοιπόν από τα ιστογράμματα των συντελεστών διασυσχέτισης Pearson, τα οποία αντιπροσωπεύουν $_{10000}C_2$ συγκρίσεις έκαστο, η κατανομή από τα μοτίβα με ανάλυση 128×128 παρουσιάζει μια εντονότερη και συνεχή ουρά προς την μηδενική τιμή, υποδηλώνοντας ότι ένα επαρκές πλήθος πειραματικών αποκρίσεων προκύπτει πλέον αρκούντως ασυσχέτιστο. Συνεπώς, η αύξηση της ανάλυσης των εφαρμοζόμενων διεγέρσεων και η μεγέθυνση του ειδώλου τους επί του υπό μελέτη ανομοιογενούς υλικού οδηγεί στην αυξανόμενη διαφοροποίηση των παραγόμενων πειραματικών αποκρίσεων, επιτρέποντας τη βελτίωση της απόδοσης του συστήματος ως προς τη ζητούμενη ιδιότητα του unpredictability. Το εν λόγω αποτέλεσμα επιβεβαιώνεται και από τα αντίστοιχα ιστογράμματα των αποστάσεων Hamming, εκ των οποίων η κατανομή από τα challenges με ανάλυση 128×128 micromirrors εμφανίζει εντονότερη θετική ασυμμετρία έναντι της κατανομής από τα challenges διαστάσεων 64x64, υποδεικνύοντας δυαδικές ακολουθίες με περισσότερες διαφοροποιήσεις.

6.3 Επίδραση Ποσοστού Ενεργών Micromirrors

Στο πλαίσιο της παρούσας ενότητας διερευνάται πειραματικά η επίδραση του ποσοστού των «ενεργών» micromirrors πάνω στην συνολική απόδοση της χρησιμοποιούμενης διάταξης ως ένα ολοκληρωμένο σύστημα PUF. Η εν λόγω μελέτη διεξήχθη εστιάζοντας μόνο στις ιδιότητες του Robustness και του Unpredictability, καθώς η προκαταρκτική ανάλυση των δεδομένων από το dataset D_3 οδήγησε σε αποτελέσματα που θεωρήθηκαν αρκούντως ικανοποιητικά.

Για αυτόν τον σκοπό λοιπόν κατασκευάστηκαν 4 διαφορετικά σετ δυαδικών εικόνων, τα οποία ουσιαστικά περιλαμβάνουν 10^4 challenges με ανάλυση μοτίβων $N^2 = 128\times128$ micromirrors, και αναλογία «ενεργών» μικροκατόπτρων ίση με το 1/2, το 1/4, το 1/8 και το 1/16 του συνολικού τους πλήθους. Εν συνεχεία, για κάθε σετ διεγέρσεων λήφθηκαν δυο διαφορετικά σύνολα αποκρίσεων, με ανάλυση 1200×800 pixels και μέγεθος κηλίδων ~ 6 pixels ανά διάσταση, όπως αυτό υπαγορεύεται από τα ευρήματα του προηγούμενου κεφαλαίου.



Σχήμα 6.6: Ενδεικτικό παράδειγμα διεγέρσεων με ανάλυση 128x128 micromirrors, εκ των οποίων μόνο **α)** το 1/2, **β)** το 1/4, **γ)** το 1/8 και **δ)** το 1/16 του συνολικού πλήθους τους συνεισφέρει στην τελική ακτινοβόληση του diffuser.

Ειδικότερα, το πρώτο σύνολο δεδομένων περιέχει 2000 καταγραφές της ίδιας απόκρισης r, οι οποίες προέκυψαν εφαρμόζοντας ένα και μοναδικό challenge c σε έναν μόνο diffuser p για ~45 συναπτές ώρες. Το εν λόγω σύνολο ουσιαστικά περιέχει όλες τις μετρήσεις που χρειάζονται για να διερευνηθεί η επίδραση της αναλογίας των «ενεργών» κατόπτρων πάνω στην επαναληψιμότητα του μελετούμενου συστήματος και να ποσοτικοποιηθεί η ιδιότητα του Robustness. Από την άλλη πλευρά, το δεύτερο σύνολο δεδομένων περιέχει 10000 διαφορετικές αποκρίσεις r, οι οποίες παράχθηκαν εφαρμόζοντας κάθε διαθέσιμο challenge c εκάστου σετ διεγέρσεων μία μόνο φορά σε έναν και μοναδικό diffuser p. Το σύνολο αυτό περιλαμβάνει όλες τις εικόνες των speckle patterns που απαιτούνται, ώστε να αξιολογηθεί η μοναδικότητα των ακολουθιών που προκύπτουν από έκαστη αναλογία και να ποσοτικοποιηθεί η ιδιότητα του Unpredictability. Επομένως, λαμβάνοντας υπόψιν ότι ο αριθμός των «ενεργών» μικρο-κατόπτρων ισούται με το συνολικό άθροισμα s όλων των μοναδιαίων ψηφίων που απαρτίζουν το μοτίβο κάθε εφαρμοζόμενου challenge, $c_i \in \{0,1\}^{N\times N}$ όπου N = 128, τα σύνολα αποκρίσεων που χρησιμοποιήθηκαν στο πλαίσιο της παρούσας διερεύνησης μπορούν να συνοψιστούν ακολούθως:

- $D_4 = \{r_i,c_j,p_k \mid 1 \le i \le 2000, j = 1, k = 1\}$ και $D_5 = \{r_i,c_j,p_k \mid i =1, 1 \le j \le 10000, k = 1\}$ τα σύνολα αποκρίσεων για το robustness και το unpredictability με $s = N^2/2$.
- $D_6 = \{r_i,c_j,p_k \mid 1 \le i \le 2000, j = 1, k = 1\}$ και $D_7 = \{r_i,c_j,p_k \mid i =1, 1 \le j \le 10000, k = 1\}$ τα σύνολα αποκρίσεων για το robustness και το unpredictability με $s = N^2/4$.

- $D_8 = \{r_i,c_j,p_k \mid 1 \leq i \leq 2000, j = 1, k = 1\}$ και $D_9 = \{r_i,c_j,p_k \mid i =1, 1 \leq j \leq 10000, k = 1\}$ τα σύνολα αποκρίσεων για το robustness και το unpredictability με $s = N^2/8$.
- $D_{10} = \{r_i,c_j,p_k \mid 1 \leq i \leq 2000, j = 1, k = 1\}$ και $D_{11} = \{r_i,c_j,p_k \mid i =1, 1 \leq j \leq 10000, k = 1\}$ τα σύνολα αποκρίσεων για το robustness και το unpredictability με $s = N^2/16$.

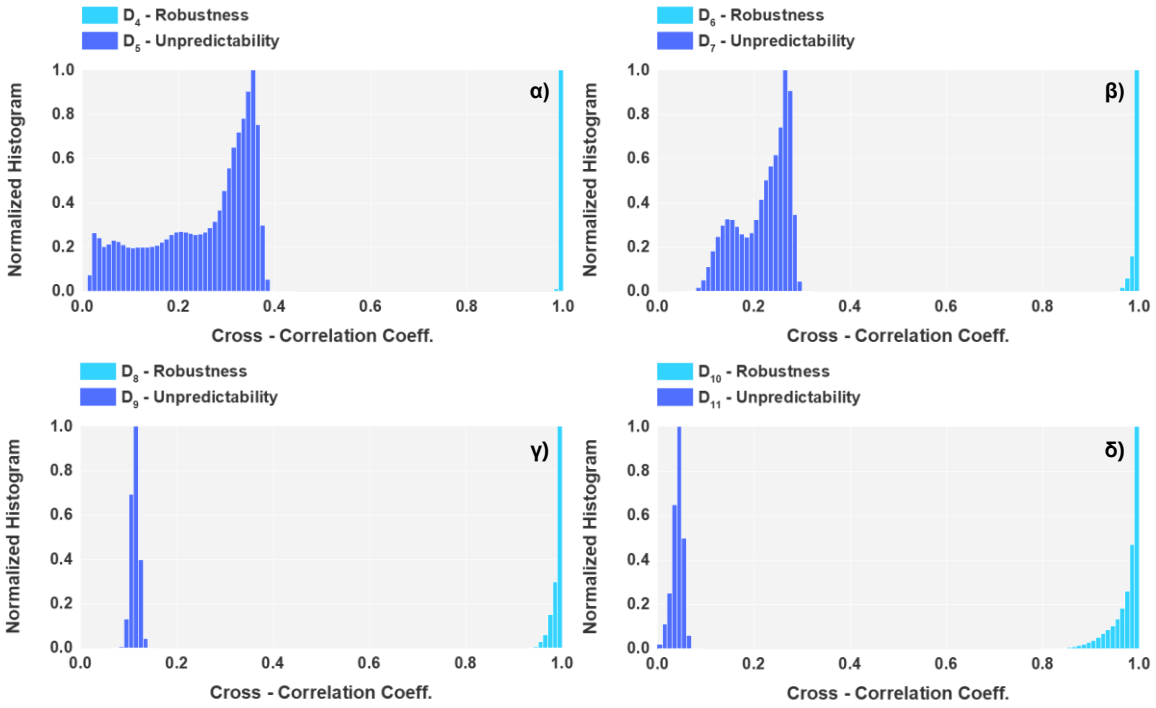
Θα πρέπει να σημειωθεί, ότι καθώς το ποσοστό των «ενεργών» μικρο-κατόπτρων από την DMD μεταβάλλεται, καθίσταται απαραίτητη και η τροποποίηση του exposure time της κάμερας, ούτως ώστε η μέση ένταση των λαμβανόμενων speckle patterns να διατηρείται σταθερή. Αντίθετα, η απόσταση της κάμερας από την έξοδο του diffuser παρέμεινε σταθερή καθόλη την διάρκεια των πειραματικών μετρήσεων, αφού η συνολική ανάλυση των διεγέρσεων, άρα και η τελευταία κόρη εξόδου του συστήματος, παρέμεινε αμετάβλητη.

6.3.1 Συντελεστές Διασυσχέτισης Pearson

Ακολουθώντας την μεθοδολογία των προηγούμενων ενοτήτων αρχικά υπολογίστηκαν οι συντελεστές διασυσχέτισης Pearson μεταξύ όλων των κανονικοποιημένων αποκρίσεων εκάστου συνόλου δεδομένων. Έπειτα, οι κατανομές που προέκυψαν από την διαδικασία αυτή ομαδοποιήθηκαν σε ζεύγη ανά χρησιμοποιούμενη αναλογία «ενεργών» κατόπτρων και αναπαραστάθηκαν γραφικά υπό την μορφή κανονικοποιημένων ιστογραμμάτων, τα οποία παρουσιάζονται στα γραφήματα του σχήματος 6.7.

Αναλυτικότερα, οι κατανομές του Robustness, όπως αυτές επιδεικνύονται στο παρακάτω σχήμα, αντιπροσωπεύουν ${}_{2000}C_2 = 1999000$ συγκρίσεις, οι οποίες πραγματοποιήθηκαν μεταξύ των 2000 επαναληπτικών μετρήσεων που απαρτίζουν τα σύνολα D_4, D_6, D_8 και D_{10}. Από την άλλη μεριά, οι αντίστοιχες κατανομές Unpredictability παριστάνουν ${}_{10000}C_2 = 49995000$ συγκρίσεις από τις 10000 διαφορετικές αποκρίσεις των συνόλων D_5, D_7, D_9 και D_{11}.

Όπως λοιπόν μπορεί να παρατηρηθεί από τα παρακάτω αποτελέσματα, όταν το πλήθος των «ενεργών» κατόπτρων αυξάνεται, οι κατανομές των συντελεστών διασυσχέτισης από τα δεδομένα του Robustness επιδεικνύουν μια εντονότερη αρνητική ασυμμετρία, η οποία οδηγεί στη σταδιακή πτώση όλων των αντιστοίχων στατιστικών μεγεθών τους, πλην της τυπικής απόκλισης. Η εν λόγω συμπεριφορά, η οποία αντικατοπτρίζει την ισχυροποίηση του περιβαλλοντικού θορύβου και την ενίσχυση της επιρροής του πάνω στην αναπαραγωγιμότητα των καταγραφόμενων αποκρίσεων, μπορεί να ερμηνευθεί ως ακολούθως: όταν ο αριθμός των «ενεργών» μικρο-κατόπτρων φθίνει, το μέγεθος των λευκών συσσωματωμάτων στις εικόνες των εφαρμοζόμενων διεγέρσεων συρρικνώνεται και η συνολική επιφάνεια ακτινοβόλησης του diffuser διασπάται σε επιμέρους περιοχές με μειούμενο εμβαδόν και μεγαλύτερη ενδιάμεση απόσταση. Ως εκ τούτου, οποιαδήποτε μετατόπιση της δέσμης που μπορεί να προκληθεί κατά την διάρκεια της πειραματικής διαδικασίας επιφέρει ισχυρότερες διαφοροποιήσεις στις επαναληπτικές λήψεις των speckles, αφού η κοινή επιφάνεια ακτινοβόλησης μεταξύ δύο διαδοχικών μετρήσεων μειώνεται και τα σημεία πρόσπτωσης επί του μέσου μεταβάλλονται. Ταυτόχρονα όμως, η ίδια μείωση των κοινών σημείων πρόσπτωσης του φωτός επί του diffuser ενισχύει αναλόγως και την ανομοιότητα των αποκρίσεων που παράγονται από διαφορετικές εφαρμοζόμενες διεγέρσεις: όσο το πλήθος των «ενεργών» κατόπτρων μειώνεται, οι αντίστοιχες κατανομές Unpredictability μετατοπίζονται σταδιακά προς την μηδενική τιμή, εμφανίζοντας μικρότερο μέσο όρο και στενότερο εύρος.



Σχήμα 6.7: Οι κατανομές των συντελεστών διασυσχέτισης Pearson, όπως αυτές εξήχθησαν από τα 2000 speckles που λήφθηκαν υπό πανομοιότυπες συνθήκες ακτινοβόλησης (Robustness) και τα 10000 speckles που προέκυψαν εφαρμόζοντας όλες τις πειραματικές διεγέρσεις (Unpredictability), για πλήθος ενεργών κατόπτρων ίσο με **α)** $N^2/2$, **β)** $N^2/4$, **γ)** $N^2/8$ και **δ)** $N^2/16$.

Ακολούθως, στους πίνακες 12 και 13 συνοψίζονται τα βασικά στατιστικά μέτρα των εν λόγω κατανομών.

Πίνακας 12: Στατιστικές τιμές των συντελεστών διασυσχέτισης Pearson, όπως αυτές υπολογίστηκαν για κάθε σύνολο δεδομένων robustness

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_4	+0.9865	+0.9997	+0.9961	0.0024
D_6	+0.9548	+0.9997	+0.9934	0.0067
D_8	+0.9326	+0.9996	+0.9897	0.0102
D_{10}	+0.8065	+0.9994	+0.9735	0.0291

Πίνακας 13: Στατιστικές τιμές των συντελεστών διασυσχέτισης Pearson, όπως αυτές υπολογίστηκαν για κάθε σύνολο δεδομένων unpredictability.

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_5	-0.0104	+0.4207	+0.2366	0.1064
D_7	+0.0457	+0.3163	+0.2184	0.0523
D_9	+0.0679	+0.1594	+0.1129	0.0083
D_{11}	-0.0137	+0.0907	+0.0414	0.0111

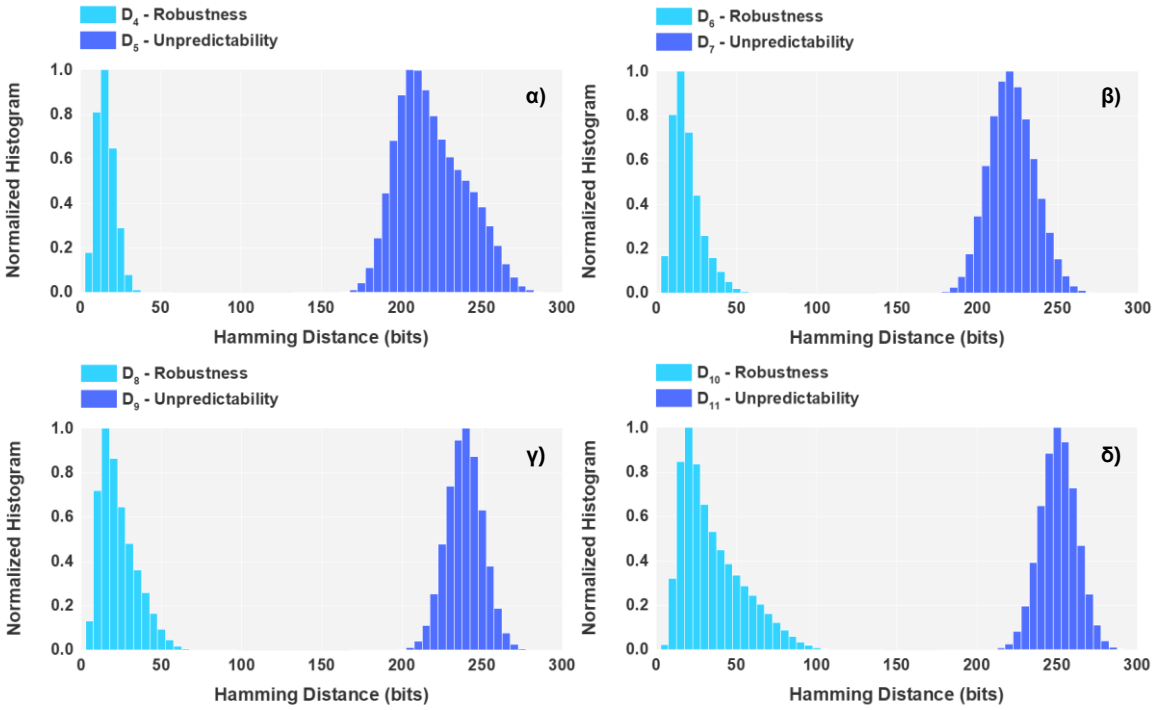
Εν κατακλείδι, από την προκαταρκτική ανάλυση των 8 διαθέσιμων datasets εξάγεται το εξής πρωταρχικό συμπέρασμα: όταν το πλήθος των μικροκατόπτρων που συνεισφέρουν στην τελική ακτινοβόληση του γυάλινου σκεδαστή φθίνει, βελτιώνεται το Unpredictability της χρησιμοποιούμενης διάταξης αλλά υποβαθμίζεται το Robustness της.

6.3.2 Αποστάσεις Hamming και Πιθανότητες Ιδιοτήτων

Εν συνεχεία διερευνήθηκε κατά τα γνωστά η αντίστοιχη επίδοση της παρούσας υλοποίησης σε επίπεδο δυαδικών ακολουθιών, όπως αυτές εξάγονται από τα οκτώ προαναφερθέντα σύνολα δεδομένων, μέσω της τεχνικής RBM. Θα πρέπει να σημειωθεί ότι για την περίπτωση του Unpredictability χρησιμοποιήθηκε μόνο ένα

αντιπροσωπευτικό υποσύνολο από 2000 speckles, το οποίο επιλέχθηκε δειγματοληπτώντας τα αντίστοιχα datasets αποκρίσεων ανά 5 εικόνες.

Συγκεκριμένα, από το dataset D_4 κατασκευάστηκαν 2000 δυαδικές ακολουθίες μήκους 511 bits, θέτοντας μία εκ των διαθέσιμων πειραματικών αποκρίσεων ως εικόνα εγγραφής και θεωρώντας τις υπόλοιπες 1999 ως εισόδους του σταδίου αυθεντικοποίησης. Η διαδικασία αυτή επαναλήφθηκε μέχρις ότου χρησιμοποιηθούν όλα τα speckles ως εικόνα αναφοράς μια φορά, οδηγώντας σε 2000 διαφορετικά σύνολα δυαδικών ακολουθιών, κάθε ένα από τα οποία αντιστοιχεί και σε ένα μοναδικό σετ βοηθητικών δεδομένων. Έπειτα, προσδιορίστηκαν οι αποστάσεις Hamming μεταξύ των δυαδικών ακολουθιών για κάθε σύνολο ξεχωριστά και υπολογίστηκαν οι πιθανότητες του να προκύψουν πανομοιότυπες έξοδοι και από τα δύο στάδια του fuzzy extractor. Με τον ίδιο ακριβώς τρόπο παράχθηκαν 2000 σύνολα 2000 δυαδικών ακολουθιών και από τα υπόλοιπα datasets.



Σχήμα 6.8: Οι κατανομές των αποστάσεων Hamming μεταξύ 2000 δυαδικών ακολουθιών, όπως αυτές εξήχθησαν για πλήθος ενεργών κατόπτρων ίσο με **α)** $N^2/2$, **β)** $N^2/4$, **γ)** $N^2/8$ και **δ)** $N^2/16$.

Εν προκειμένω, στα διαγράμματα του σχήματος 6.8 παρουσιάζονται οι συγκεντρωτικές κατανομές των αποστάσεων Hamming, υπό τη μορφή κανονικοποιημένων ιστογραμμά-των, όπως αυτές προέκυψαν από τις $2000\times({}_{2000}C_2)$ συγκρίσεις που πραγματοποιήθηκαν μεταξύ των δυαδικών ακολουθιών έκαστου συνόλου δεδομένων. Ακολούθως, στους πίνακες 14 και 15 συνοψίζονται οι αντίστοιχες στατιστικές τους τιμές. Όπως φαίνεται λοιπόν από τα εν λόγω αποτελέσματα, όλα τα στατιστικά μεγέθη, όπως αυτά προέκυψαν από κάθε κατανομή αποστάσεων, παρουσιάζουν μια σταδιακή ενίσχυση των αντιστοίχων τιμών τους όταν το πλήθος των «ενεργών» micromirrors αυξάνει. Η σταδιακή αυτή ενίσχυση, η οποία αποδίδεται στην προαναφερθείσα αυξανόμενη ανομοιότητα των παραγόμενων πειραματικών αποκρίσεων, βρίσκεται σε πλήρη συμφωνία με τα συμπεράσματα της προηγούμενης ενότητας, επιβεβαιώνοντας ότι το μεταβαλλόμενο πλήθος των «ενεργών» micromirrors έχει αντιστρόφως ανάλογη επίδραση στις ιδιότητες του Robustness και του Unpredictability. Με άλλα λόγια, όταν ο αριθμός των «ενεργών» micromirrors ελαττώνεται, η συνολική ασφάλεια του

συστήματος ενισχύεται, αλλά ταυτοχρόνως η επαναληψιμότητα και η αξιοπιστία των εξαγόμενων δυαδικών του εξόδων υποβαθμίζεται. Τέλος όπως επιπλέον μπορεί να παρατηρηθεί από τα παρουσιαζόμενα διαγράμματα, όλα τα εικονιζόμενα ζεύγη κατανομών Robustness και Unpredictability, δεν παρουσιάζουν ουδεμία επικάλυψη στα αντίστοιχα ιστογράμματά τους, ελαχιστοποιώντας την πιθανότητα να προκύψουν ψευδώς θετικά ή ψευδώς αρνητικά αποτελέσματα.

Πίνακας 14: Στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν για κάθε σύνολο δεδομένων robustness

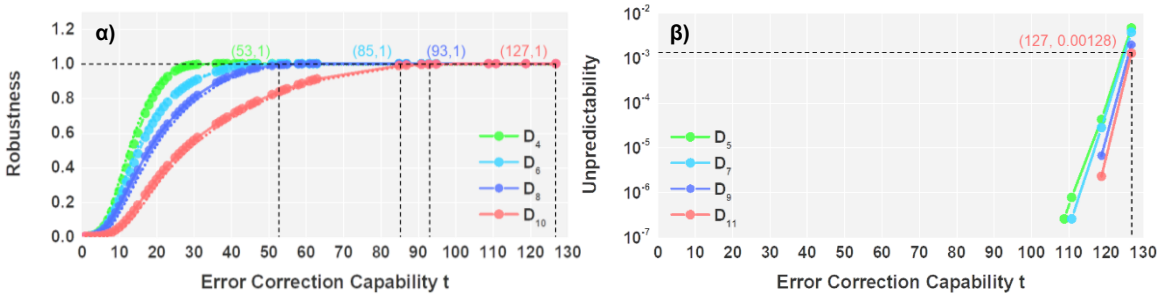
Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_4	0	51	13.6	5.7
D_6	0	77	16.9	9.0
D_8	0	92	21.0	11.4
D_{10}	0	136	32.8	19.2

Πίνακας 15: Στατιστικές τιμές των αποστάσεων Hamming, όπως αυτές υπολογίστηκαν για κάθε σύνολο δεδομένων unpredictability.

Σύνολο Δεδομένων	Ελάχιστη Τιμή	Μέγιστη Τιμή	Μέση Τιμή	Τυπική Απόκλιση
D_5	132	316	216.8	21.0
D_7	140	303	219.4	14.3
D_9	170	306	237.0	11.5
D_{11}	179	321	248.8	11.4

Όσον αφορά τώρα τις πιθανότητες του σχήματος 6.9, αυτές υπολογίστηκαν για έκαστο σύνολο δεδομένων και κάθε δυνατή διορθωτική ικανότητα t του χρησιμοποιούμενου BCH με δύο εναλλακτικούς τρόπους: είτε με την απευθείας καταμέτρηση των δυαδικών εξόδων που προκύπτουν πανομοιότυπες και από τα δύο στάδια του fuzzy extractor (συνεχής γραμμή με σημεία), είτε προσεγγιστικά από τις CDF των άνωθεν αποστάσεων Hamming (διακεκομμένη γραμμή).

Στην περίπτωση του διαγράμματος 6.9α λοιπόν, η τιμή της διορθωτικής ικανότητας t που χρειάζεται ώστε η πιθανότητα του Robustness να σταθεροποιηθεί στη μονάδα αυξάνεται όσο το πλήθος των «ενεργών» micromirrors ελαττώνεται. Όπως μάλιστα παρατηρείται και από την αντίστοιχη γραφική παράσταση, η ζητούμενη μοναδιαία τιμή για τα datasets D_4, D_6, D_8 και D_{10} επιτυγχάνεται όταν $t_4 = 53$ bits, $t_6 = 85$ bits, $t_8 = 93$ bits και $t_{10} = 127$ bits, εκ των οποίων η τελευταία είναι και η μέγιστη δυνατή ικανότητα t που μπορεί να εφαρμοστεί για δεδομένο μήκος δυαδικών ακολουθιών ίσο με 511 bits. Ομοίως, όπως φαίνεται από το διάγραμμα β) του ίδιου σχήματος, η μείωση των «ενεργών» micromirrors έχει ως αποτέλεσμα την διόρθωση όλο και λιγότερων δυαδικών εξόδων από τα αντίστοιχα datasets του Unpredictability, D_5, D_7, D_9 και D_{11}, ακόμη και εάν η διορθωτική ικανότητα t του χρησιμοποιούμενου BCH αυξάνει. Εντούτοις όμως, το γεγονός αυτό δεν υποδηλώνει απαραιτήτως ότι η συνολική απόδοση του υπό μελέτη συστήματος βελτιώνεται: ενώ το Unpredictability των D_5, D_7 και D_9 παραμένει μηδενικό για τις διορθωτικές ικανότητες t_4, t_6 και t_8, η αντίστοιχη πιθανότητα του D_{11} για $t_{10} = 127$ bits προκύπτει ίση με 0.00128. Με άλλα λόγια, ενώ το Unpredictability του συστήματος υπό την εφαρμογή διεγέρσεων $N^2/16$ προκύπτει εν γένει οριακά καλύτερο, η αυξημένη διορθωτική ικανότητα που απαιτείται για την εξασφάλιση της ζητούμενης επαναληψιμότητας του οδηγεί σε πιθανότητα μεγαλύτερη του μηδενός, καθώς για $t \geq 100$ ένας μικρός αριθμός δυαδικών ακολουθιών αντιστοιχίζεται τυχαία σε έγκυρες κωδικές λέξεις του χρησιμοποιούμενου κώδικα BCH.



Σχήμα 6.9: Η πιθανότητα να προκύψουν πανομοιότυπες δυαδικές έξοδοι και από τα δύο στάδια του fuzzy extractor, συναρτήσει της διορθωτικής ικανότητας t του BCH κώδικα για **α)** τα δεδομένα που λήφθηκαν υπό τις ίδιες συνθήκες ακτινοβόλησης (Robustness) και για **β)** τα δεδομένα που λήφθηκαν εφαρμόζοντας όλες τις διαθέσιμες πειραματικές διεγέρσεις (Unpredictability). Σε κάθε περίπτωση, οι διακεκομμένες γραμμές αντιστοιχούν στις προσεγγιστικές καμπύλες που προέκυψαν μέσω των αποστάσεων Hamming, οι οποίες για όλα τα σύνολα δεδομένων του Unpredictability, D_5, D_7, D_9 και D_{11}, ισούνται με το μηδέν.

Εν κατακλείδι, από τις τιμές των παραπάνω πιθανοτήτων μπορεί να εξαχθεί το ακόλουθο τελικό συμπέρασμα: ο αριθμός των «ενεργών» μικροκατόπτρων που συνεισφέρουν στην ακτινοβόληση του χρησιμοποιούμενου diffuser, διαδραματίζει καθοριστικό ρόλο πάνω στην συνολική απόδοση του υπό μελέτη συστήματος, καθώς η επιλογή του επηρεάζει με αντίστροφο τρόπο τις ιδιότητες του Robustness και του Unpredictability· όταν ο εν λόγω αριθμός ελαττώνεται, το Unpredictability του συστήματος βελτιώνεται, ενώ το Robustness αυτού χειροτερεύει. Εντούτοις, ο αριθμός αυτός θα πρέπει να διατηρείται άνω του 6.25%, καθώς η αυξανόμενη διορθωτική ικανότητα που απαιτείται για την αποκατάσταση των ολοένα και περισσότερων σφαλμάτων ενδέχεται να οδηγήσει τυχαία σε λανθασμένη αυθεντικοποίηση ακολουθιών. Σε κάθε περίπτωση όμως, η συνολική απόδοση της εν λόγω διάταξης προκύπτει αισθητά βελτιωμένη σε σύγκριση αυτήν του προηγούμενου κεφαλαίου, αφού η διάρκεια αξιόπιστης λειτουργίας διευρύνθηκε από 20 λεπτά σε 2 μέρες αξιόπιστης λειτουργίας, το σύνολο των εφαρμοζόμενων διεγέρσεων αυξήθηκε κατά 2 τάξεις μεγέθους, ενώ όλα τα ζεύγη ιστογραμμάτων Robustness και Unpredictability δεν παρουσιάζουν ουδεμία επικάλυψη.

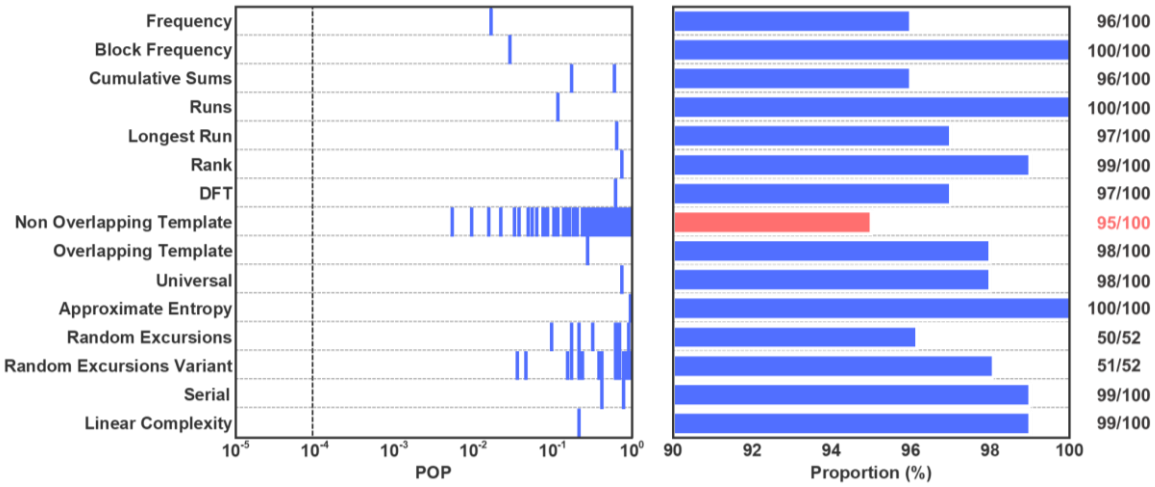
Στο σημείο αυτό θα πρέπει να υπογραμμιστεί, ότι τόσο ο έλεγχος της ύπαρξης ψευδώς θετικών ή αρνητικών αυθεντικοποιήσεων, όσο και η ποσοτικοποίηση των τριών βασικών ιδιοτήτων μιας PUF, αποδεικνύουν την αξιόπιστη λειτουργία της παρούσας διάταξης στο επίπεδο ενός πρώιμου εργαστηριακού πρωτοτύπου. Ωστόσο, η χρησιμοποιούμενη αυτή μεθοδολογία, παρότι επιτρέπει την συγκριτική αξιολόγηση των υπό μελέτη συστημάτων, δεν οδηγεί σε ένα καθολικά αποδεκτό συμπέρασμα ως προς τη τυχαιότητα των εξαγόμενων δυαδικών ακολουθιών τους. Προς αυτή την κατεύθυνση λοιπόν, θεωρήθηκε απαραίτητη μια επιπλέον εξέταση των δυαδικών δεδομένων που παράγονται από τη τεχνική RBM σε επίπεδο εφαρμογής, μέσω των 15 διαγνωστικών ελέγχων του λογισμικού πακέτου NIST. Τα βασικά σημεία των αποτελεσμάτων από την εν λόγω εξέταση παρατίθενται συνοπτικά στην επόμενη υποενότητα, ενώ η αναλυτικότερη παρουσίασή τους μπορεί να βρεθεί στο παράρτημα ΙΙ.

6.4 Αποτελέσματα Ελέγχων NIST

Το τρίτο και τελευταίο σκέλος του παρόντος κεφαλαίου εστιάζει σε ένα ενδεικτικό δείγμα από τα αποτελέσματα που προέκυψαν εφαρμόζοντας τους 15 διαγνωστικούς ελέγχους του NIST σε 10 διαφορετικά αρχεία με μέγεθος 10^9 bits, τα οποία κατασκευάστηκαν μέσω της τεχνικής RBM για κάθε διαθέσιμο σύνολο δεδομένων.

Ειδικότερα, κάθε εξεταζόμενο αρχείο περιέχει την οριζόντια συνένωση 10000 δυαδικών ακολουθιών μήκους 10^5 bits, οι οποίες παράχθηκαν διατηρώντας τον ψευδοτυχαίο πίνακα B της χρησιμοποιούμενης τεχνικής σταθερό, αλλά μεταβάλλοντας τον ψευδοτυχαίο πίνακα αυτής S. Με άλλα λόγια, έκαστο μελετούμενο αρχείο περιλαμβάνει ένα σύνολο ακολουθιών, όπου η διαπλάτυνση του φάσματος των εικόνων από τις οποίες προέρχονται, έχει λάβει χώρα με έναν κοινό πίνακα B, αλλά τα στοιχεία του μιγαδικού φάσματος που τελικά τις απαρτίζουν διαφέρουν.

Εν προκειμένω, στο διάγραμμα του ακόλουθου σχήματος παρουσιάζονται τα συνοπτικά αποτελέσματα ενός εκ των δέκα δυαδικών αρχείων που κατασκευάστηκαν από το σύνολο δεδομένων D_3 (Unclonability), με το αριστερό γράφημα να οπτικοποιεί όλες τις τιμές POP, όπως αυτές προέκυψαν από κάθε εφαρμοζόμενο έλεγχο, και το δεξί να αναπαριστά το αντίστοιχο ποσοστό των επιτυχημένων ακολουθιών του. Θα πρέπει να σημειωθεί ότι για τα τεστ με επιμέρους υποελέγχους, όπως για παράδειγμα το Non-Overlapping Template Test, το παρουσιαζόμενο αυτό ποσοστό αντιστοιχεί στο χειρότερο αποτέλεσμα όλων.



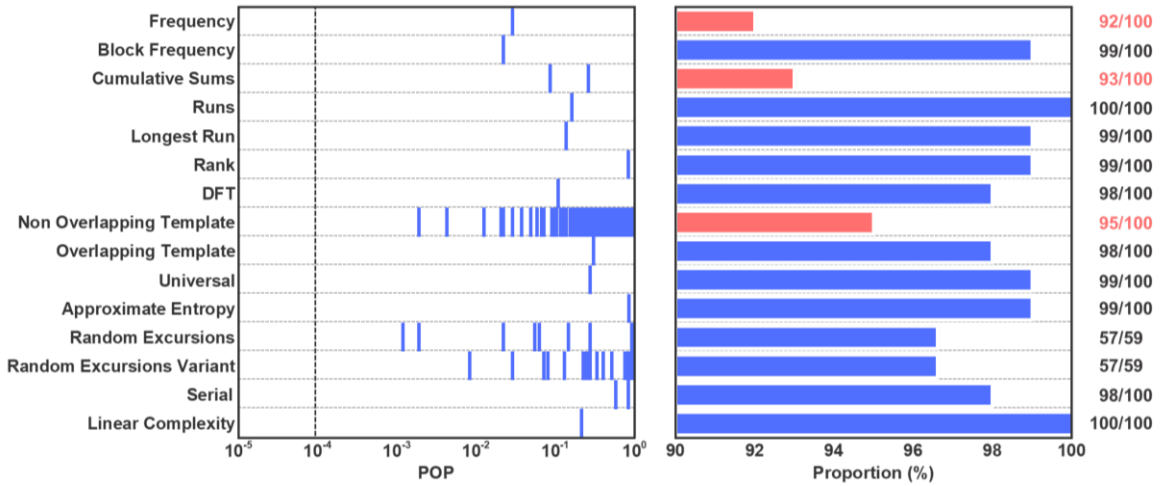
Σχήμα 6.10: Τα συνοπτικά αποτελέσματα που προέκυψαν από την εφαρμογή όλων των διαγνωστικών ελέγχων του πακέτου NIST, επί ενός αρχείου με μέγεθος 100Mbit, το οποίο παράχθηκε μέσω της τεχνικής RBM από το dataset D_3 (Unclonability). Το όριο ανοχής για τις τιμές POP είναι ίσο με 10^{-4}, ενώ το κατώτατο ποσοστό επιτυχημένων ακολουθιών για όλα τα τεστ, πλην των Random Excursions (Variant) είναι 96%. Για τους ελέγχους Random Excursions και Random Excursions Variant το αντίστοιχο ποσοστό είναι 94.23%

Σύμφωνα λοιπόν με το παραπάνω σχήμα, από τους 15 ελέγχους που εφαρμόστηκαν συνολικά, το Non-Overlapping Template τεστ αρχικά διαφαίνεται ότι αποτυγχάνει, καθώς το ποσοστό των επιτυχημένων ακολουθιών για έναν υποέλεγχό του είναι μικρότερο του 96%. Η αποτυχία αυτή όμως μπορεί να αποδοθεί σε κάποιο στατιστικό λάθος, αφού δεν επαναλαμβάνεται κατά τον έλεγχο των 9 υπόλοιπων αρχείων. Ταυτόχρονα, όλες οι τιμές της στήλης POP ξεπερνούν το προκαθορισμένο όριο ανοχής του 10^{-4}. Συμπερασματικά, η συμπεριφορά των δυαδικών ακολουθιών που παράχθηκαν από το σύνολο δεδομένων D_3 προκύπτει αρκούντως τυχαία, με όλους τους ελέγχους του λογισμικού πακέτου NIST να θεωρούνται επιτυχείς.

Ομοίως, στα γραφήματα του σχήματος 6.11 επιδεικνύονται τα αντίστοιχα αποτελέσματα των ίδιων ελέγχων, όπως αυτά προέκυψαν για τις δυαδικές ακολουθίες του dataset D_2. Να υπενθυμιστεί ότι το αναφερθέν σύνολο δεδομένων περιλαμβάνει τις αποκρίσεις που καταγράφηκαν υπό την εφαρμογή 10000 διαφορετικών διεγέρσεων με ανάλυση 64×64 μικρο-καθρεπτών, εκ των οποίων

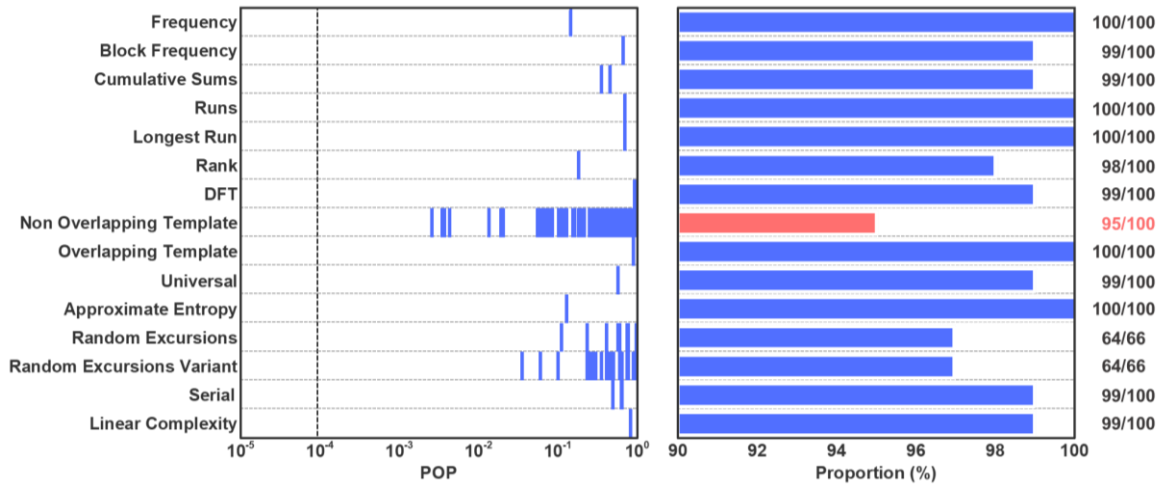
μόνο το 1/2 του συνολικού πλήθους τους συνεισφέρει στη τελική ακτινοβόληση του diffuser.

Όπως παρουσιάζεται λοιπόν στο αντίστοιχο διάγραμμα, το ποσοστό των ακολουθιών που επιτυγχάνουν στο Frequency Test του χρησιμοποιούμενου πακέτου ανέρχεται μόλις στο 92%, ενώ το αντίστοιχο ποσοστό για το Cumulative Sums Test εντοπίζεται εξίσου χαμηλό και ίσο με 93%. Οι τιμές αυτές είναι αισθητά μικρότερες του κατώτατου ορίου επιτυχίας, όπως αυτό καθορίζεται στο 96%, με τα εν λόγω αποτελέσματα μάλιστα να επαναλαμβάνονται και κατά τον έλεγχο των 9 υπολειπόμενων αρχείων. Επομένως οι δυαδικές ακολουθίες που προκύπτουν από το dataset D_2 αποτυγχάνουν συστηματικά τόσο στο Frequency Monobit Test όσο και στο Cumulative Sums Test του NIST, με τη συμπεριφορά τους να απέχει παρασάγγας από αυτήν μιας γεννήτριας πραγματικά τυχαίων αριθμών.

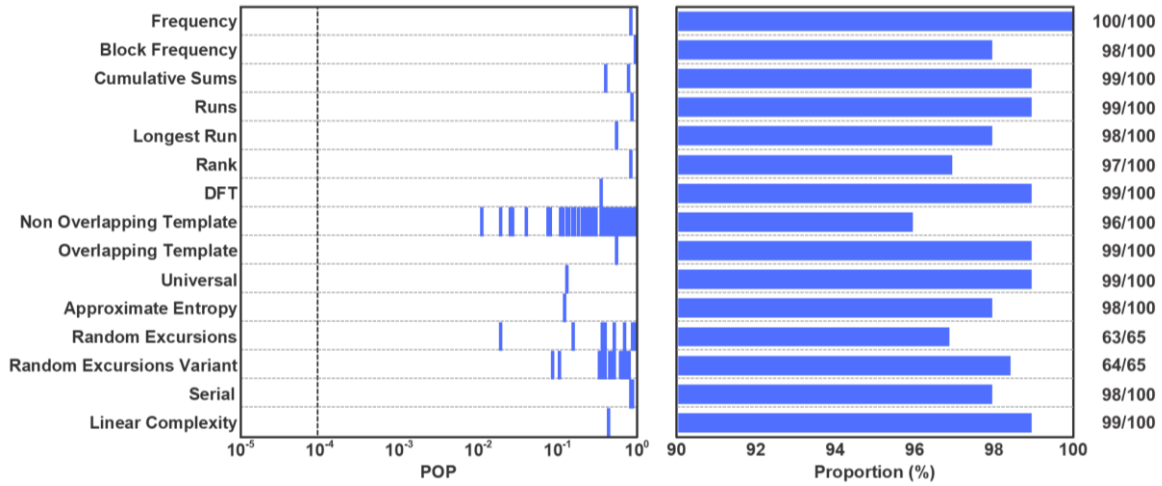


Σχήμα 6.11: Τα συνοπτικά αποτελέσματα που προέκυψαν από την εφαρμογή όλων των διαγνωστικών ελέγχων του πακέτου NIST, επί ενός αρχείου με μέγεθος 100Mbit, το οποίο παράχθηκε μέσω της τεχνικής RBM από το dataset D_2 (αποκρίσεις Unpredictability από διεγέρσεις με ανάλυση 64×64 micromirrors εκ των οποίων μόνο το 1/2 του συνολικού πλήθους τους συνεισφέρει την τελική ακτινοβόληση του diffuser). Το όριο ανοχής για τις τιμές POP είναι ίσο με 10^{-4}, ενώ το κατώτατο ποσοστό επιτυχημένων ακολουθιών για όλα τα τεστ, πλην των Random Excursions (Variant) είναι 96%. Για τους ελέγχους Random Excursions και Random Excursions Variant το αντίστοιχο ποσοστό είναι 94.91%

Ακολούθως στα σχήματα 6.12, 6.13, 6.14, 6.15 παρουσιάζονται τα αποτελέσματα των ελέγχων για τα datasets D_5, D_7, D_9 και D_{11} αντιστοίχως, σύμφωνα με τα οποία όλες οι πειραματικές αποκρίσεις που παράγονται από διεγέρσεις με ανάλυση 128×128 οδηγούν σε αρκούντως τυχαίες δυαδικές ακολουθίες ανεξαιρέτως του πλήθους των ενεργών καθρεπτών.

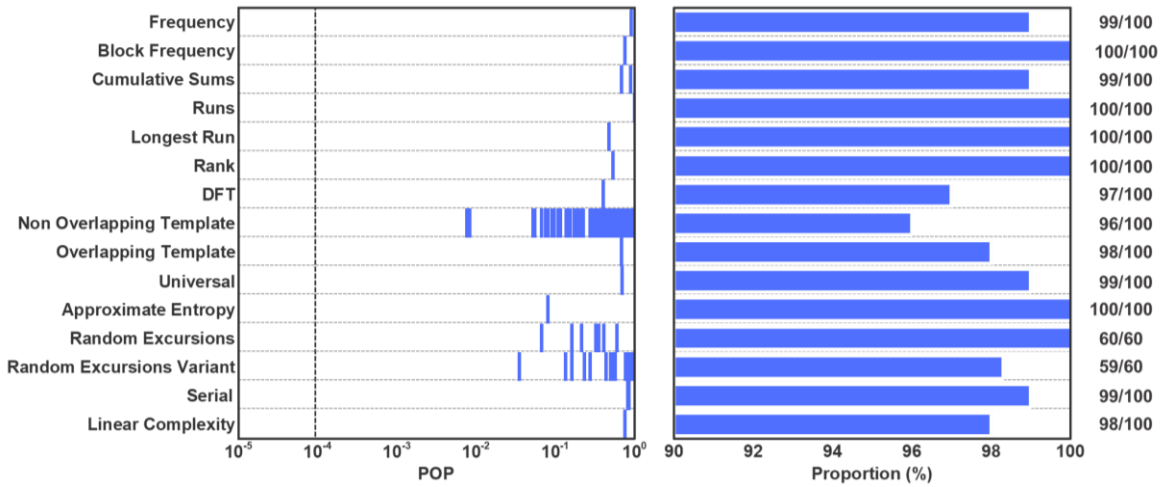


Σχήμα 6.12: Τα συνοπτικά αποτελέσματα που προέκυψαν από την εφαρμογή όλων των διαγνωστικών ελέγχων του πακέτου NIST, επί ενός αρχείου με μέγεθος 100Mbit, το οποίο παράχθηκε μέσω της τεχνικής RBM από το dataset D_5 (αποκρίσεις Unpredictability από διεγέρσεις με ανάλυση 128×128 micromirrors εκ των οποίων μόνο το 1/2 του συνολικού τους πλήθους συνεισφέρει την τελική ακτινοβόληση του diffuser). Το όριο ανοχής για τις τιμές POP είναι ίσο με 10^{-4}, ενώ το κατώτατο ποσοστό επιτυχημένων ακολουθιών για όλα τα τεστ, πλην των Random Excursions (Variant) είναι 96%. Για τους ελέγχους Random Excursions και Random Excursions Variant το αντίστοιχο ποσοστό είναι 93.93%

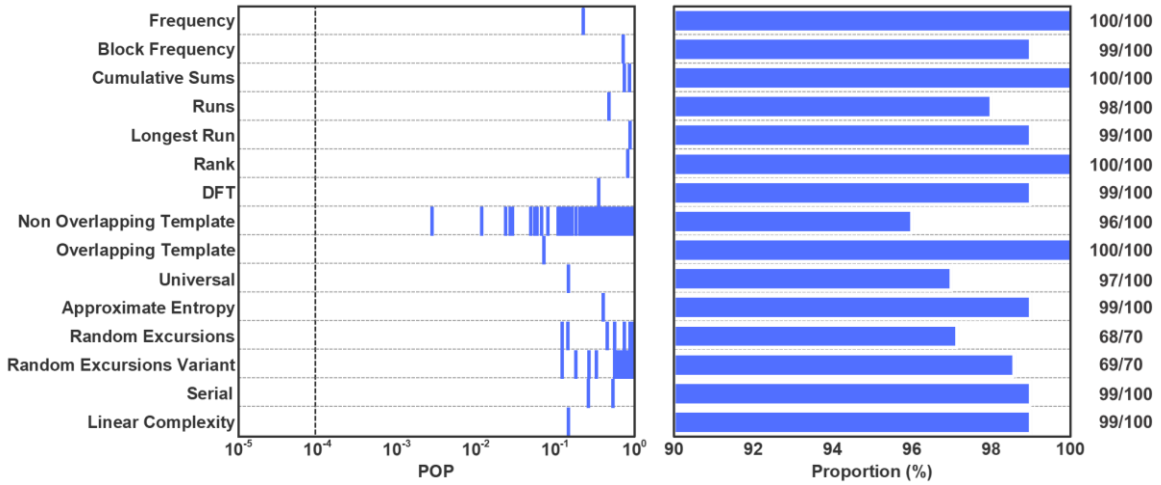


Σχήμα 6.13: Τα συνοπτικά αποτελέσματα που προέκυψαν από την εφαρμογή όλων των διαγνωστικών ελέγχων του πακέτου NIST, επί ενός αρχείου με μέγεθος 100Mbit, το οποίο παράχθηκε μέσω της τεχνικής RBM από το dataset D_7 (αποκρίσεις Unpredictability από διεγέρσεις με ανάλυση 128×128 micromirrors εκ των οποίων μόνο το 1/4 του συνολικού τους πλήθους συνεισφέρει την τελική ακτινοβόληση του diffuser). Το όριο ανοχής για τις τιμές POP είναι ίσο με 10^{-4}, ενώ το κατώτατο ποσοστό επιτυχημένων ακολουθιών για όλα τα τεστ, πλην των Random Excursions (Variant) είναι 96%. Για τους ελέγχους Random Excursions και Random Excursions Variant το αντίστοιχο ποσοστό είναι 93.85%

Στο σημείο αυτό θα πρέπει να υπογραμμιστεί ότι τα εν λόγω αποτελέσματα αντιστοιχούν σε ακολουθίες, οι οποίες έχουν παραχθεί διατηρώντας τον πίνακα B της τεχνικής RBM σταθερό, αλλά μεταβάλλοντας τον ψευδοτυχαίο πίνακα αυτής S. Στην περίπτωση όμως όπου και οι δύο αυτοί πίνακες διατηρηθούν αμετάβλητοι καθόλη την διάρκεια εξαγωγής των δυαδικών ακολουθιών, τα αρχεία που εν τέλει παράγονται επιτυγχάνουν συστηματικά σε όλους τους διαθέσιμους ελέγχους του πακέτου NIST πλην αυτού του DFT.



Σχήμα 6.14: Τα συνοπτικά αποτελέσματα που προέκυψαν από την εφαρμογή όλων των διαγνωστικών ελέγχων του πακέτου NIST, επί ενός αρχείου με μέγεθος 100Mbit, το οποίο παράχθηκε μέσω της τεχνικής RBM από το dataset D_9 (αποκρίσεις Unpredictability από διεγέρσεις με ανάλυση 128×128 micromirrors εκ των οποίων μόνο το 1/8 του συνολικού τους πλήθους συνεισφέρει την τελική ακτινοβόληση του diffuser). Το όριο ανοχής για τις τιμές POP είναι ίσο με 10^{-4}, ενώ το κατώτατο ποσοστό επιτυχημένων ακολουθιών για όλα τα τεστ, πλην των Random Excursions (Variant) είναι 96%. Για τους ελέγχους Random Excursions και Random Excursions Variant το αντίστοιχο ποσοστό είναι 95%



Σχήμα 6.15: Τα συνοπτικά αποτελέσματα που προέκυψαν από την εφαρμογή όλων των διαγνωστικών ελέγχων του πακέτου NIST, επί ενός αρχείου με μέγεθος 100Mbit, το οποίο παράχθηκε μέσω της τεχνικής RBM από το dataset D_{11} (αποκρίσεις Unpredictability από διεγέρσεις με ανάλυση 128×128 micromirrors εκ των οποίων μόνο το 1/16 του συνολικού τους πλήθους συνεισφέρει την τελική ακτινοβόληση του diffuser). Το όριο ανοχής για τις τιμές POP είναι ίσο με 10^{-4}, ενώ το κατώτατο ποσοστό επιτυχημένων ακολουθιών για όλα τα τεστ, πλην των Random Excursions (Variant) είναι 96%. Για τους ελέγχους Random Excursions και Random Excursions Variant το αντίστοιχο ποσοστό είναι 94.29%

6.5 Συμπεράσματα

Στο πλαίσιο του παρόντος κεφαλαίου μελετήθηκε η επίδοση μιας τρίτης και τελευταίας υλοποίησης ενός οπτικού συστήματος PUF, ως προς τις ιδιότητες του Robustness, του Unpredictability και του Unclonability του. Η εν λόγω μελέτη πραγματοποιήθηκε με κύριο σκοπό την αύξηση της αξιοπιστίας των παραγόμενων δυαδικών ακολουθιών, όπως αυτές εξάγονται μέσω της μεθόδου RBM, και την ενίσχυση της ανομοιότητας μεταξύ τους. Η συγκεκριμένη μελέτη έλαβε χώρα ως ακολούθως: ένα σύνολο από ανά 2 ασυσχέτιστα δυαδικά μοτίβα (challenges), με ισοπληθή μοναδιαία και μηδενικά pixels, προβάλλεται μέσω μιας συσκευής DMD στην επιφάνεια ενός γυάλινου σκεδαστικού μέσου (diffuser). Τα μοναδιαία ψηφία

των μοτίβων αυτών μεταβάλλουν τα σημεία πρόσπτωσης του φωτός επί του χρησιμοποιούμενου μέσου, οδηγώντας στην παραγωγή μοναδικών speckle patterns (responses), τα οποία καταγράφονται από μια κάμερα CMOS με ενσωματωμένο σύστημα ψύξης. Τα κύρια ευρήματα της εν λόγω μελέτης συνοψίζονται ως εξής:

- Η χρήση κάμερας με ενσωματωμένο σύστημα ψύξης επιτυγχάνει την αισθητή καταστολή του θορύβου dark current, εξασφαλίζοντας την επαναληψιμότητα των καταγραφόμενων αποκρίσεων για τουλάχιστον έναν μήνα.
- Η χρήση της αναφερθείσας κάμερας σε συνδυασμό με την εφαρμογή διεγέρσεων ανάλυσης 64x64 μικροκατόπτρων, επιτυγχάνει επιπροσθέτως και τον επιθυμητό διαχωρισμό των ιστογραμμάτων Robustness - Unpredictability και Robustness - Unclonability, τόσο στο επίπεδο των παραγόμενων εικόνων όσο και στο επίπεδο των δυαδικών τους ακολουθιών. Επομένως, το ενδεχόμενο του να προκύψουν ψευδώς θετικές ή ψευδώς αρνητικές αυθεντικοποιήσεις ελαχιστοποιείται.
- Η περαιτέρω αύξηση της ανάλυσης των εφαρμοζόμενων διεγέρσεων, από 64×64 σε 128x128 micromirrors, οδηγεί σε μια μικρή βελτίωση του Unpredictability, η οποία χαρακτηρίζεται ως καθόλα επαρκής, καθώς οι αντίστοιχες δυαδικές τους ακολουθίες θεωρούνται αρκούντως τυχαίες σύμφωνα με τα αποτελέσματα του λογισμικού πακέτου NIST. Η βελτίωση αυτή μάλιστα έρχεται σε πλήρη συμφωνία με τα συμπεράσματα του Iskandar Atakhodjaev [76], ο οποίος στο πλαίσιο της διδακτορικής του διατριβής απέδειξε ότι όσο η ανάλυση των εφαρμοζόμενων διεγέρσεων αυξάνει, τόσο η επιτυχής πρόβλεψη μελλοντικών αποκρίσεων, μέσω ενός κατάλληλα εκπαιδευμένου βαθύ νευρωνικού δικτύου (Deep Neural Network - DNN), δυσχεραίνει[10].
- Η μείωση των «ενεργών» micromirrors που συνεισφέρουν στην ακτινοβόληση του χρησιμοποιούμενου ανομοιογενούς υλικού, άρα και η μείωση των κοινών σημείων πρόσπτωσης του φωτός επί αυτού, οδηγεί στην σταδιακή υποβάθμιση του Robustness, επιτυγχάνοντας ταυτοχρόνως την βαθμιαία αλλά σημαντική ενίσχυση του Unpredictability. Η εν λόγω ενίσχυση μάλιστα βρίσκεται σε καλή συμφωνία με τα συμπεράσματα της μελέτης [77], η οποία όμως δεν παρουσιάζει καθόλου αποτελέσματα όσον αφορά την αντίστοιχη επαναληψιμότητα του συστήματος, καθώς τα χρησιμοποιούμενα δεδομένα προέρχονται από ένα αριθμητικό μοντέλο στο οποίο δεν έχει ληφθεί καθόλου υπόψιν η επίδραση του μετρητικού θορύβου.

[10] Συγκεκριμένα, στο πλαίσιο της διδακτορικής του διατριβής ο Iskandar Atakhodjaev κατασκεύασε τέσσερα διαφορετικά σύνολα 100000 δυαδικών διεγέρσεων, με ανάλυση 8×8, 16×16, 32×32 και 64×64 pixels, και εν συνεχεία παρήγαγε τέσσερα αντίστοιχα σύνολα από υπολογιστικά speckle patterns, επιστρατεύοντας ένα αριθμητικό μοντέλο που βασίζεται στον μετασχηματισμό Fourier μίας μάσκας από ψευδο-τυχαίες φάσεις. Εν συνεχεία, με ένα τμήμα από τα ζεύγη των παραγόμενων δεδομένων εκπαίδευσε τέσσερα διαφορετικά μοντέλα DNN, μέσω των οποίων αποπειράθηκε να προβλέψει τις αποκρίσεις των διεγέρσεων που δεν χρησιμοποιήθηκαν κατά το προαναφερθέν στάδιο της εκπαίδευσης.

7. ΣΥΓΚΕΝΤΡΩΤΙΚΑ ΣΥΜΠΕΡΑΣΜΑΤΑ

Στο πλαίσιο της παρούσας διδακτορικής εργασίας έγινε θεωρητική και πειραματική μελέτη πάνω σε τρεις κατευθύνσεις. Αρχικά, η πρώτη υλοποίηση επικεντρώθηκε στη διερεύνηση της μεταβολής του μήκους κύματος ως μέθοδος για την παραγωγή διεγέρσεων σε ένα οπτικό PUF. Εν συνεχεία πραγματοποιήθηκε μια υλοποίηση οπτικού PUF με την παρεμβολή απεικονιστικής διάταξης τύπου LCD ως τρόπος μεταβολής της ακτινοβολίας στο οπτικό μέσο. Τέλος, και χρησιμοποιώντας τη συσσωρευμένη εμπειρία από τις δύο πρώτες υλοποιήσεις, κατασκευάστηκε μια νέα πειραματική διάταξη, στην οποία η ακτινοβολία διαχειρίστηκε μέσω μιας συσκευής τύπου DMD, ενώ το οπτικό μέσο επιλέχθηκε να είναι ένας γυάλινος diffuser.

Συνοπτικά, από την πρώτη μελέτη έγινε σαφές πως όταν το μήκος κύματος της δέσμης ακτινοβολίας είναι η μεταβαλλόμενη ποσότητα, η χρήση πολυμερικής οπτικής ίνας (POF) είναι ενδεδειγμένη και παρουσιάζει σαφώς ανώτερη συμπεριφορά. Παρ' όλα αυτά, ένα τέτοιο σύστημα μπορεί να χρησιμοποιηθεί με ασφάλεια μόνο ως σύστημα αυθεντικοποίησης μοναδιαίας απόκρισης, καθώς η λειτουργία του ως γεννήτρια τυχαίων αριθμών είναι επισφαλής, αφού το πλήθος των δυνατών διεγέρσεων είναι μικρό και πεπερασμένο.

Εν συνεχεία, στη διάρκεια της δεύτερης μελέτης έγιναν σαφή τα όρια της διάταξης, ενώ διερευνήθηκε η μεταβολή των σημείων πρόσπτωσης ως μέθοδος παραγωγής διεγέρσεων. Σε αυτή τη διάταξη έγινε επιπλέον διερεύνηση διάφορων υπολογιστικών μεθόδων για τη βελτίωση των αποτελεσμάτων. Παράλληλα, η μη πρακτικότητα της χρήσης οπτικής ίνας σε αυτή τη μέθοδο έγινε σαφής, όπως και η επίδραση της συσκευής LCD ως μέσο διαχείρισης της ακτινοβολίας.

Εν τέλει, η τρίτη και τελευταία υλοποίηση χρησιμοποίησε την εμπειρία των προηγούμενων δύο για τη σχεδίαση και κατασκευή μιας διάταξης στην οποία έχουν αντιμετωπιστεί, kata το δυνατόν, τα προαναφερθέντα προβλήματα. Η συσκευή LCD αντικαταστάθηκε με μια συσκευή «ψηφιακής επεξεργασίας φωτός», όπως ονομάζεται η εν λόγω συσκευή DMD, με την οποία εξαλείφθηκε ο θόρυβος, η διάχυση, και άλλα ανεπιθύμητα φαινόμενα των οποίων αιτία ήταν η διέλευση της δέσμης από τα πολλά επίπεδα της LCD. Παράλληλα, επιλέχθηκε νέος αισθητήρας, με σύστημα ψύξης αλλά και χωρίς φίλτρο Bayer, για τον μεγαλύτερο έλεγχο της λειτουργίας. Το αποτέλεσμα ήταν η σημαντική αύξηση του αριθμού των πιθανών διεγέρσεων, η μείωση του θορύβου, αλλά και η ενίσχυση της απόδοσης και των χαρακτηριστικών ασφαλείας του συστήματος.

Συνολικά, τα συστήματα PUF αποτελούν την πλέον δημοφιλή κατεύθυνση στον τομέα της ασφάλειας. Παράλληλα, η αναμενόμενη στροφή προς την κατεύθυνση των silicon photonics κάνει την έρευνα στον τομέα των οπτικών PUFs ιδιαιτέρως χρήσιμη, καθώς πιθανή ενσωμάτωσή τους στο επίπεδο του wafer θα αποτελούσε το απόλυτο σε χρησιμότητα, εκτοξεύοντας την ασφάλεια όλων ανεξαιρέτως των συστημάτων κρυπτογράφησης και αυθεντικοποίησης. Αλλά και στο επίπεδο υλοποίησης της παρούσης διατριβής, τα οπτικά PUFs παραμένουν συστήματα εξαιρετικού ενδιαφέροντος, με πάμπολλες δυνατότητες χρήσης σε συστήματα αυθεντικοποίησης, ψηφιακών υπογραφών, γεωεντοπισμού, ακόμη και ασφαλείας στον χώρο του Internet of Things.

8. ΜΕΛΛΟΝΤΙΚΗ ΜΕΛΕΤΗ

Η περαιτέρω μελέτη και εξέλιξη των οπτικών PUFs μπορεί να διεξαχθεί, χρησιμοποιώντας την εμπειρία της παρούσης διατριβής ως εφαλτήριο για τη βελτίωση των σχετικών μεθόδων και των διατάξεων.

Χρησιμοποιώντας τις τελευταίες εξελίξεις της έρευνας – όπως τη χρήση quantum dots ή single photon emitters – αλλά και ώριμων τεχνολογιών, όπως voice coil actuators, για τον μεγαλύτερο έλεγχο της θέσης και της γεωμετρίας της προσπίπτουσας ακτινοβολίας ή και την σταθεροποίηση του αισθητήρα, είναι δυνατή η σχεδίαση και η κατασκευή ακόμη καλύτερων συστημάτων PUF, με μικρότερο μέγεθος, μεγαλύτερη ανοχή σε περιβαλλοντικές συνθήκες, αλλά και ακόμη καλύτερη απόδοση.

Ειδικότερα, για την ακριβέστερη θεωρητική μελέτη των οπτικών PUFs χρειάζεται να ληφθούν υπόψιν οι ατέλειες των φακών στο υπάρχον υπολογιστικό μοντέλο και να μοντελοποιηθούν οι πηγές του πειραματικού θορύβου, οι οποίες όπως αναφέρθηκε και στο κεφάλαιο 2 επηρεάζουν την επίδοση μιας οπτικής PUF ως προς την ιδιότητα του robustness της. Όσον αφορά την πειραματική μελέτη αξίζει να πραγματοποιηθεί η περαιτέρω πειραματική διερεύνηση του θορύβου παρατήρησης (πχ πως επηρεάζεται το robustness από την θερμοκρασία του περιβάλλοντος χώρου και την υγρασία).

Από την άλλη πλευρά, για τα υπάρχοντα πειραματικά δεδομένα και αποτελέσματα, όπως αυτά προέκυψαν από την διάταξη με την συσκευή DMD: επιβάλλεται η περαιτέρω πειραματική διερεύνηση του θορύβου παρατήρησης (πχ πως επηρεάζεται το robustness από την θερμοκρασία του περιβάλλοντος χώρου και την υγρασία). Επιπροσθέτως μπορεί να πραγματοποιηθεί ο αυστηρότερος έλεγχος των παραγόμενων δυαδικών ακολουθιών μέσω των πακέτων DIEHARD και DIEHARDER, ενώ με χρήση conditional generative adversarial networks (cGAN) μπορεί να αποπειραθεί η πρόβλεψη των παραγόμενων speckle pattern (machine learning attack στις πειραματικές αποκρίσεις).

Τέλος,: να εντοπιστούν εναλλακτικές τεχνικές εξαγωγής δυαδικών ακολουθιών από τα παραγόμενα speckle patterns, οι οποίες χαρακτηρίζονται από μικρότερο υπολογιστικό κόστος και καλύτερη συνολική απόδοση. Να διερευνηθεί η χρήση deep hashing και ενδεχομένως να αντικατασταθεί η κρυπτογραφική συνάρτηση SHA-256 που εφαρμόζεται στο πλαίσιο του fuzzy extractor με μία πιο σύγχρονη και ασφαλέστερη συνάρτηση.

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Physical Unclonable Function	Μη κλωνοποιήσιμη Φυσική Συνάρτηση
Challenge	Διέγερση
Response	Απόκριση
Robustness	Ευρωστία
Unpredictability	Μη προβλεψιμότητα
Unclonability	Μη κλωνοποιησιμότητα
Liquid Crystal Display	Οθόνη Υγρών Κρυστάλλων
Digital Micromirror Device	Συσκευή Ψηφιακών Μικροκατόπτρων
Polymer Optical Fiber	Πολυμερική Οπτική Ίνα
Diffuser	Πλακίδιο Διάχυσης Φωτός
Fuzzy Extractor	Ασαφής Εξαγωγέας
Secure Sketch	Ασφαλές Σχήμα
Error Correction Code	Κώδικας Διόρθωσης Λαθών
Hash Function	Συνάρτηση Κατακερματισμού
Randomness Extractor	Εξαγωγέας Τυχαιότητας
Enrolment	Εγγραφή
Authentication	Αυθεντικοποίηση
Signal To Noise Ratio	Λόγος Σήματος Προς Θόρυβο
Contrast	Φωτοαντίθεση
Message	Μήνυμα
Code Word	Κωδική Λέξη
Error Correction Capability	Διορθωτική Ικανότητα
Power Spectral Density	Φασματική Πυκνότητα Ισχύος
Autocorrelation Function	Συνάρτηση Αυτοσυσχετίσεως
Probability Density Function	Συνάρτηση Πυκνότητας Πιθανότητας
Nearest Neighbor Interpolation	Παρεμβολή Εγγύτερου Γείτονα
Frequency	Συχνότητα
Octave	Οκτάβα
Lacunarity	Κενότητα
Persistence	Ανθεκτικότητα
Core	Πυρήνας
Cladding	Μανδύας
Total Internal Reflection	Ολική Εσωτερική Ανάκλαση
Numerical Aperture	Αριθμητικό Άνοιγμα
Mode	Ρυθμός Διάδοσης
Meridional Ray	Μεσημβρινή Ακτίνα
Skewed Ray	Στρεβλή Ακτίνα
Affine Transformation	Ομοπαράλληλος Μετασχηματισμός
Sum Of Square Differences	Άθροισμα Τετραγωνικών Διαφορών
Histogram Equalization	Ισοστάθμιση Ιστογράμματος
Compressive Sensing	Συμπιεστική Δειγματοληψία
Sparsity	Αραιότητα
Incoherence	Ασυμφωνία
Discrete Fourier Transformation	Διακριτός Μετασχηματισμός Fourier
Cumulative Distribution Function	Αθροιστική Συνάρτηση Κατανομής
Helper Data	Βοηθητικά Δεδομένα
Cross-Correlation Coefficient	Συντελεστής Διασυσχέτισης

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
PUF	Physical Unclonable Function
LCD	Liquid Crystal Display
SNR	Signal To Noise Ratio
ACF	Autocorrelation Function
PSD	Power Spectral Density
PDF	Probability Density Function
CDF	Cumulative Distribution Function
DMD	Digital Micromirror Device
POF	Polymer Optical Fiber
ECC	Error Correction Code
BCH	Bose Chaudhuri Hocquenghem
DFT	Discrete Fourier Transformation
RBM	Random Binary Method
GBM	Gabor Binary Method
SVD	Singular Value Decomposition
NMF	Negative Matrix Factorization

ΠΑΡΑΡΤΗΜΑ Ι

Ι.1 Συμπιεστική Δειγματοληψία

Ι.1.1 Θεώρημα Nyquist

Από το 1928, όπου ο εργαζόμενος στα εργαστήρια της Bell Harold Nyquist έθεσε τις αρχές για την δειγματοληψία ενός συνεχούς σήματος με πεπερασμένο εύρος ζώνης διατυπώνοντας το ομώνυμο θεώρημα του, το κριτήριο Nyquist συνεχίζει να αποτελεί μέχρι σήμερα τον κύριο πυλώνα των περισσοτέρων μεθόδων καταγραφής, επεξεργασίας και ανάκτησης σημάτων.

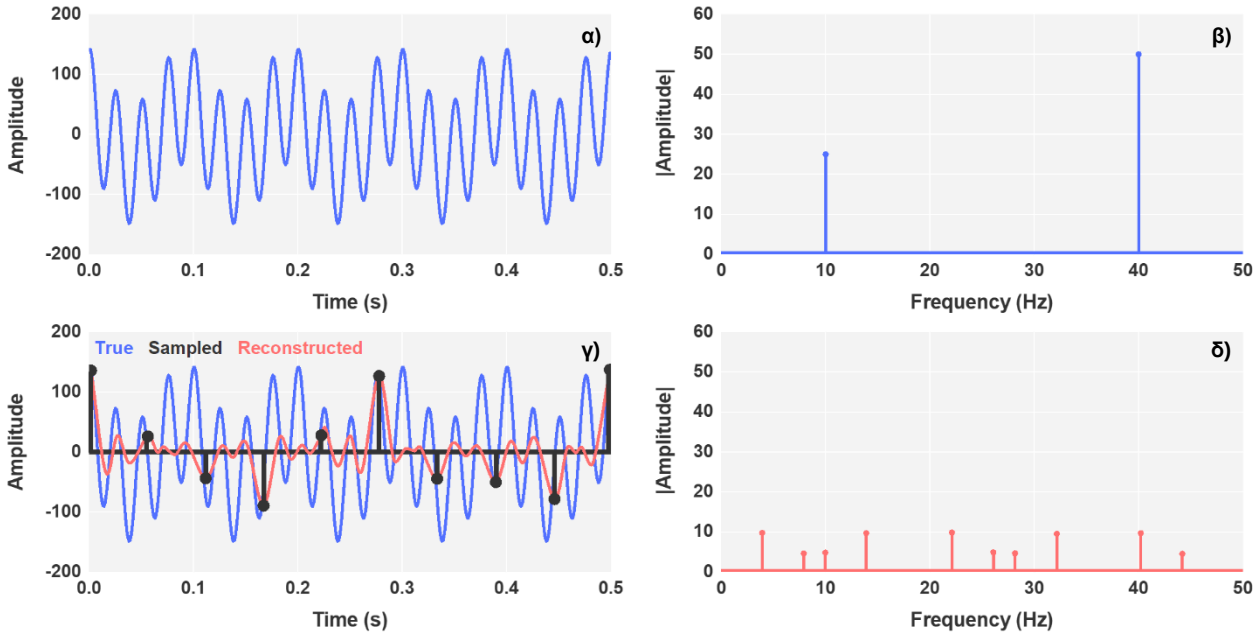
Σύμφωνα με το θεώρημα του Nyquist, η συχνότητα f_s με την οποία διενεργείται η ομοιόμορφη δειγματοληψία ενός οποιουδήποτε αναλογικού σήματος θα πρέπει να είναι τουλάχιστον διπλάσια της μέγιστης συχνότητα f_m που εμπεριέχεται στο φάσμα αυτού, ώστε να αποτραπεί η απώλεια πληροφορίας και να είναι εφικτή η πλήρης και ορθή ανακατασκευή του.

$$f_s \geq 2f_m \tag{Ι.1}$$

Στην αντίθετη περίπτωση, όπου ο ρυθμός δειγματοληψίας δεν πληροί το παραπάνω κριτήριο, οι συνιστώσες υψηλών συχνοτήτων του αρχικού σήματος δεν καταγράφονται και ένας ικανός όγκος πληροφορίας χάνεται. Αυτό έχει ως αποτέλεσμα να εμφανίζεται αναδίπλωση του συχνοτικού περιεχομένου (aliasing) κατά την ανακατασκευή του σήματος, η οποία εν τέλει οδηγεί στην αλλοίωση του. Στο Σχήμα Ι.1 παρουσιάζεται η προσπάθεια ανάκτησης του σήματος:

$$X(t) = 50\sin(2\pi f_1 + \varphi_1) + 100\sin(2\pi f_2 + \varphi_2) \tag{Ι.2}$$

με f_1 = 10 Hz, f_2 = 40 Hz, $\phi_1 = \pi/5$, $\phi_2 = \pi/9$ και ρυθμό δειγματοληψίας 5 φορές μικρότερο από αυτόν που επιτάσσει το θεώρημα του Nyquist [78].



Σχήμα Ι.1: α) Το αρχικό σήμα στο πεδίο του χρόνου με **β)** το αντίστοιχο φάσμα συχνοτήτων του. **γ)** Ανακατασκευή του σήματος με ρυθμό δειγματοληψίας 5 φορές μικρότερο από αυτόν του κριτηρίου Nyquist δ) Εμφάνιση πλασματικών συνιστωσών στο φάσμα του ανακατασκευασμένου σήματος (aliasing) [78]

Αναμφισβήτητα, η συνεισφορά του θεωρήματος Nyquist στην μετάβαση από την αναλογική στη ψηφιακή εποχή υπήρξε καθοριστική, οδηγώντας στην υλοποίηση ψηφιακών συστημάτων που υπερτερούν έναντι των αναλογικών τους ισοδυνάμων τόσο

από πλευράς αξιοπιστίας όσο και από πλευράς ευελιξίας ή κόστους. Εντούτοις σε πολλές αναδυόμενες εφαρμογές, η συχνότητα Nyquist είναι τόσο υψηλή που η κατασκευή των αναγκαίων συσκευών για την λήψη των δεδομένων καθίσταται πρακτικά αδύνατη. Έτσι, παρά την συνεχή αύξηση της υπολογιστικής δύναμης, η διαχείριση σημάτων σε μια πληθώρα πεδίων συνεχίζει να αποτελεί πρόκληση [79].

Μία από τις πιο πρόσφατες τεχνικές που αναπτύχθηκαν για την επίλυση αυτών των προβλημάτων είναι η προσέγγιση της συμπιεστικής δειγματοληψίας. Η συμπιεστική δειγματοληψία, εκμεταλλευόμενη τις ιδιότητες της αραιότητας (sparsity) των σημάτων και της ασυμφωνίας (incoherency) μεταξύ των βάσεων αναπαράστασης αυτών, επιτυγχάνει την ανακατασκευή τους με αριθμό μετρήσεων αρκετά μικρότερο από αυτόν που απαιτεί το θεώρημα του Nyquist [59].

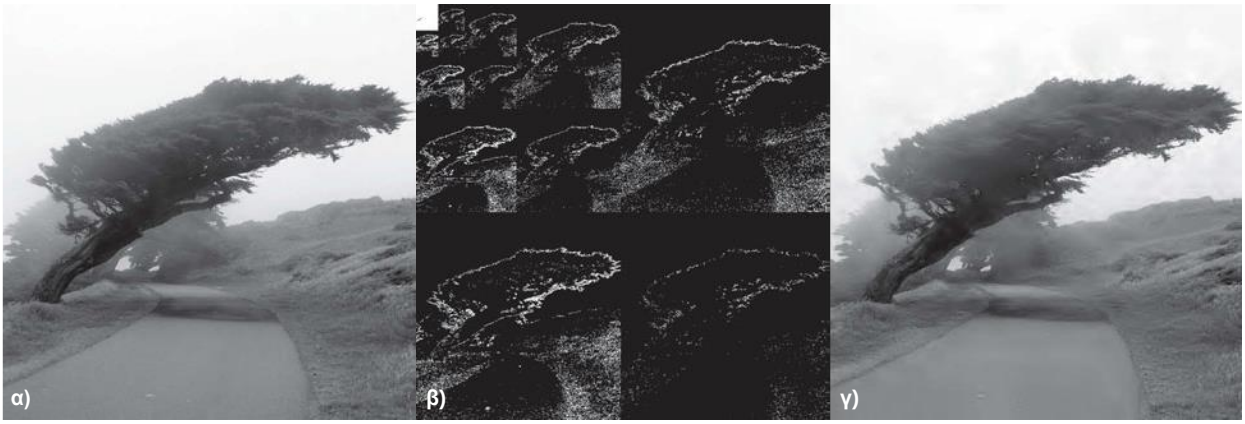
I.1.2 Αραιότητα

Η αραιότητα εκφράζει την ιδέα ότι ο ρυθμός πληροφορίας ενός συνεχούς σήματος είναι πολύ μικρότερος από αυτόν που υποδηλώνει το εύρος ζώνης του ή ότι ένα διακριτό σήμα εξαρτάται από αρκετά λιγότερους βαθμούς ελευθερίας σε σχέση με το πλήθος των στοιχείων αυτού [59].

Υπό μαθηματική σκοπιά, ένα σήμα ονομάζεται K-αραιό (K-sparse) όταν αυτό περιέχει το πολύ K μη μηδενικά στοιχεία. Συνήθως όμως, τα σήματα στα οποία αναφερόμαστε δεν είναι sparse εκ φύσεως αλλά έχουν αραιή αναπαράσταση σε μία κατάλληλα επιλεγμένη βάση Ψ. Έστω λοιπόν ένα διακριτό και μονοδιάστατο σήμα $X \in \mathbb{R}^N$, όπως μια φωτογραφία με N pixels εκφρασμένη ως διάνυσμα (στήλη). Το σήμα αυτό μπορεί να αναπαρασταθεί ως προς μία ορθοκανονική βάση $\Psi \in \mathbb{R}^{NxN}$ σαν γραμμικός συνδυασμός των διανυσμάτων ψ_i αυτής:

$$X = \Psi S \text{ ή } X = \sum_{i=1}^{N} s_i \psi_i \qquad (I.3)$$

όπου $S \in \mathbb{R}^N$ είναι το διάνυσμα των συντελεστών στάθμισης με $s_i = \langle x, \psi_i \rangle$. Εάν το πλήθος K των μη μηδενικών στοιχείων s_i ικανοποιεί την συνθήκη $K << N$ τότε το σήμα θεωρείται K-αραιό. Εάν από την άλλη πλευρά, η πλειοψηφία των συντελεστών s_i έχει τόσο μικρή τιμή ώστε οι περισσότεροι να μπορούν να θεωρηθούν αμελητέοι, τότε το σήμα ονομάζεται συμπιέσιμο (compressible).



Σχήμα I.2: α) Αρχική εικόνα **β)** Αποτέλεσμα μετασχηματισμού κυματιδίων **γ)** Ανακατασκευή της εικόνας από το 10% των συντελεστών με την μεγαλύτερη τιμή [80].

Στο σχήμα I.2 παρατίθεται ένα τυπικό παράδειγμα χρήσης της αραιότητας στο πεδίο της επεξεργασίας εικόνας: μια φωτογραφία, η οποία χαρακτηρίζεται από εκτεταμένες ομοιόμορφες περιοχές και σχετικά λίγες ακμές, εκφράζεται με έναν μετασχηματισμό κυματιδίων (wavelets). Ο μετασχηματισμός αυτός διαχωρίζει με περιοδικό τρόπο τις

συνιστώσες χαμηλών συχνοτήτων από αυτές των υψηλών, οδηγώντας σε ένα σύνολο συντελεστών που η πλειοψηφία τους έχει πολύ μικρή τιμή. Εάν οι συντελεστές που δεν υπερβαίνουν ένα συγκεκριμένο κατώφλι μηδενιστούν, προκύπτει μια αραιή αλλά ικανοποιητική αναπαράσταση της φωτογραφίας, η διαφορά της οποίας από την αρχική είναι ελάχιστα αισθητή [80].

Εν γένει, η ιδιότητα της αραιότητας αποτελεί την βασική ιδέα πολλών συμβατικών αλγορίθμων συμπίεσης, όπως είναι οι JPEG, MPEG και MP3, οι οποίοι όμως για να λειτουργήσουν απαιτούν την a priori γνώση ολόκληρου του σήματος ώστε στην συνέχεια να απορρίψουν το μεγαλύτερο μέρος της διαθέσιμης πληροφορίας. Αντίθετα, στην προσέγγιση της συμπιεστικής δειγματοληψίας με την χρήση μιας επιπλέον ιδιότητας, αυτή της ασυμφωνίας, γίνεται εφικτό τα βήματα της λήψης και της συμπίεσης των δεδομένων να λάβουν χώρα ταυτοχρόνως δαπανώντας έτσι ακόμα λιγότερους υπολογιστικούς πόρους [79].

I.1.3 Ασυμφωνία

Όπως ήδη αναφέρθηκε στην προηγούμενη ενότητα, η χρήση της αραιότητας στα πλαίσια μιας τυπικής διαδικασίας συμπίεσης προϋποθέτει την λήψη ολόκληρου του σήματος X και τον υπολογισμό του συνόλου των συντελεστών στο πεδίο Ψ, ώστε τελικά να γίνει εφικτή η επιλογή των στοιχείων που απαρτίζουν την αραιή αναπαράστασή του.

Απεναντίας στη συμπιεστική δειγματοληψία, οι μηχανισμοί καταγραφής και συμπίεσης λαμβάνουν χώρα ταυτοχρόνως μειώνοντας έτσι τόσο την υπολογιστική πολυπλοκότητα της συγκεκριμένης προσέγγισης όσο και τις απαιτήσεις αποθήκευσης που αυτή έχει. Αυτό επιτυγχάνεται λαμβάνοντας απευθείας ένα σύνολο μετρήσεων $Y \in \mathbb{R}^M$ από το σήμα $X \in \mathbb{R}^N$, εφαρμόζοντας τον ακόλουθο γραμμικό μετασχηματισμό:

$$Y = \Phi X = \Phi(\Psi S) \tag{I.4}$$

όπου $\Phi \in \mathbb{R}^{MxN}$ είναι ένας πίνακας, M × N διαστάσεων με K < M << N, επιλεγμένος έτσι ώστε να είναι ασύμφωνος με τη βάση Ψ. Ο βαθμός συμφωνίας των δύο πινάκων υπολογίζεται από την σχέση:

$$\mu(\Phi,\Psi) = \sqrt{N} \cdot \max\left|\left\langle \varphi_i, \psi_j \right\rangle\right| \tag{I.5}$$

όπου $1 \le i \le M$, $1 \le j \le N$ και $\mu(\Phi,\Psi) \in [1,\sqrt{N}]$ το πεδίο τιμών της, με τη μοναδιαία τιμή να υποδηλώνει τη πλήρη ασυμφωνία των πινάκων και τη χαμηλή συσχέτιση των μεταξύ τους στοιχείων. Επομένως, πρωταρχικός σκοπός της συμπιεστικής δειγματοληψίας είναι η εύρεση μιας κατάλληλης υπέρθεσης Θ = ΦΨ, τα διανύσματα της οποίας θα είναι όσο το δυνατόν περισσότερο ασύμφωνα ώστε να μεγιστοποιείται η πληροφορία που διατηρείται από τις συνιστώσες του σήματος με τον μικρότερο δυνατό αριθμό γραμμικών συνδυασμών M. Μερικά ενδεικτικά παραδείγματα από ζεύγη συναρτήσεων που χρησιμοποιούνται για την κατασκευή τέτοιων υπερθέσεων παρατίθενται στον πίνακα I.1 μαζί με τις αντίστοιχες τιμές συμφωνίας τους [59].

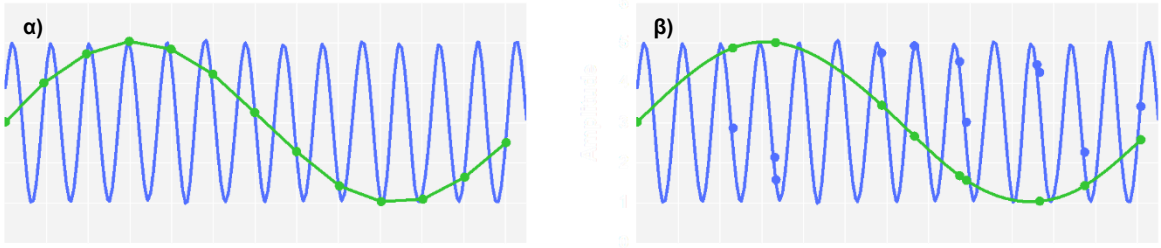
Πίνακας I.1: Ενδεικτικά ζεύγη συναρτήσεων που χρησιμοποιούνται για την κατασκευή των πινάκων Φ και Ψ, συνοδευόμενα από τις αντίστοιχες τιμές της μεταξύ τους συμφωνίας [59].

φ_i	ψ_j	$\mu(\Phi,\Psi)$
Συνάρτηση Dirac	Συνάρτηση Fourier	1
Noiselet	Haar Wavelet	√2
Noiselet	Daubechies D4 Wavelet	2.2
Noiselet	Daubechies D8 Wavelet	2.9
Noiselet	Συνάρτηση Dirac	1

Στο σημείο αυτό θα πρέπει να επισημανθεί ότι οι πιο ευρέως χρησιμοποιούμενοι Φ είναι πίνακες, τα στοιχεία των οποίων είναι στατιστικά ανεξάρτητοι και τυχαίοι αριθμοί, με τιμές

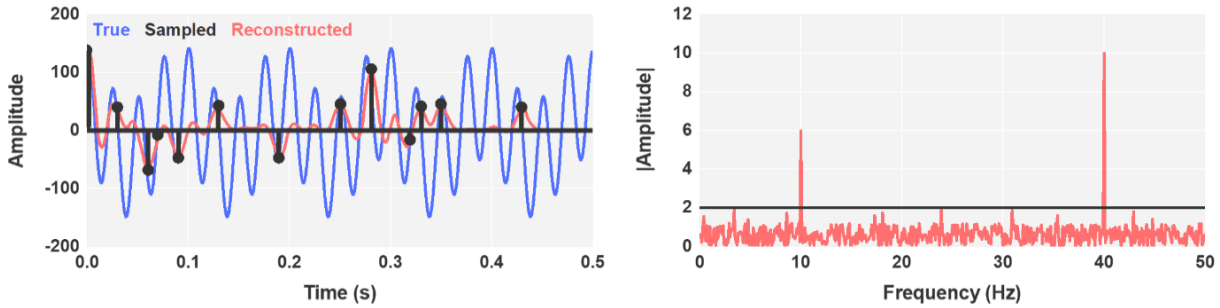
που ακολουθούν μια ομοιόμορφη (uniform), διωνυμική (Bernoulli) ή κανονική (Gaussian) κατανομή. Οι Φ αυτοί δεν έχουν συμπεριληφθεί στον παραπάνω πίνακα καθώς έχει αποδειχθεί ότι είναι επαρκώς ασύμφωνοι με την πλειοψηφία όλων των γνωστών βάσεων αραιής αναπαράστασης Ψ [59].

Εστιάζοντας λοιπόν στις υπερθέσεις Θ που συνίστανται από τυχαίους πίνακες Φ, στο σχήμα Ι.3 αντιπαραβάλλονται τα αποτελέσματα δειγματοληψίας για το ίδιο ημιτονοειδές σήμα, χρησιμοποιώντας μια σύμφωνη και μια ασύμφωνη μεθοδολογία μετρήσεων [78]. Όπως μπορεί να παρατηρηθεί, η σύμφωνη μετρητική διαδικασία που αντιστοιχεί σε έναν περιοδικό και ομοιόμορφο τρόπο δειγματοληψίας παράγει ένα σύνολο τιμών από το οποίο δεν είναι δυνατόν να εντοπισθεί η συχνότητα του αρχικού σήματος, όταν το κριτήριο του Nyquist παραβιάζεται, οδηγώντας στο προαναφερθέν φαινόμενο της αναδίπλωσης. Αντίθετα, χρησιμοποιώντας μια τυχαία, και επομένως απεριοδική και ανομοιόμορφη μεθοδολογία, ο ίδιος αριθμός μετρήσεων αντιπροσωπεύει καλύτερα τις γρήγορες αυξομειώσεις του σήματος και συγκρατεί με μεγαλύτερη αξιοπιστία τις τιμές που χρειάζονται για την σωστή ανακατασκευή του.



Σχήμα Ι.3: α) Αναδίπλωση σήματος με σύμφωνη (περιοδική) δειγματοληψία **β)** Απουσία αναδίπλωσης λόγω ασύμφωνης (τυχαίας) δειγματοληψίας [78]

Συνεπώς, για να επιτευχθεί η καταγραφή ενός σήματος με ρυθμό δειγματοληψίας χαμηλότερο από αυτόν που επιτάσσει το θεώρημα του Nyquist, ο χρησιμοποιούμενος πίνακας προβολών Φ (sensing matrix) θα πρέπει να είναι απεριοδικός στο πεδίο λήψης του σήματος αυτού. Εάν θεωρηθεί το σήμα της σχέσης (Ι.2) για το οποίο τα πεδία μέτρησης και αραιής αναπαράστασης ισοδυναμούν με τα πεδία χρόνου και συχνότητας αντιστοίχως, η έλλειψη περιοδικότητας του πίνακα Φ στο πρώτο συνεπάγεται ένα ευρύ φάσμα που καλύπτει όλο το δεύτερο. Με άλλα λόγια, τα διανύσματα του πίνακα Φ θα πρέπει να έχουν πολύ πυκνή αναπαράσταση στη βάση Ψ σε αντίθεση με το προς ανακατασκευή σήμα [59]. Το γεγονός αυτό φέρει ως αποτέλεσμα οι αναδιπλούμενες συχνότητες να εμφανίζονται ως λευκός θόρυβος στο πεδίο των συχνοτήτων, όπως φαίνεται και στο ακόλουθο σχήμα, ο οποίος μπορεί να αφαιρεθεί με ευκολία θέτοντας απλά μια τιμή κατωφλίου [78].



Σχήμα Ι.4: α) Ανακατασκευή του σήματος που δίνεται από την σχέση (Ι.2) με τυχαία και απεριοδική δειγματοληψία **β)** Εμφάνιση παραποιημένων συνιστωσών στο φάσμα του ανακατασκευασμένου σήματος ως λευκός θόρυβος [78].

Τελικά, η ιδιότητα της ασυμφωνίας μπορεί να θεωρηθεί ως μια εναλλακτική έκφραση της αρχής της αβεβαιότητας: όπως το φάσμα ενός σήματος με μηδενική έκταση στο χρόνο (συνάρτηση δέλτα) εμπεριέχει όλες τις συχνότητες, έτσι και ένα σήμα που έχει αραιή

αναπαράσταση σε μία βάση Ψ θα πρέπει να απλώνεται σε όλο το πεδίο μέτρησης του. Με άλλα λόγια, όπως διατυπώθηκε και στην προηγούμενη παράγραφο, τα διανύσματα του πίνακα Φ πρέπει να έχουν πολύ πυκνή αναπαράσταση στη βάση Ψ σε αντίθεση με το προς ανακατασκευή σήμα [59][81].

I.1.4 Συνθήκη Περιορισμένης Ισομετρίας

Συνοψίζοντας, οι ιδιότητες της αραιότητας και της ασυμφωνίας αποτελούν τις δύο θεμελιώδεις προυποθέσεις για να γίνει εφικτή η ταυτόχρονη καταγραφή και συμπίεση ενός σήματος με sub-Nyquist ρυθμούς, θέτοντας τα κριτήρια σχεδιασμού και κατασκευής του πίνακα συμπιεστικής δειγματοληψίας Θ. Για την αντίστροφη διαδικασία όμως, δηλαδή την διαδικασία της ανακατασκευής, ο πίνακας Θ, ως έχει, δεν εξασφαλίζει πάντα την ορθή και πλήρη ανάκτηση του αρχικού σήματος, καθιστώντας αναγκαία την εισαγωγή μιας επιπλέον συνθήκης, αυτή της περιορισμενης ισομετρίας (Restricted Isometry Property).

Αντικαθιστώντας την ισότητα Θ = ΦΨ στην σχέση (I.4), όπου S ∈ $\mathbb{R}^N$, Θ ∈ $\mathbb{R}^{MxN}$ και Y ∈ $\mathbb{R}^M$, ο μετασχηματισμός συμπιεστικής δειγματοληψίας γράφεται ακολούθως:

$$Y = (\Phi\Psi)S = \Theta S \tag{I.6}$$

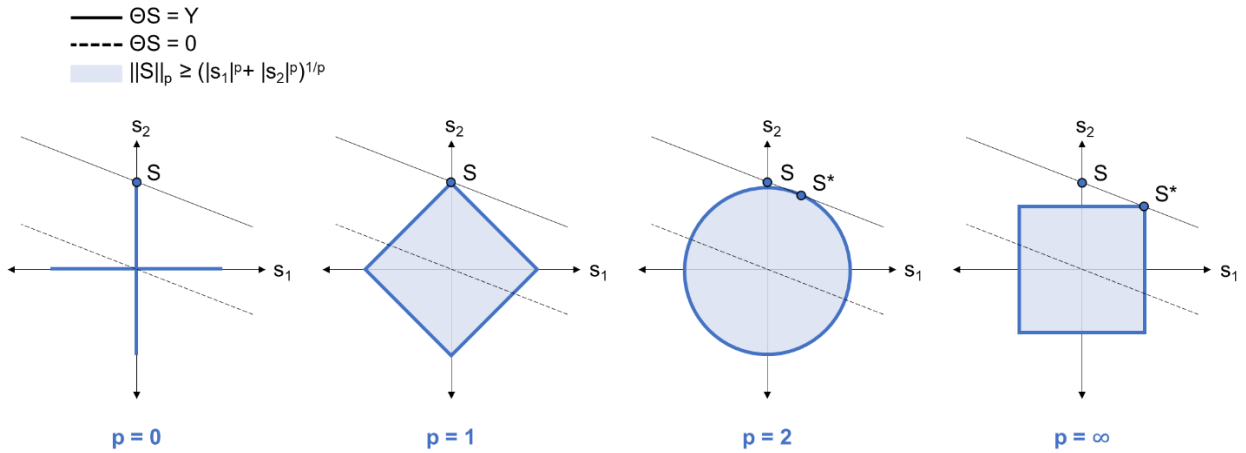
με το στάδιο της επιστροφής στην αραιή αναπαράσταση S να επαναδιατυπώνεται ως η επίλυση ενός αόριστου γραμμικού συστήματος από M εξισώσεις και N > M αγνώστους, για το οποίο υπάρχει ένας άπειρος αριθμός λύσεων. Ο περιορισμός του πλήθους αυτού συνήθως αντιμετωπίζεται αλγοριθμικά ως ένα πρόβλημα βελτιστοποίησης P_f:

$$P_f : \min_S \left[f(S) \right] \text{ με το C να ικανοποιεί την σχέση } Y = \Theta S \tag{I.7}$$

όπου f(S) είναι μια συνάρτηση κόστους που αποτιμά την καταλληλότητα της εκάστοτε λύσης και οδηγεί με την ελαχιστοποίηση της στον εντοπισμό της βέλτιστης εξ αυτών. Μία από τις πιο διαδεδομένες κατηγορίες συναρτήσεων κόστους αποτελεί η μετρική της ℓ_p νόρμας:

$$\|S\|_p = \left(\sum_{i=1}^{N} |s_i|^p \right)^{1/p} \tag{I.8}$$

με συνηθέστερες επιλογές της οποίας να είναι οι ℓ_0, ℓ_1 και ℓ_2 για p = 0, p = 1 και p = 2 αντιστοίχως. Από αυτές, όπως παρουσιάζεται και στο ακόλουθο σχήμα, καταλληλότερη για τις ανάγκες της συμπιεστικής δειγματοληψίας έχει αποδειχθεί η ℓ_1.



Σχήμα I.5: Γραφική επίλυση του P_f με χρήση των ℓ_0, ℓ_1, ℓ_2 και ℓ_∞ νορμών, όπου το S = [s_1,s_2] ∈ $\mathbb{R}^2$ είναι η αραιή αναπαράσταση του αρχικού σήματος και το S* η βέλτιστη ανακατασκευή της. Η συνεχής γραμμή συμβολίζει τις δυνατές λύσεις της εξίσωσης ΘS = Y, ενώ η διακεκομμένη αυτές της ΘS = 0 (μηδενοχώρος του πίνακα Θ). Η σκιαγραφημένη περιοχή αντιπροσωπεύει όλα τα διανύσματα, η νόρμα των οποίων είναι ίση ή μικρότερη με αυτήν του S.

Στο σχήμα Ι.5 παρατίθεται ένα παράδειγμα γραφικής επίλυσης του προβλήματος P_f με χρήση των ℓ_0, ℓ_1, ℓ_2 και ℓ_∞ νορμών για ένα αραιό σήμα S που έχει δύο μόνο στοιχεία. Ουσιαστικά αναζητούμε το σημείο τομής S*, το οποίο αντιστοιχεί στην ελάχιστη δυνατή τιμή νόρμας που ικανοποιεί την εξίσωση (Ι.6). Όπως φαίνεται από το σχήμα όμως, μόνο οι νόρμες με $p \leq 1$ προωθούν την εύρεση αραιών λύσεων, οι οποίες βρίσκονται επί των αξόνων του επιπέδου, και διατηρούν το σφάλμα ανακατασκευής $||S - S^*||_p$ στο ελάχιστο. Από αυτές, η ℓ_0 αντιστοιχεί σε πρόβλημα NP-hard κλάσης απαιτώντας την δοκιμή όλων των δυνατών διατάξεων από τα στοιχεία που θα μπορούσαν να αποτελούν το διάνυσμα του S*, ενώ αντίθετα, η ℓ_1 μπορεί να πραγματοποιηθεί πολύ εύκολα μέσω κλασσικών μεθόδων γραμμικού προγραμματισμού [59][82].

Υπό αυτό το πλαίσιο, η τελική μορφή του προβλήματος βελτιστοποίησης (Ι.7) με χρήση της ℓ_1 νόρμας για ένα K-sparse σήμα S δίνεται από την σχέση:

$$P_1 : \min_S \left[\|S\|_1 \right] \text{ με το S να ικανοποιεί την σχέση } Y = \Theta S \tag{I.9}$$

για την οποία, οι θεμελιωτές της συμπιεστικής δειγματοληψίας Candes και Tao εισήγαγαν μια καινούρια παράμετρο $\delta_K \in (0,1)$ που ονομάζεται σταθερά ισομετρίας [59]. Η σταθερά ισομετρίας, όπως έχει αποδειχθεί, αποτελεί ένα ισχυρό εργαλείο αξιολόγησης τόσο της καταλληλότητας των χρησιμοποιούμενων πινάκων Θ όσο και της επίδοσης των αλγορίθμων ανακατασκευής που εφαρμόζονται για την επίλυση του παραπάνω προβλήματος [82].

Συγκεκριμένα, όταν η τιμή της σταθεράς δ_K δεν είναι κοντά στην μονάδα, ο πίνακας συμπιεστικής δειγματοληψίας Θ ικανοποιεί την λεγόμενη συνθήκη της περιορισμένης ισομετρίας:

$$(1-\delta_K)\|S\|_2^2 \leq \|\Theta S\|_2^2 \leq (1+\delta_K)\|S\|_2^2 \tag{I.10}$$

Με την συνθήκη αυτή, ο Θ διατηρεί το μέτρο του διανύσματος S κατά τον μετασχηματισμό του σχεδόν σταθερό και εξασφαλίζει ότι οι αναζητούμενες λύσεις δεν ανήκουν στον μηδενοχώρο του. Έτσι, αποκλείει την πιθανότητα της απροσδιοριστίας ΘS = 0, η οποία θα καθιστούσε την ανακατασκευή αδύνατη. Με άλλα λόγια, ο πίνακας Θ είναι σχεδόν ορθογώνιος, και κάθε υποσύνολο K ή και λιγότερων στηλών του σχηματίζει ένα σχεδόν ορθοκανονικό σύστημα.

Επεκτείνοντας την συνθήκη περιορισμένης ισομετρίας για δύο K-sparse σήματα S_1 και S_2, η άνωθεν ανισότητα επαναδιατυπώνεται ακολούθως:

$$(1-\delta_{2K})\|S_1 - S_2\|_2^2 \leq \|\Theta(S_1 - S_2)\|_2^2 \leq (1+\delta_{2K})\|(S_1 - S_2)\|_2^2 \tag{I.11}$$

Και σε αυτή τη περίπτωση, εάν η τιμή της δ_{2K} δεν είναι κοντά στην μονάδα, ο πίνακας Θ διατηρεί την απόσταση των δύο σημάτων σταθερή κατά την προβολή τους στην διάσταση M, με την διαφορά τους να αντιστοιχεί σε ένα διάνυσμα το πολύ 2K μη μηδενικών στοιχείων, εγγυοδοτώντας τη μονοσήμαντη σχέση μεταξύ των S,Y αναπαραστάσεων. Συνδυάζοντας τις ερμηνείες των ανισοτήτων (Ι.10) και (Ι.11), μπορεί εύκολα να εξαχθεί το συμπέρασμα ότι όταν η τιμή της σταθεράς ισομετρίας προσεγγίζει το μηδέν εξασφαλίζεται η εύρεση μιας και μοναδικής λύσης S* για την εξίσωση (Ι.7). Εάν μάλιστα ισχύει η σχέση $\delta_{2K} < \sqrt{2} - 1$, τότε η λύση αυτή ικανοποιεί τις ακόλουθες δύο εξισώσεις:

$$\|\Theta(S^* - S)\|_1 \leq C_0 \|S - S_K\|_1 \tag{I.12}$$

$$\|S^* - S\|_2 \leq \frac{C_0}{\sqrt{K}} \|S - S_K\|_1 \tag{I.13}$$

όπου C_0 είναι μία σταθερά και S_K το διάνυσμα που προκύπτει από το αρχικό σήμα S, όταν από αυτό κρατήσουμε μόνο τα στοιχεία με τις μεγαλύτερες τιμές του. Στο ενδεχόμενο που το S είναι πραγματικά αραιό και ταυτίζεται με το S_K, η ανακατασκευή S* είναι τέλεια με $S = S_K = S^*$. Στην αντίθετη περίπτωση όμως που το σήμα είναι απλά συμπιέσιμο, οι παραπάνω εξισώσεις αξιολογούν την ποιότητα αυτής της προσεγγιστικής ανακατασκευής [59].

Στο σημείο αυτό θα πρέπει να σημειωθεί, ότι η επαλήθευση της συνθήκης της περιορισμένης ισομετρίας είναι μια αρκετά δύσκολη διαδικασία και δεν επιστρατεύεται συχνά, αφού η ιδιότητα της ασυμφωνίας συνήθως επαρκεί για την κατασκευή και την αξιολόγηση των πινάκων συμπιεστικής δειγματοληψίας Θ. Εντούτοις, έχει παρατηρηθεί ότι πίνακες τυχαίων και στατιστικά ανεξάρτητων στοιχείων, όπως αυτοί που αναφέρθηκαν στις προηγούμενες ενότητες, παρουσιάζουν μικρή σταθεράς ισομετρίας αρκεί ο αριθμός των γραμμών τους N να είναι της τάξης του Kln(M/K) [59].

ΠΑΡΑΡΤΗΜΑ ΙΙ

I.1 Αποτελέσματα Ελέγχων NIST

Πίνακας ΙΙ.1: Αναλυτικός πίνακας αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα unclonability.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη.

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\unclonability.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
18	14	16	9	5	11	5	10	5	7	0.01672	96/100	Frequency
7	6	5	8	17	14	15	5	9	14	0.02882	100/100	Block Frequency
15	10	16	13	8	5	10	8	5	10	0.17187	97/100	Cumulative Sums
15	12	13	10	8	8	12	6	8	8	0.59555	96/100	Cumulative Sums
15	15	6	16	10	8	6	8	6	10	0.11539	100/100	Runs
10	13	12	15	9	7	11	8	9	6	0.63712	97/100	Longest Run
9	12	10	10	16	9	8	11	8	7	0.73992	99/100	Rank
13	12	11	9	9	7	11	13	4	11	0.61631	97/100	DFT
13	11	9	6	12	12	9	8	5	15	0.43727	100/100	Non-Overlapping Temp
7	14	14	9	10	9	8	9	12	8	0.77919	100/100	Non-Overlapping Temp
7	9	9	7	10	6	6	18	12	16	0.07572	100/100	Non-Overlapping Temp
8	12	10	13	10	10	13	9	8	7	0.91141	99/100	Non-Overlapping Temp
14	7	13	11	9	9	12	9	6	10	0.75976	99/100	Non-Overlapping Temp
11	9	13	8	5	11	15	7	6	15	0.23681	100/100	Non-Overlapping Temp
13	10	10	8	14	9	6	7	10	13	0.69931	98/100	Non-Overlapping Temp
9	14	8	9	6	16	19	8	7	4	0.01560	98/100	Non-Overlapping Temp
16	5	8	13	8	12	14	5	10	9	0.19169	99/100	Non-Overlapping Temp
7	11	7	9	14	14	6	8	7	17	0.16261	99/100	Non-Overlapping Temp
8	7	11	12	13	13	8	17	5	6	0.16261	100/100	Non-Overlapping Temp
12	6	5	10	10	11	9	12	12	13	0.69931	99/100	Non-Overlapping Temp
11	9	10	7	7	10	12	11	14	9	0.89776	99/100	Non-Overlapping Temp
9	11	7	13	5	12	12	8	12	11	0.71975	100/100	Non-Overlapping Temp
8	16	11	10	8	9	8	9	11	10	0.81654	100/100	Non-Overlapping Temp
14	10	11	8	10	11	8	11	4	13	0.61631	98/100	Non-Overlapping Temp
10	10	10	12	13	8	8	7	12	10	0.94631	100/100	Non-Overlapping Temp
11	7	8	11	9	12	10	9	8	15	0.83431	100/100	Non-Overlapping Temp
5	9	14	11	12	10	11	7	13	8	0.63712	100/100	Non-Overlapping Temp
13	9	11	10	9	6	9	11	10	12	0.94631	98/100	Non-Overlapping Temp
11	13	10	7	8	7	17	8	11	8	0.43727	100/100	Non-Overlapping Temp
7	12	10	11	8	17	11	7	7	10	0.47499	100/100	Non-Overlapping Temp
9	9	7	11	11	10	8	14	12	9	0.92408	100/100	Non-Overlapping Temp
14	8	9	5	13	9	12	9	10	11	0.71975	100/100	Non-Overlapping Temp
8	6	5	14	6	12	14	8	9	18	0.05536	100/100	Non-Overlapping Temp
8	11	14	7	13	5	14	6	9	13	0.30413	100/100	Non-Overlapping Temp
14	10	10	10	10	9	8	9	8	12	0.96430	100/100	Non-Overlapping Temp
13	8	7	8	10	10	8	15	9	12	0.73992	99/100	Non-Overlapping Temp
9	15	8	11	7	11	12	10	11	6	0.71975	98/100	Non-Overlapping Temp
11	12	8	14	5	15	6	10	11	8	0.38383	98/100	Non-Overlapping Temp
8	8	15	12	12	7	11	11	5	11	0.55442	99/100	Non-Overlapping Temp
7	10	8	13	7	10	15	7	15	8	0.40120	99/100	Non-Overlapping Temp
4	11	12	8	7	10	11	15	11	11	0.51412	100/100	Non-Overlapping Temp
10	14	11	6	6	9	14	12	8	10	0.59555	100/100	Non-Overlapping Temp
6	11	7	14	10	8	11	12	11	10	0.81654	99/100	Non-Overlapping Temp
7	9	5	16	14	9	18	9	6	7	0.03757	100/100	Non-Overlapping Temp
11	17	9	9	4	8	5	11	10	16	0.08052	97/100	Non-Overlapping Temp
13	5	7	9	11	10	10	16	8	11	0.47499	99/100	Non-Overlapping Temp
9	9	16	9	11	9	14	4	11	8	0.36692	100/100	Non-Overlapping Temp
14	6	9	10	11	10	10	13	10	7	0.81654	98/100	Non-Overlapping Temp

6	12	8	12	13	10	14	7	9	9	0.69931	99/100	Non-Overlapping Temp
7	7	18	8	9	10	13	14	6	8	0.15376	98/100	Non-Overlapping Temp
10	9	9	9	8	6	11	10	14	14	0.77919	98/100	Non-Overlapping Temp
8	15	6	9	7	11	13	11	8	12	0.59555	99/100	Non-Overlapping Temp
6	8	14	13	10	10	6	15	8	10	0.43727	100/100	Non-Overlapping Temp
8	9	11	8	4	14	8	12	16	10	0.30413	98/100	Non-Overlapping Temp
7	10	13	13	11	4	11	7	12	12	0.51412	99/100	Non-Overlapping Temp
6	6	10	7	10	15	11	8	12	15	0.35049	99/100	Non-Overlapping Temp
9	15	12	7	7	7	7	8	14	14	0.33454	100/100	Non-Overlapping Temp
7	10	6	12	6	9	16	10	13	11	0.41902	100/100	Non-Overlapping Temp
13	7	11	4	15	10	14	13	5	8	0.14533	100/100	Non-Overlapping Temp
10	9	11	9	6	10	13	11	13	8	0.89776	98/100	Non-Overlapping Temp
10	4	15	5	11	12	9	17	8	9	0.10253	99/100	Non-Overlapping Temp
9	11	12	17	9	11	9	6	6	10	0.43727	100/100	Non-Overlapping Temp
10	7	9	16	7	7	8	10	14	12	0.45594	99/100	Non-Overlapping Temp
11	9	9	9	8	10	12	13	8	11	0.97807	98/100	Non-Overlapping Temp
8	9	9	8	13	16	7	11	11	8	0.63712	99/100	Non-Overlapping Temp
8	7	8	13	3	13	8	16	18	6	0.01560	100/100	Non-Overlapping Temp
8	8	8	11	10	12	9	13	8	13	0.91141	98/100	Non-Overlapping Temp
11	12	11	11	10	10	8	12	7	8	0.97170	99/100	Non-Overlapping Temp
6	12	9	16	8	7	13	7	9	13	0.36692	100/100	Non-Overlapping Temp
15	6	7	12	13	5	9	9	16	8	0.16261	100/100	Non-Overlapping Temp
10	9	12	9	7	5	9	20	14	5	0.03292	99/100	Non-Overlapping Temp
12	8	13	7	13	9	9	6	9	14	0.63712	99/100	Non-Overlapping Temp
12	5	12	10	14	8	10	11	8	10	0.75976	100/100	Non-Overlapping Temp
21	12	10	11	6	7	6	7	7	13	0.02200	97/100	Non-Overlapping Temp
9	9	6	10	19	7	7	12	12	9	0.18156	97/100	Non-Overlapping Temp
14	11	11	6	12	10	10	8	9	9	0.88317	98/100	Non-Overlapping Temp
16	9	12	13	3	11	11	6	11	8	0.20227	96/100	Non-Overlapping Temp
12	11	13	6	11	12	6	10	11	8	0.77919	98/100	Non-Overlapping Temp
7	9	10	12	17	7	9	10	9	10	0.59555	99/100	Non-Overlapping Temp
11	11	6	8	6	8	11	14	13	12	0.61631	99/100	Non-Overlapping Temp
11	7	12	7	13	7	6	9	17	11	0.28967	98/100	Non-Overlapping Temp
13	13	8	11	11	8	10	10	13	3	0.47499	100/100	Non-Overlapping Temp
13	11	9	6	12	12	9	8	5	15	0.43727	100/100	Non-Overlapping Temp
9	8	9	10	16	8	12	8	9	11	0.77919	99/100	Non-Overlapping Temp
12	8	12	8	6	9	10	13	8	14	0.71975	98/100	Non-Overlapping Temp
13	10	10	9	10	8	10	9	9	12	0.99147	99/100	Non-Overlapping Temp
6	6	14	9	12	12	12	12	7	10	0.59555	99/100	Non-Overlapping Temp
14	6	6	11	11	11	12	9	12	8	0.69931	99/100	Non-Overlapping Temp
7	4	8	6	16	8	10	21	8	12	0.00536	99/100	Non-Overlapping Temp
11	5	13	12	9	9	8	14	7	12	0.59555	100/100	Non-Overlapping Temp
8	11	9	14	14	5	10	4	13	12	0.26225	100/100	Non-Overlapping Temp
7	11	7	13	12	12	13	4	13	8	0.40120	100/100	Non-Overlapping Temp
8	7	10	12	11	13	9	11	10	9	0.96430	100/100	Non-Overlapping Temp
6	7	9	18	13	7	7	4	11	18	0.00954	100/100	Non-Overlapping Temp
9	5	8	7	10	14	12	11	11	13	0.63712	100/100	Non-Overlapping Temp
10	9	8	10	13	14	10	8	15	3	0.28967	98/100	Non-Overlapping Temp
12	5	15	9	9	7	13	5	13	12	0.26225	99/100	Non-Overlapping Temp
8	9	8	4	20	10	9	11	12	9	0.08559	100/100	Non-Overlapping Temp
9	8	10	10	17	10	7	6	15	8	0.28967	97/100	Non-Overlapping Temp
9	5	14	15	13	9	13	9	5	8	0.23681	100/100	Non-Overlapping Temp
10	8	7	8	14	8	11	12	11	11	0.88317	98/100	Non-Overlapping Temp
9	16	9	7	11	11	10	9	8	10	0.79814	100/100	Non-Overlapping Temp
13	14	6	11	11	8	9	10	13	5	0.51412	100/100	Non-Overlapping Temp
10	10	11	6	8	12	15	10	10	8	0.79814	98/100	Non-Overlapping Temp
8	7	11	13	6	15	9	11	11	9	0.65793	99/100	Non-Overlapping Temp
10	11	4	12	15	4	11	8	6	19	0.01560	99/100	Non-Overlapping Temp
6	10	8	12	11	13	14	7	11	8	0.69931	100/100	Non-Overlapping Temp
8	13	3	11	10	6	10	17	15	7	0.06282	99/100	Non-Overlapping Temp
9	17	6	7	12	11	8	16	10	4	0.07572	99/100	Non-Overlapping Temp
9	9	3	15	6	5	12	13	16	12	0.04872	99/100	Non-Overlapping Temp

12	15	8	10	9	7	12	11	4	12	0.45594	99/100	Non-Overlapping Temp
8	7	10	10	6	12	13	11	11	12	0.85138	100/100	Non-Overlapping Temp
7	15	12	6	5	10	7	17	9	12	0.11539	98/100	Non-Overlapping Temp
12	9	9	12	9	11	9	15	10	4	0.59555	100/100	Non-Overlapping Temp
9	4	9	14	11	9	19	10	9	6	0.08052	98/100	Non-Overlapping Temp
15	11	6	8	14	12	9	12	6	7	0.38383	95/100*	Non-Overlapping Temp
11	8	10	10	12	13	13	11	7	5	0.71975	99/100	Non-Overlapping Temp
7	10	8	6	17	10	9	17	8	8	0.13728	99/100	Non-Overlapping Temp
5	8	11	8	7	9	11	13	12	16	0.40120	99/100	Non-Overlapping Temp
14	7	12	9	6	3	19	13	7	10	0.02200	98/100	Non-Overlapping Temp
7	9	13	12	8	8	11	10	11	11	0.94631	98/100	Non-Overlapping Temp
9	10	17	7	6	8	12	8	13	10	0.38383	98/100	Non-Overlapping Temp
13	12	8	11	10	11	7	8	10	10	0.95584	98/100	Non-Overlapping Temp
10	10	10	12	8	5	14	13	11	7	0.65793	97/100	Non-Overlapping Temp
7	14	5	17	13	9	8	8	7	12	0.16261	99/100	Non-Overlapping Temp
9	12	11	6	10	10	13	10	9	10	0.95584	99/100	Non-Overlapping Temp
10	7	5	10	9	8	7	14	17	13	0.20227	100/100	Non-Overlapping Temp
10	4	9	16	14	6	15	11	8	7	0.10879	98/100	Non-Overlapping Temp
10	7	11	12	10	11	16	6	9	8	0.61631	98/100	Non-Overlapping Temp
7	7	12	13	11	5	8	13	9	15	0.38383	100/100	Non-Overlapping Temp
12	9	5	10	16	13	7	10	12	6	0.31908	99/100	Non-Overlapping Temp
9	7	8	10	7	9	8	13	13	16	0.51412	100/100	Non-Overlapping Temp
10	7	11	9	9	10	16	13	9	6	0.59555	98/100	Non-Overlapping Temp
12	8	12	14	11	8	10	8	9	8	0.89776	99/100	Non-Overlapping Temp
6	10	12	9	17	8	7	10	8	13	0.38383	97/100	Non-Overlapping Temp
13	7	13	13	8	3	8	10	13	12	0.30413	97/100	Non-Overlapping Temp
7	16	8	8	10	9	12	11	7	12	0.61631	100/100	Non-Overlapping Temp
10	8	19	4	13	6	11	7	9	13	0.05536	99/100	Non-Overlapping Temp
12	7	8	9	6	6	14	14	15	9	0.28967	98/100	Non-Overlapping Temp
9	10	16	15	5	11	11	9	7	7	0.28967	98/100	Non-Overlapping Temp
14	13	10	9	16	5	10	9	4	10	0.19169	96/100	Non-Overlapping Temp
12	7	13	12	14	12	5	5	11	9	0.36692	98/100	Non-Overlapping Temp
14	6	9	9	12	12	15	7	11	5	0.33454	99/100	Non-Overlapping Temp
8	7	17	12	8	10	9	9	10	10	0.61631	98/100	Non-Overlapping Temp
5	12	10	13	9	10	12	8	9	12	0.81654	99/100	Non-Overlapping Temp
11	8	12	10	3	11	13	9	7	16	0.24928	100/100	Non-Overlapping Temp
14	5	6	9	11	12	14	9	14	6	0.26225	100/100	Non-Overlapping Temp
9	5	15	8	9	7	14	12	11	10	0.47499	100/100	Non-Overlapping Temp
14	10	9	13	8	10	12	10	3	11	0.49439	99/100	Non-Overlapping Temp
10	10	9	6	13	13	9	8	11	11	0.89776	99/100	Non-Overlapping Temp
12	9	8	10	9	13	9	5	10	15	0.63712	99/100	Non-Overlapping Temp
11	9	16	10	10	2	11	14	8	9	0.19169	99/100	Non-Overlapping Temp
14	7	11	5	11	8	14	14	5	11	0.24928	99/100	Non-Overlapping Temp
10	7	7	7	9	8	18	7	15	12	0.14533	98/100	Non-Overlapping Temp
9	12	12	3	9	10	15	8	9	13	0.36692	100/100	Non-Overlapping Temp
13	13	8	11	11	8	10	10	13	3	0.47499	100/100	Non-Overlapping Temp
11	13	9	11	12	8	9	8	16	3	0.27571	98/100	Overlapping Temp
11	8	12	14	5	10	11	8	12	9	0.73992	98/100	Maurer’s Universal
14	10	10	6	10	10	11	10	10	9	0.94631	100/100	Approximate Entropy
6	1	3	4	9	6	5	9	3	6	0.21331	52/52	Random Excursions
4	5	4	9	5	3	10	3	5	4	0.31908	51/52	Random Excursions
3	5	6	6	7	4	7	3	8	3	0.69931	52/52	Random Excursions
2	5	4	4	7	4	4	7	8	7	0.65793	52/52	Random Excursions
5	4	7	4	9	3	1	3	8	8	0.17187	52/52	Random Excursions
6	3	6	7	5	2	8	3	5	7	0.61631	50/52	Random Excursions
4	4	11	8	3	2	5	8	4	3	0.09658	52/52	Random Excursions
4	8	5	4	5	3	7	6	5	5	0.91141	52/52	Random Excursions
5	2	6	6	4	6	4	4	9	6	0.69931	51/52	Random Excursions V
4	7	4	6	4	5	6	5	5	6	0.99147	52/52	Random Excursions V
4	6	7	5	4	6	6	2	8	4	0.77919	52/52	Random Excursions V
3	6	4	6	3	9	7	3	6	5	0.61631	52/52	Random Excursions V
3	3	4	9	6	6	7	4	1	9	0.17187	52/52	Random Excursions V

3	7	3	8	6	2	9	6	2	6	0.23681	52/52	Random Excursions V
6	3	5	7	6	4	5	5	5	6	0.98345	52/52	Random Excursions V
4	4	6	2	6	9	8	8	3	2	0.21331	52/52	Random Excursions V
0	3	7	2	8	10	5	8	4	5	0.04568	52/52	Random Excursions V
3	8	5	3	4	6	3	8	6	6	0.65793	52/52	Random Excursions V
7	3	6	7	4	6	3	6	5	5	0.91141	52/52	Random Excursions V
7	4	4	7	6	5	7	5	5	2	0.85138	51/52	Random Excursions V
7	5	8	6	3	7	4	6	4	2	0.65793	51/52	Random Excursions V
6	9	3	8	6	3	4	3	7	3	0.38383	51/52	Random Excursions V
6	9	8	2	4	7	5	4	3	4	0.41902	52/52	Random Excursions V
8	10	5	4	5	2	3	8	2	5	0.15376	52/52	Random Excursions V
10	8	4	4	4	5	8	5	3	1	0.15376	52/52	Random Excursions V
10	8	1	8	2	7	7	4	3	2	0.03517	52/52	Random Excursions V
6	7	10	12	15	10	11	9	10	10	0.77919	99/100	Serial
7	4	10	12	9	12	14	12	7	13	0.41902	99/100	Serial
8	12	7	10	13	8	14	11	11	6	0.69931	99/100	Linear Complexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 49 for a sample size = 52 binary sequences.

Πίνακας II.2: Αναλυτικός πίνακας αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα unpredictability128_n2.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη.

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\unpredictability128_n2.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
5	16	8	10	10	15	7	5	11	13	0.14533	100/100	Frequency
7	16	11	12	7	10	10	10	7	10	0.65793	99/100	Block Frequency
6	8	15	5	9	13	13	9	13	9	0.35049	99/100	Cumulative Sums
6	11	10	6	7	12	14	15	9	10	0.45594	100/100	Cumulative Sums
9	7	11	7	13	12	8	13	7	13	0.69931	100/100	Runs
10	12	5	6	10	11	12	9	12	13	0.69931	100/100	Longest Run
9	16	5	11	8	13	13	12	4	9	0.18156	98/100	Rank
7	10	9	9	10	13	13	12	9	8	0.92408	99/100	DFT
15	11	6	5	8	14	11	4	12	14	0.10879	98/100	Non-Overlapping Temp
14	10	10	7	9	9	11	11	8	11	0.94631	97/100	Non-Overlapping Temp
12	9	6	14	14	13	6	9	11	6	0.38383	99/100	Non-Overlapping Temp
11	10	13	8	10	7	10	10	6	15	0.69931	99/100	Non-Overlapping Temp
5	12	8	7	9	8	13	14	11	13	0.51412	99/100	Non-Overlapping Temp
10	14	5	14	9	9	11	10	4	14	0.26225	99/100	Non-Overlapping Temp
11	6	10	12	9	8	15	8	8	13	0.65793	100/100	Non-Overlapping Temp
19	13	7	9	11	11	9	6	10	5	0.10879	98/100	Non-Overlapping Temp
7	11	15	11	8	7	6	15	10	10	0.43727	100/100	Non-Overlapping Temp
8	10	12	8	12	8	15	8	8	11	0.79814	99/100	Non-Overlapping Temp
5	6	6	7	16	13	10	10	15	12	0.12233	100/100	Non-Overlapping Temp
9	8	14	5	11	8	9	7	16	13	0.30413	99/100	Non-Overlapping Temp
10	7	10	11	13	5	8	11	11	14	0.67869	99/100	Non-Overlapping Temp
10	12	6	12	12	8	6	13	10	11	0.75976	100/100	Non-Overlapping Temp
11	12	9	15	9	12	5	9	6	12	0.51412	100/100	Non-Overlapping Temp
17	9	13	11	7	8	10	10	6	9	0.43727	99/100	Non-Overlapping Temp
7	11	11	13	10	12	4	10	10	12	0.69931	99/100	Non-Overlapping Temp
11	4	6	15	9	8	10	16	13	8	0.15376	99/100	Non-Overlapping Temp
15	7	12	9	10	13	8	8	7	11	0.67869	99/100	Non-Overlapping Temp
12	15	10	8	10	7	10	9	11	8	0.85138	100/100	Non-Overlapping Temp
6	7	9	17	11	11	9	9	9	12	0.49439	99/100	Non-Overlapping Temp
5	12	13	5	11	7	9	15	7	16	0.10879	99/100	Non-Overlapping Temp
7	13	7	7	9	13	5	14	10	15	0.26225	100/100	Non-Overlapping Temp

10	5	15	7	13	8	11	15	10	6	0.24928	100/100	Non-Overlapping Temp
10	11	6	9	7	9	12	15	13	8	0.63712	99/100	Non-Overlapping Temp
7	8	6	11	11	9	13	14	11	10	0.75976	99/100	Non-Overlapping Temp
11	11	7	8	9	14	11	13	7	9	0.81654	99/100	Non-Overlapping Temp
14	10	10	12	7	12	12	9	10	4	0.59555	100/100	Non-Overlapping Temp
10	17	15	6	7	4	13	8	13	7	0.05536	98/100	Non-Overlapping Temp
21	6	13	11	7	11	5	5	10	11	0.01357	97/100	Non-Overlapping Temp
10	14	15	8	10	8	11	13	5	6	0.35049	98/100	Non-Overlapping Temp
4	13	10	11	8	7	12	8	13	14	0.41902	99/100	Non-Overlapping Temp
6	12	8	13	14	12	7	14	4	10	0.24928	100/100	Non-Overlapping Temp
6	9	11	14	12	8	12	8	11	9	0.81654	100/100	Non-Overlapping Temp
4	13	10	7	9	10	10	19	10	8	0.12233	100/100	Non-Overlapping Temp
11	4	11	10	8	5	14	10	14	13	0.28967	97/100	Non-Overlapping Temp
12	10	10	7	9	10	12	13	5	12	0.77919	98/100	Non-Overlapping Temp
5	7	11	8	12	14	11	13	10	9	0.63712	100/100	Non-Overlapping Temp
6	7	22	11	10	8	9	9	12	6	0.02055	99/100	Non-Overlapping Temp
10	9	8	7	10	15	11	6	11	13	0.67869	99/100	Non-Overlapping Temp
14	5	8	19	8	10	8	7	13	8	0.07572	98/100	Non-Overlapping Temp
12	12	9	13	11	3	9	9	11	11	0.61631	99/100	Non-Overlapping Temp
13	12	10	11	13	10	6	6	12	7	0.65793	98/100	Non-Overlapping Temp
14	10	11	6	13	8	7	14	7	10	0.53415	100/100	Non-Overlapping Temp
17	8	7	7	14	12	8	10	10	7	0.31908	98/100	Non-Overlapping Temp
17	12	16	2	7	7	10	9	16	4	0.00371	96/100	Non-Overlapping Temp
5	14	9	8	6	7	10	13	19	9	0.06282	100/100	Non-Overlapping Temp
14	11	11	8	15	6	11	3	7	14	0.12962	96/100	Non-Overlapping Temp
11	12	6	9	11	11	14	15	4	7	0.27571	99/100	Non-Overlapping Temp
19	9	12	8	6	5	8	9	11	13	0.10253	99/100	Non-Overlapping Temp
7	11	11	8	13	11	14	6	13	6	0.51412	100/100	Non-Overlapping Temp
13	8	13	8	8	12	11	10	9	8	0.91141	98/100	Non-Overlapping Temp
9	19	8	8	10	12	5	10	9	10	0.21331	100/100	Non-Overlapping Temp
8	7	11	15	6	10	12	12	10	9	0.69931	99/100	Non-Overlapping Temp
18	8	14	10	5	10	10	5	8	12	0.11539	99/100	Non-Overlapping Temp
9	9	13	7	12	10	7	9	11	13	0.88317	100/100	Non-Overlapping Temp
7	13	11	11	7	17	2	13	9	10	0.08559	99/100	Non-Overlapping Temp
11	6	12	7	10	12	11	9	7	15	0.63712	100/100	Non-Overlapping Temp
7	9	12	13	8	11	8	11	8	13	0.86769	100/100	Non-Overlapping Temp
7	13	10	9	9	9	11	15	7	10	0.77919	98/100	Non-Overlapping Temp
8	9	11	10	6	16	9	8	8	15	0.41902	99/100	Non-Overlapping Temp
11	10	10	11	8	14	9	10	12	5	0.81654	100/100	Non-Overlapping Temp
11	5	8	11	13	14	5	14	8	11	0.33454	99/100	Non-Overlapping Temp
10	11	16	11	9	9	9	9	10	6	0.75976	99/100	Non-Overlapping Temp
9	12	12	10	10	12	9	9	12	5	0.88317	100/100	Non-Overlapping Temp
6	11	8	11	7	14	7	12	12	12	0.65793	100/100	Non-Overlapping Temp
12	6	10	7	10	12	14	13	5	11	0.49439	98/100	Non-Overlapping Temp
15	13	14	9	7	11	11	5	6	9	0.31908	99/100	Non-Overlapping Temp
14	16	8	14	7	12	4	5	8	12	0.08052	100/100	Non-Overlapping Temp
11	13	12	9	4	7	13	8	13	10	0.51412	99/100	Non-Overlapping Temp
15	12	15	7	9	10	8	5	9	10	0.40120	99/100	Non-Overlapping Temp
6	11	10	10	8	14	7	15	12	7	0.49439	100/100	Non-Overlapping Temp
9	9	11	11	7	12	8	8	15	10	0.83431	100/100	Non-Overlapping Temp
9	8	12	14	12	9	8	10	10	8	0.92408	99/100	Non-Overlapping Temp
15	11	6	5	8	14	11	4	12	14	0.10879	98/100	Non-Overlapping Temp
8	11	7	9	12	7	12	9	7	18	0.30413	100/100	Non-Overlapping Temp
8	8	12	8	13	10	10	15	10	6	0.67869	100/100	Non-Overlapping Temp
6	6	8	10	11	11	14	13	9	12	0.65793	98/100	Non-Overlapping Temp
12	9	10	11	11	6	12	8	5	16	0.41902	99/100	Non-Overlapping Temp
12	11	4	15	7	15	9	10	4	13	0.10253	97/100	Non-Overlapping Temp
7	7	14	17	12	10	14	5	7	7	0.10253	99/100	Non-Overlapping Temp
13	11	8	9	13	6	7	11	11	11	0.81654	98/100	Non-Overlapping Temp
12	10	6	14	10	7	9	7	10	15	0.53415	100/100	Non-Overlapping Temp
10	12	5	9	8	11	15	13	2	15	0.07118	99/100	Non-Overlapping Temp
6	11	9	13	8	9	9	16	7	12	0.51412	98/100	Non-Overlapping Temp

14	9	10	9	12	13	7	11	8	7	0.79814	100/100	Non-Overlapping Temp
15	13	6	11	6	17	6	11	10	5	0.07118	100/100	Non-Overlapping Temp
10	7	9	11	6	16	11	14	7	9	0.43727	100/100	Non-Overlapping Temp
13	15	10	7	4	17	2	12	11	9	0.01919	96/100	Non-Overlapping Temp
8	8	8	16	12	7	15	9	11	6	0.31908	99/100	Non-Overlapping Temp
14	9	12	12	6	10	11	5	10	11	0.65793	99/100	Non-Overlapping Temp
5	9	6	14	18	8	11	8	13	8	0.10879	99/100	Non-Overlapping Temp
14	11	6	12	11	10	9	11	7	9	0.83431	100/100	Non-Overlapping Temp
12	6	15	11	7	10	13	6	11	9	0.51412	97/100	Non-Overlapping Temp
8	12	14	11	18	9	8	10	4	6	0.10253	100/100	Non-Overlapping Temp
11	14	9	6	14	13	6	8	9	10	0.53415	99/100	Non-Overlapping Temp
14	10	12	12	8	15	5	5	5	14	0.10879	98/100	Non-Overlapping Temp
7	8	9	7	10	13	15	11	10	10	0.75976	99/100	Non-Overlapping Temp
10	8	9	7	9	10	10	13	10	14	0.91141	98/100	Non-Overlapping Temp
4	17	5	8	10	11	15	11	9	10	0.11539	100/100	Non-Overlapping Temp
16	8	8	10	8	11	11	8	8	12	0.71975	99/100	Non-Overlapping Temp
11	12	14	10	8	10	9	10	8	8	0.94631	100/100	Non-Overlapping Temp
6	12	10	12	5	10	15	15	5	10	0.19169	99/100	Non-Overlapping Temp
9	13	12	13	6	11	10	11	5	10	0.67869	99/100	Non-Overlapping Temp
7	8	12	7	11	15	11	5	14	10	0.40120	99/100	Non-Overlapping Temp
7	6	9	13	10	14	10	12	10	9	0.77919	99/100	Non-Overlapping Temp
17	11	9	8	13	14	10	11	4	3	0.05536	100/100	Non-Overlapping Temp
10	9	14	10	12	15	10	6	10	4	0.36692	100/100	Non-Overlapping Temp
11	9	2	11	13	7	14	13	14	6	0.11539	97/100	Non-Overlapping Temp
12	10	7	9	12	7	14	12	9	8	0.81654	99/100	Non-Overlapping Temp
12	9	7	8	8	13	9	13	11	10	0.89776	98/100	Non-Overlapping Temp
13	11	12	15	13	7	10	7	2	10	0.16261	99/100	Non-Overlapping Temp
15	11	7	17	6	14	7	7	7	9	0.10879	95/100*	Non-Overlapping Temp
9	9	7	9	9	12	15	9	6	15	0.49439	100/100	Non-Overlapping Temp
9	7	8	6	14	9	16	10	14	7	0.28967	98/100	Non-Overlapping Temp
11	10	8	8	14	9	6	14	12	8	0.67869	99/100	Non-Overlapping Temp
15	6	12	10	14	9	7	6	10	11	0.45594	98/100	Non-Overlapping Temp
5	9	10	11	10	13	10	8	14	10	0.77919	99/100	Non-Overlapping Temp
6	12	14	8	10	12	4	11	16	7	0.18156	98/100	Non-Overlapping Temp
13	11	9	8	10	6	11	8	13	11	0.86769	99/100	Non-Overlapping Temp
10	6	5	7	12	18	14	6	13	9	0.06688	99/100	Non-Overlapping Temp
4	11	8	11	15	4	10	12	10	15	0.15376	100/100	Non-Overlapping Temp
10	14	13	7	9	10	11	5	7	14	0.47499	98/100	Non-Overlapping Temp
10	19	9	13	13	10	5	6	10	5	0.05536	99/100	Non-Overlapping Temp
8	7	11	7	7	13	13	11	9	14	0.65793	99/100	Non-Overlapping Temp
11	15	14	6	10	5	14	10	5	10	0.19169	99/100	Non-Overlapping Temp
2	10	9	16	8	14	10	10	12	9	0.18156	100/100	Non-Overlapping Temp
13	7	11	12	9	11	10	10	5	12	0.79814	99/100	Non-Overlapping Temp
12	11	9	8	7	9	11	8	7	18	0.36692	99/100	Non-Overlapping Temp
10	7	12	11	16	12	8	8	7	9	0.61631	99/100	Non-Overlapping Temp
13	10	10	7	10	11	5	7	17	10	0.33454	100/100	Non-Overlapping Temp
2	7	20	11	6	6	10	16	10	12	0.00345	100/100	Non-Overlapping Temp
11	12	9	14	5	8	12	10	10	9	0.77919	100/100	Non-Overlapping Temp
11	9	10	6	15	14	6	11	8	10	0.53415	99/100	Non-Overlapping Temp
14	9	11	9	11	8	11	5	10	12	0.79814	98/100	Non-Overlapping Temp
8	8	8	11	7	16	14	9	7	12	0.45594	99/100	Non-Overlapping Temp
11	7	11	21	3	6	14	6	14	7	0.00256	97/100	Non-Overlapping Temp
10	8	12	16	5	9	8	11	9	12	0.53415	98/100	Non-Overlapping Temp
14	10	7	9	7	14	11	16	7	5	0.20227	99/100	Non-Overlapping Temp
13	10	5	9	6	8	10	12	9	18	0.19169	98/100	Non-Overlapping Temp
14	11	10	12	12	6	10	8	7	10	0.79814	99/100	Non-Overlapping Temp
11	10	10	7	11	5	16	8	12	10	0.53415	98/100	Non-Overlapping Temp
9	6	10	18	15	11	7	8	9	7	0.16261	100/100	Non-Overlapping Temp
12	12	6	7	9	15	7	9	10	13	0.55442	99/100	Non-Overlapping Temp
7	12	8	15	2	20	7	10	6	13	0.00430	99/100	Non-Overlapping Temp
13	7	3	10	9	12	14	4	12	16	0.05898	97/100	Non-Overlapping Temp
7	11	9	16	10	14	8	9	6	10	0.49439	99/100	Non-Overlapping Temp

9	8	12	14	11	10	8	10	10	8	0.94631	99/100	Non-Overlapping Temp
6	11	10	13	11	9	10	7	12	11	0.89776	100/100	Overlapping Temp
10	7	9	6	10	13	11	10	8	16	0.57490	99/100	Maurer’s Universal
8	7	11	8	15	6	16	7	7	15	0.12962	100/100	Approximate Entropy
2	6	8	6	8	9	5	9	9	4	0.40709	65/66	Random Excursions
3	8	7	10	6	7	6	7	7	5	0.77276	66/66	Random Excursions
6	5	5	9	10	7	6	8	6	4	0.73992	66/66	Random Excursions
7	9	11	5	4	4	12	4	5	5	0.11095	66/66	Random Excursions
5	9	8	5	8	6	9	2	7	7	0.56806	66/66	Random Excursions
9	8	6	6	7	6	5	7	6	6	0.97606	65/66	Random Excursions
7	7	4	6	9	4	5	6	5	13	0.23276	66/66	Random Excursions
8	4	5	8	9	5	6	4	10	7	0.60246	64/66	Random Excursions
5	5	5	10	6	7	11	4	6	7	0.50093	66/66	Random Excursions V
4	7	6	7	8	8	7	7	6	6	0.97606	66/66	Random Excursions V
3	8	7	5	12	3	8	6	6	8	0.25355	66/66	Random Excursions V
4	9	6	12	5	2	9	9	6	4	0.10051	66/66	Random Excursions V
6	7	9	6	12	3	3	8	7	5	0.23276	66/66	Random Excursions V
5	13	9	4	5	1	7	10	7	5	0.03517	66/66	Random Excursions V
6	10	5	10	5	5	4	7	6	8	0.60246	66/66	Random Excursions V
9	5	6	8	9	5	5	7	6	6	0.88814	65/66	Random Excursions V
11	5	7	9	4	8	4	4	6	8	0.40709	65/66	Random Excursions V
8	7	8	8	7	5	8	8	4	3	0.73992	65/66	Random Excursions V
8	8	7	3	8	10	6	3	4	9	0.35049	65/66	Random Excursions V
7	7	6	6	2	8	4	7	9	10	0.46860	64/66	Random Excursions V
8	7	6	2	8	5	4	10	8	8	0.43727	65/66	Random Excursions V
7	4	8	5	3	10	3	8	9	9	0.27571	66/66	Random Excursions V
5	8	5	4	8	6	5	4	12	9	0.29925	66/66	Random Excursions V
6	6	4	7	4	7	6	8	10	8	0.77276	66/66	Random Excursions V
5	9	2	3	5	12	4	8	9	9	0.06024	66/66	Random Excursions V
6	9	5	3	6	8	7	5	10	7	0.63712	66/66	Random Excursions V
5	7	10	12	13	14	8	11	9	11	0.63712	99/100	Serial
9	6	10	13	16	8	11	11	6	10	0.49439	99/100	Serial
8	10	11	12	5	13	11	8	10	12	0.81654	99/100	Linear Complexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 62 for a sample size = 66 binary sequences.

Πίνακας ΙΙ.3: Αναλυτικός πίνακας αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα unpredictability128_n4.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη.

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\unpredictability128_n4.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
11	9	12	5	7	11	11	10	12	12	0.83431	100/100	Frequency
10	11	9	9	13	12	8	7	9	12	0.94631	98/100	Block Frequency
11	5	9	15	10	8	8	7	14	13	0.40120	99/100	Cumulative Sums
10	9	10	7	10	6	11	10	12	15	0.77919	100/100	Cumulative Sums
9	8	9	7	10	9	14	9	12	13	0.86769	99/100	Runs
10	13	15	8	8	5	9	13	10	9	0.55442	98/100	Longest Run
11	6	12	12	10	8	8	12	8	13	0.83431	97/100	Rank
11	10	8	8	11	10	7	6	11	18	0.35049	99/100	DFT
8	16	9	10	13	6	7	12	14	5	0.21331	100/100	Non-Overlapping Temp
12	2	8	8	13	14	14	10	12	7	0.16261	100/100	Non-Overlapping Temp
11	9	9	10	12	15	12	12	3	7	0.36692	100/100	Non-Overlapping Temp
11	9	12	12	6	10	7	7	14	12	0.69931	100/100	Non-Overlapping Temp
8	10	8	5	9	10	15	8	15	12	0.41902	100/100	Non-Overlapping Temp
8	11	13	8	10	8	12	8	13	9	0.91141	100/100	Non-Overlapping Temp

6	12	7	6	12	12	11	13	7	14	0.45594	98/100	Non-Overlapping Temp
13	10	16	5	9	9	10	14	8	6	0.28967	98/100	Non-Overlapping Temp
11	5	12	11	10	16	11	5	11	8	0.36692	98/100	Non-Overlapping Temp
12	9	13	12	9	17	5	10	6	7	0.22482	100/100	Non-Overlapping Temp
7	8	12	6	8	10	10	7	16	16	0.22482	98/100	Non-Overlapping Temp
11	14	14	12	7	11	11	7	6	7	0.51412	99/100	Non-Overlapping Temp
6	12	20	3	14	8	10	7	10	10	0.01919	99/100	Non-Overlapping Temp
5	8	14	12	9	12	12	8	10	10	0.71975	100/100	Non-Overlapping Temp
7	8	6	13	11	7	12	12	8	16	0.38383	100/100	Non-Overlapping Temp
14	8	10	7	12	13	5	11	12	8	0.57490	100/100	Non-Overlapping Temp
8	8	3	9	14	13	11	12	14	8	0.28967	100/100	Non-Overlapping Temp
9	16	6	12	6	9	12	9	13	8	0.41902	100/100	Non-Overlapping Temp
16	11	12	6	5	10	9	12	11	8	0.41902	100/100	Non-Overlapping Temp
11	11	11	9	3	12	8	9	11	15	0.45594	100/100	Non-Overlapping Temp
7	17	11	10	9	8	12	7	10	9	0.55442	99/100	Non-Overlapping Temp
8	16	6	10	12	5	9	11	11	12	0.41902	99/100	Non-Overlapping Temp
12	7	5	13	13	11	12	10	9	8	0.67869	99/100	Non-Overlapping Temp
10	10	14	13	12	5	15	9	5	7	0.24928	99/100	Non-Overlapping Temp
6	9	10	9	14	7	12	10	15	8	0.57490	100/100	Non-Overlapping Temp
7	6	10	10	14	13	9	12	11	8	0.73992	99/100	Non-Overlapping Temp
14	9	11	9	9	12	11	6	8	11	0.86769	99/100	Non-Overlapping Temp
11	11	6	12	9	10	10	14	6	11	0.77919	100/100	Non-Overlapping Temp
9	10	11	12	9	8	9	10	10	12	0.99634	99/100	Non-Overlapping Temp
6	7	13	13	8	11	11	7	11	13	0.65793	99/100	Non-Overlapping Temp
12	9	10	8	11	11	6	15	9	9	0.79814	99/100	Non-Overlapping Temp
12	15	10	5	6	13	7	14	14	4	0.07572	99/100	Non-Overlapping Temp
10	11	6	8	7	15	11	12	11	9	0.71975	100/100	Non-Overlapping Temp
10	10	8	11	14	5	9	16	7	10	0.41902	99/100	Non-Overlapping Temp
10	10	11	13	10	7	10	8	10	11	0.98345	98/100	Non-Overlapping Temp
8	11	11	6	13	11	9	15	6	10	0.59555	100/100	Non-Overlapping Temp
9	14	10	12	8	5	17	11	5	9	0.18156	98/100	Non-Overlapping Temp
10	13	10	8	13	7	9	15	8	7	0.63712	99/100	Non-Overlapping Temp
8	13	8	7	9	14	5	13	8	15	0.30413	99/100	Non-Overlapping Temp
10	16	5	16	10	13	14	4	6	6	0.02519	100/100	Non-Overlapping Temp
9	11	11	7	7	14	13	8	10	10	0.83431	98/100	Non-Overlapping Temp
10	14	9	11	13	4	9	7	9	14	0.43727	100/100	Non-Overlapping Temp
13	10	15	10	6	5	14	11	6	10	0.28967	98/100	Non-Overlapping Temp
9	10	8	12	8	12	13	11	10	7	0.93572	96/100	Non-Overlapping Temp
6	11	9	16	15	4	10	11	10	8	0.21331	100/100	Non-Overlapping Temp
13	8	10	8	13	6	8	12	10	12	0.79814	99/100	Non-Overlapping Temp
6	8	8	9	10	10	18	10	14	7	0.24928	100/100	Non-Overlapping Temp
8	8	13	6	8	11	13	12	12	9	0.77919	100/100	Non-Overlapping Temp
10	9	7	11	11	11	7	10	9	15	0.85138	99/100	Non-Overlapping Temp
9	11	9	15	4	8	12	10	15	7	0.30413	99/100	Non-Overlapping Temp
7	11	6	12	12	11	10	11	13	7	0.79814	98/100	Non-Overlapping Temp
8	8	10	10	11	13	10	8	15	7	0.77919	99/100	Non-Overlapping Temp
11	4	12	9	15	6	9	11	12	11	0.43727	97/100	Non-Overlapping Temp
10	9	11	14	11	11	9	13	6	6	0.71975	100/100	Non-Overlapping Temp
16	8	13	10	12	9	11	7	7	7	0.51412	99/100	Non-Overlapping Temp
6	11	8	14	8	20	8	8	8	9	0.08052	99/100	Non-Overlapping Temp
10	7	9	10	4	10	16	7	18	9	0.07572	100/100	Non-Overlapping Temp
11	10	9	10	9	9	12	10	12	8	0.99634	100/100	Non-Overlapping Temp
9	12	11	8	9	12	12	12	9	6	0.91141	99/100	Non-Overlapping Temp
8	9	9	13	11	15	9	8	10	8	0.83431	99/100	Non-Overlapping Temp
10	9	12	10	10	8	15	8	7	11	0.85138	100/100	Non-Overlapping Temp
8	11	15	9	12	16	10	6	10	3	0.13728	100/100	Non-Overlapping Temp
10	12	8	16	9	12	12	7	8	6	0.51412	97/100	Non-Overlapping Temp
10	11	7	8	4	13	9	13	15	10	0.40120	100/100	Non-Overlapping Temp
11	12	13	10	4	10	10	14	9	7	0.57490	99/100	Non-Overlapping Temp
13	8	14	9	12	9	12	10	6	7	0.69931	98/100	Non-Overlapping Temp
6	12	10	5	12	10	10	12	13	10	0.71975	100/100	Non-Overlapping Temp
9	10	9	7	10	11	13	10	11	10	0.98790	100/100	Non-Overlapping Temp

11	9	12	12	10	6	11	9	9	11	0.96430	99/100	Non-Overlapping Temp
15	5	7	13	6	13	11	8	9	13	0.28967	99/100	Non-Overlapping Temp
2	9	12	13	9	16	11	9	12	7	0.16261	100/100	Non-Overlapping Temp
7	10	14	9	10	10	6	15	7	12	0.53415	99/100	Non-Overlapping Temp
15	7	12	7	11	6	16	8	9	9	0.30413	98/100	Non-Overlapping Temp
7	11	13	9	15	8	9	12	11	5	0.53415	98/100	Non-Overlapping Temp
8	16	9	10	13	6	7	12	14	5	0.21331	100/100	Non-Overlapping Temp
16	7	11	12	8	10	12	9	7	8	0.61631	98/100	Non-Overlapping Temp
11	13	7	11	10	12	16	6	7	7	0.40120	96/100	Non-Overlapping Temp
8	11	10	9	12	14	10	10	4	12	0.67869	100/100	Non-Overlapping Temp
13	12	15	6	9	4	10	14	8	9	0.26225	98/100	Non-Overlapping Temp
8	9	22	9	9	6	11	4	9	13	0.01099	100/100	Non-Overlapping Temp
11	9	14	10	10	11	8	8	9	10	0.97170	99/100	Non-Overlapping Temp
13	11	10	8	13	8	7	11	10	9	0.92408	99/100	Non-Overlapping Temp
8	6	7	11	11	17	9	13	11	7	0.35049	100/100	Non-Overlapping Temp
10	12	10	13	6	11	10	15	7	6	0.53415	99/100	Non-Overlapping Temp
16	13	10	7	10	12	9	4	11	8	0.35049	99/100	Non-Overlapping Temp
17	12	10	9	10	5	13	6	9	9	0.30413	99/100	Non-Overlapping Temp
10	6	12	13	12	11	9	11	9	7	0.86769	98/100	Non-Overlapping Temp
13	7	12	12	11	7	8	14	8	8	0.69931	100/100	Non-Overlapping Temp
8	7	12	11	4	13	14	11	13	7	0.36692	99/100	Non-Overlapping Temp
9	6	10	9	11	6	13	11	12	13	0.75976	98/100	Non-Overlapping Temp
15	10	11	9	10	9	9	12	6	9	0.83431	100/100	Non-Overlapping Temp
8	8	12	17	13	8	9	7	8	10	0.45594	100/100	Non-Overlapping Temp
9	8	16	8	14	8	9	13	8	7	0.45594	100/100	Non-Overlapping Temp
12	11	8	11	9	14	12	7	7	9	0.83431	96/100	Non-Overlapping Temp
6	11	10	9	9	12	11	10	11	11	0.97807	100/100	Non-Overlapping Temp
10	9	7	15	9	13	9	11	9	8	0.81654	99/100	Non-Overlapping Temp
12	17	4	5	9	10	9	11	13	10	0.18156	98/100	Non-Overlapping Temp
9	5	17	8	9	15	10	7	12	8	0.20227	100/100	Non-Overlapping Temp
10	9	7	11	10	7	13	13	9	11	0.91141	98/100	Non-Overlapping Temp
10	8	11	12	10	13	7	10	10	9	0.97170	98/100	Non-Overlapping Temp
14	9	7	12	12	7	8	13	9	9	0.75976	100/100	Non-Overlapping Temp
14	8	6	7	5	11	10	11	9	19	0.08052	100/100	Non-Overlapping Temp
9	10	13	10	16	8	8	7	10	9	0.69931	100/100	Non-Overlapping Temp
8	10	10	9	11	14	10	7	10	11	0.95584	100/100	Non-Overlapping Temp
10	13	11	13	11	5	5	10	10	12	0.59555	100/100	Non-Overlapping Temp
11	7	15	14	5	8	10	11	14	5	0.20227	100/100	Non-Overlapping Temp
14	16	8	6	9	10	9	9	12	7	0.45594	99/100	Non-Overlapping Temp
11	14	11	10	6	6	7	13	12	10	0.61631	99/100	Non-Overlapping Temp
12	7	15	10	5	16	11	5	12	7	0.12962	99/100	Non-Overlapping Temp
13	6	16	12	12	14	7	5	10	5	0.10879	100/100	Non-Overlapping Temp
11	10	8	7	14	9	10	12	9	10	0.93572	100/100	Non-Overlapping Temp
10	9	13	9	8	8	9	16	8	10	0.73992	100/100	Non-Overlapping Temp
10	8	9	5	13	10	13	12	10	10	0.81654	99/100	Non-Overlapping Temp
4	9	7	9	13	17	15	11	7	8	0.10879	98/100	Non-Overlapping Temp
14	11	10	9	12	8	7	12	6	11	0.77919	98/100	Non-Overlapping Temp
7	11	11	4	12	13	11	14	10	7	0.47499	100/100	Non-Overlapping Temp
12	7	9	13	6	12	10	12	9	10	0.85138	99/100	Non-Overlapping Temp
9	10	8	9	12	15	3	13	13	8	0.30413	98/100	Non-Overlapping Temp
14	11	7	11	7	9	6	8	12	15	0.47499	100/100	Non-Overlapping Temp
11	13	6	5	13	11	12	7	14	8	0.40120	98/100	Non-Overlapping Temp
5	8	15	6	14	7	11	8	10	16	0.13728	99/100	Non-Overlapping Temp
13	10	8	10	10	11	11	4	7	16	0.38383	100/100	Non-Overlapping Temp
9	13	12	10	10	10	9	10	13	4	0.73992	100/100	Non-Overlapping Temp
6	14	11	7	9	11	9	10	14	9	0.71975	99/100	Non-Overlapping Temp
8	12	12	6	5	13	18	9	8	9	0.15376	99/100	Non-Overlapping Temp
12	5	13	9	16	15	10	6	9	5	0.11539	98/100	Non-Overlapping Temp
8	12	11	10	12	9	12	10	6	10	0.94631	99/100	Non-Overlapping Temp
9	12	8	13	12	7	7	8	11	13	0.79814	98/100	Non-Overlapping Temp
12	8	10	9	6	15	11	9	12	8	0.73992	99/100	Non-Overlapping Temp
11	11	11	6	8	7	10	12	11	13	0.86769	100/100	Non-Overlapping Temp

11	8	13	3	10	10	10	7	18	10	0.13728	100/100	Non-Overlapping Temp
4	19	9	12	6	8	12	5	11	14	0.02695	100/100	Non-Overlapping Temp
10	9	7	12	5	11	9	13	15	9	0.57490	99/100	Non-Overlapping Temp
9	16	10	8	8	11	10	11	7	10	0.77919	99/100	Non-Overlapping Temp
11	9	6	9	11	11	6	14	11	12	0.75976	100/100	Non-Overlapping Temp
7	17	9	5	9	9	11	9	12	12	0.38383	98/100	Non-Overlapping Temp
13	11	12	11	9	9	9	10	5	11	0.88317	99/100	Non-Overlapping Temp
12	12	7	13	8	8	11	10	8	11	0.91141	100/100	Non-Overlapping Temp
11	3	14	8	18	7	14	10	6	9	0.04011	99/100	Non-Overlapping Temp
8	7	10	8	10	16	9	13	10	9	0.69931	99/100	Non-Overlapping Temp
11	6	8	7	13	15	14	10	11	5	0.30413	100/100	Non-Overlapping Temp
6	13	10	9	10	7	12	15	11	7	0.59555	100/100	Non-Overlapping Temp
10	7	7	11	11	10	16	11	8	9	0.71975	98/100	Non-Overlapping Temp
7	13	14	9	12	13	6	10	10	6	0.53415	99/100	Non-Overlapping Temp
9	9	14	5	14	9	8	10	7	15	0.36692	99/100	Non-Overlapping Temp
14	10	8	12	9	8	10	10	13	6	0.79814	100/100	Non-Overlapping Temp
10	9	13	11	10	12	8	9	11	7	0.96430	99/100	Non-Overlapping Temp
7	11	13	9	15	8	9	12	11	5	0.53415	98/100	Non-Overlapping Temp
10	11	5	9	11	16	9	10	7	12	0.55442	99/100	Overlapping Temp
18	13	8	7	7	6	7	11	14	9	0.12962	99/100	Maurer’s Universal
13	11	12	8	8	18	4	6	11	9	0.12233	98/100	Approximate Entropy
8	8	9	3	9	6	5	6	8	3	0.51744	64/65	Random Excursions
7	5	9	6	5	4	7	9	6	7	0.87554	65/65	Random Excursions
4	9	9	10	9	5	4	5	6	4	0.39246	65/65	Random Excursions
3	7	15	4	5	5	10	4	5	7	0.01897	64/65	Random Excursions
10	6	5	11	6	3	6	8	6	4	0.36415	65/65	Random Excursions
4	3	8	4	8	10	5	5	12	6	0.15521	64/65	Random Excursions
5	9	7	7	7	6	4	6	7	7	0.95732	63/65	Random Excursions
4	9	7	7	8	9	5	3	7	6	0.68902	64/65	Random Excursions
8	3	5	5	4	9	8	13	7	3	0.08646	65/65	Random Excursions V
5	7	3	5	5	8	11	7	9	5	0.45280	64/65	Random Excursions V
5	7	2	5	9	7	8	10	8	4	0.39246	64/65	Random Excursions V
5	9	2	7	5	8	5	7	4	13	0.10562	64/65	Random Excursions V
7	5	3	9	4	5	7	5	9	11	0.33716	64/65	Random Excursions V
7	5	7	2	6	10	7	7	6	8	0.65447	64/65	Random Excursions V
10	5	7	2	7	8	6	5	6	9	0.51744	64/65	Random Excursions V
7	9	2	6	9	8	7	5	5	7	0.61977	65/65	Random Excursions V
7	8	5	5	2	6	10	9	8	5	0.45280	65/65	Random Excursions V
5	3	10	7	6	8	4	10	7	5	0.45280	64/65	Random Excursions V
4	8	4	8	7	7	4	9	7	7	0.78873	65/65	Random Excursions V
5	8	10	1	6	5	9	7	7	7	0.36415	65/65	Random Excursions V
7	5	8	6	4	3	9	7	8	8	0.72313	64/65	Random Excursions V
7	5	7	3	8	9	11	5	7	3	0.33716	65/65	Random Excursions V
7	5	8	7	5	8	3	11	7	4	0.48465	65/65	Random Excursions V
6	8	9	3	5	5	8	7	8	6	0.78873	65/65	Random Excursions V
4	9	6	4	9	7	4	10	5	7	0.51744	65/65	Random Excursions V
6	7	3	5	7	8	6	4	8	11	0.51744	65/65	Random Excursions V
9	13	7	9	10	13	9	7	12	11	0.88317	98/100	Serial
11	6	10	9	9	14	9	8	13	11	0.83431	100/100	Serial
11	12	15	9	4	6	11	9	12	11	0.43727	99/100	Linear Complexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 61 for a sample size = 65 binary sequences.

Πίνακας ΙΙ.4: Αναλυτικός πίνακας αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα unpredictability128_n8.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη.

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\unpredictability128_n8.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
9	13	10	9	9	13	11	6	9	11	0.91141	99/100	Frequency
11	10	8	15	13	7	9	8	11	8	0.75976	100/100	Block Frequency
10	9	12	10	8	6	14	10	11	10	0.89776	99/100	Cumulative Sums
6	7	11	11	12	8	12	9	15	9	0.67869	99/100	Cumulative Sums
10	11	9	11	8	11	11	9	11	9	0.99882	100/100	Runs
9	11	5	12	8	16	13	9	9	8	0.47499	100/100	Longest Run
10	12	12	14	13	5	9	8	11	6	0.53415	100/100	Rank
15	12	11	6	15	7	8	9	7	10	0.40120	97/100	DFT
10	9	13	10	12	8	11	10	6	11	0.93572	99/100	Non-Overlapping Temp
7	8	8	9	10	9	13	11	13	12	0.89776	100/100	Non-Overlapping Temp
7	14	8	15	8	7	11	11	10	9	0.63712	99/100	Non-Overlapping Temp
7	8	12	7	19	13	6	7	7	14	0.05536	100/100	Non-Overlapping Temp
8	9	14	13	7	8	12	11	7	11	0.75976	99/100	Non-Overlapping Temp
12	8	12	16	9	10	12	5	8	8	0.47499	97/100	Non-Overlapping Temp
9	14	7	11	7	11	12	6	8	15	0.47499	100/100	Non-Overlapping Temp
10	9	11	9	8	9	8	12	12	12	0.98345	99/100	Non-Overlapping Temp
13	9	10	12	8	14	8	9	10	7	0.85138	99/100	Non-Overlapping Temp
9	10	14	8	14	9	11	8	5	12	0.61631	99/100	Non-Overlapping Temp
6	10	8	14	9	8	10	10	14	11	0.75976	100/100	Non-Overlapping Temp
12	13	7	6	7	10	11	12	5	17	0.18156	99/100	Non-Overlapping Temp
10	11	7	14	9	11	8	9	9	12	0.92408	100/100	Non-Overlapping Temp
9	9	3	13	8	8	16	13	6	15	0.08052	98/100	Non-Overlapping Temp
6	13	8	11	8	7	11	15	12	9	0.59555	99/100	Non-Overlapping Temp
12	8	8	12	10	13	12	9	5	11	0.77919	98/100	Non-Overlapping Temp
14	5	21	14	7	9	6	8	6	10	0.00769	99/100	Non-Overlapping Temp
11	5	5	10	13	9	12	14	11	10	0.51412	99/100	Non-Overlapping Temp
8	9	10	10	11	13	10	11	10	8	0.99147	100/100	Non-Overlapping Temp
8	12	9	13	11	9	11	7	9	11	0.95584	99/100	Non-Overlapping Temp
14	10	6	4	7	14	11	13	10	11	0.31908	99/100	Non-Overlapping Temp
9	13	13	9	11	3	15	9	9	9	0.36692	96/100	Non-Overlapping Temp
11	10	10	10	14	7	14	7	7	10	0.73992	98/100	Non-Overlapping Temp
16	8	10	6	4	11	11	10	8	16	0.14533	97/100	Non-Overlapping Temp
10	11	15	9	11	7	10	7	16	4	0.22482	100/100	Non-Overlapping Temp
13	9	8	4	10	11	9	16	7	13	0.30413	100/100	Non-Overlapping Temp
8	12	21	4	6	14	12	9	8	6	0.00827	99/100	Non-Overlapping Temp
8	9	13	13	7	11	10	8	6	15	0.55442	100/100	Non-Overlapping Temp
10	8	13	8	10	8	8	13	16	6	0.47499	99/100	Non-Overlapping Temp
11	10	12	11	9	6	7	10	11	13	0.89776	100/100	Non-Overlapping Temp
12	14	12	7	14	10	4	11	9	7	0.38383	99/100	Non-Overlapping Temp
6	9	6	10	12	12	7	18	12	8	0.20227	99/100	Non-Overlapping Temp
10	5	12	14	12	8	7	14	8	10	0.51412	99/100	Non-Overlapping Temp
8	9	12	11	8	10	14	9	10	9	0.95584	99/100	Non-Overlapping Temp
13	7	12	10	9	10	10	7	9	13	0.89776	100/100	Non-Overlapping Temp
14	7	9	10	10	11	6	8	6	19	0.10879	99/100	Non-Overlapping Temp
9	5	10	14	10	13	7	14	7	11	0.47499	97/100	Non-Overlapping Temp
9	7	15	8	16	9	6	14	6	10	0.19169	99/100	Non-Overlapping Temp
9	8	6	7	15	7	16	12	11	9	0.30413	99/100	Non-Overlapping Temp
8	10	14	10	10	8	10	9	11	10	0.97807	98/100	Non-Overlapping Temp
11	9	13	6	11	10	9	12	9	10	0.94631	97/100	Non-Overlapping Temp
8	9	12	10	7	9	13	9	13	10	0.92408	100/100	Non-Overlapping Temp
5	9	8	9	11	10	8	13	13	14	0.63712	100/100	Non-Overlapping Temp
8	7	11	17	14	13	5	11	6	8	0.14533	98/100	Non-Overlapping Temp
16	2	7	13	9	13	11	12	10	7	0.11539	99/100	Non-Overlapping Temp
9	6	7	11	14	8	8	14	13	10	0.57490	99/100	Non-Overlapping Temp
16	7	6	14	10	5	8	9	16	9	0.10879	99/100	Non-Overlapping Temp
7	10	10	12	11	10	6	13	8	13	0.81654	100/100	Non-Overlapping Temp
12	8	6	13	15	11	6	11	9	9	0.55442	100/100	Non-Overlapping Temp
10	11	8	8	8	3	17	9	16	10	0.09658	99/100	Non-Overlapping Temp

4	10	10	12	10	11	14	15	7	7	0.35049	100/100	Non-Overlapping Temp
9	7	11	7	15	9	6	11	13	12	0.57490	100/100	Non-Overlapping Temp
12	8	7	7	6	16	12	12	9	11	0.45594	99/100	Non-Overlapping Temp
13	16	8	12	9	9	9	9	9	6	0.59555	99/100	Non-Overlapping Temp
13	10	9	15	4	8	13	12	7	9	0.36692	99/100	Non-Overlapping Temp
8	7	8	15	9	11	9	10	12	11	0.83431	99/100	Non-Overlapping Temp
7	10	9	16	11	8	8	8	12	11	0.69931	100/100	Non-Overlapping Temp
11	10	13	9	10	11	8	13	7	8	0.92408	100/100	Non-Overlapping Temp
10	10	7	9	12	16	9	6	8	13	0.53415	100/100	Non-Overlapping Temp
11	13	4	14	10	8	9	11	9	11	0.63712	97/100	Non-Overlapping Temp
7	5	11	14	10	12	14	8	16	3	0.06688	97/100	Non-Overlapping Temp
9	11	7	9	7	13	13	10	10	11	0.91141	98/100	Non-Overlapping Temp
8	8	13	9	6	12	10	13	15	6	0.45594	97/100	Non-Overlapping Temp
12	7	11	12	14	4	11	10	8	11	0.57490	99/100	Non-Overlapping Temp
10	7	8	7	6	12	14	16	10	10	0.40120	100/100	Non-Overlapping Temp
9	10	7	8	8	14	17	11	9	7	0.40120	100/100	Non-Overlapping Temp
12	8	15	11	8	10	13	9	7	7	0.67869	99/100	Non-Overlapping Temp
8	9	13	12	7	11	8	10	15	7	0.67869	99/100	Non-Overlapping Temp
6	6	15	8	11	11	10	13	12	8	0.53415	98/100	Non-Overlapping Temp
4	12	10	11	10	12	8	14	10	9	0.67869	100/100	Non-Overlapping Temp
11	3	12	15	12	7	12	12	5	11	0.18156	99/100	Non-Overlapping Temp
8	13	12	14	5	5	12	10	13	8	0.35049	100/100	Non-Overlapping Temp
9	9	14	12	14	10	4	6	10	12	0.40120	100/100	Non-Overlapping Temp
3	12	8	11	15	4	8	10	16	13	0.05194	100/100	Non-Overlapping Temp
10	9	13	10	12	8	11	10	6	11	0.93572	99/100	Non-Overlapping Temp
8	12	6	10	12	15	11	10	5	11	0.53415	100/100	Non-Overlapping Temp
9	13	10	10	10	11	11	5	11	10	0.92408	99/100	Non-Overlapping Temp
8	10	9	5	9	15	9	11	16	8	0.36692	100/100	Non-Overlapping Temp
10	12	6	10	13	5	15	8	13	8	0.38383	97/100	Non-Overlapping Temp
7	10	12	11	10	7	13	10	12	8	0.91141	99/100	Non-Overlapping Temp
13	11	12	10	10	5	8	8	9	14	0.69931	100/100	Non-Overlapping Temp
6	7	10	9	15	11	12	9	10	11	0.75976	98/100	Non-Overlapping Temp
12	14	5	16	7	13	9	6	10	8	0.21331	98/100	Non-Overlapping Temp
8	10	12	15	8	11	9	6	12	9	0.73992	98/100	Non-Overlapping Temp
11	7	13	13	10	11	11	8	6	10	0.83431	99/100	Non-Overlapping Temp
9	11	13	13	8	7	18	8	6	7	0.18156	100/100	Non-Overlapping Temp
11	8	14	7	10	8	11	13	10	8	0.85138	100/100	Non-Overlapping Temp
9	13	14	7	9	11	6	8	8	15	0.47499	100/100	Non-Overlapping Temp
12	10	18	13	11	5	13	5	5	8	0.05536	98/100	Non-Overlapping Temp
6	8	10	10	11	11	7	9	17	11	0.51412	99/100	Non-Overlapping Temp
11	6	9	2	14	14	12	14	9	9	0.13728	99/100	Non-Overlapping Temp
8	5	9	13	13	7	13	13	12	7	0.45594	100/100	Non-Overlapping Temp
9	12	12	14	8	12	7	10	8	8	0.83431	99/100	Non-Overlapping Temp
17	14	7	9	11	8	8	8	11	7	0.36692	96/100	Non-Overlapping Temp
8	11	10	9	12	15	7	10	6	12	0.69931	98/100	Non-Overlapping Temp
11	14	11	4	6	9	15	14	10	6	0.17187	100/100	Non-Overlapping Temp
9	11	7	9	11	8	9	6	16	14	0.47499	100/100	Non-Overlapping Temp
11	13	9	15	10	5	4	6	15	12	0.11539	98/100	Non-Overlapping Temp
8	15	10	8	9	12	7	14	6	11	0.53415	98/100	Non-Overlapping Temp
12	9	10	14	7	13	6	10	12	7	0.65793	99/100	Non-Overlapping Temp
11	9	7	12	8	13	11	9	11	9	0.95584	100/100	Non-Overlapping Temp
8	4	8	10	19	6	11	12	10	12	0.09094	100/100	Non-Overlapping Temp
12	6	6	12	10	10	11	12	11	10	0.86769	99/100	Non-Overlapping Temp
12	10	5	11	8	12	14	6	14	8	0.43727	100/100	Non-Overlapping Temp
17	11	8	14	6	11	4	5	12	12	0.07572	98/100	Non-Overlapping Temp
9	16	10	13	11	5	7	10	10	9	0.51412	100/100	Non-Overlapping Temp
10	8	17	11	11	7	7	13	4	12	0.20227	98/100	Non-Overlapping Temp
10	7	7	12	16	12	8	8	10	10	0.63712	99/100	Non-Overlapping Temp
9	13	8	7	6	12	13	8	12	12	0.69931	99/100	Non-Overlapping Temp
16	13	10	8	5	7	12	10	10	9	0.45594	99/100	Non-Overlapping Temp
10	9	6	12	14	16	9	6	10	8	0.40120	98/100	Non-Overlapping Temp
12	10	6	7	9	8	12	13	13	10	0.77919	100/100	Non-Overlapping Temp

7	12	14	12	12	10	8	8	7	10	0.79814	100/100	Non-Overlapping Temp
12	6	10	5	8	12	15	11	13	8	0.41902	98/100	Non-Overlapping Temp
6	14	5	9	15	6	12	14	10	9	0.21331	99/100	Non-Overlapping Temp
11	8	8	9	12	16	10	11	8	7	0.69931	98/100	Non-Overlapping Temp
17	8	13	8	8	12	10	7	7	10	0.41902	99/100	Non-Overlapping Temp
12	8	9	13	10	6	10	9	12	11	0.91141	98/100	Non-Overlapping Temp
12	8	13	6	15	12	9	6	8	11	0.49439	98/100	Non-Overlapping Temp
15	10	7	9	7	14	11	10	6	11	0.55442	100/100	Non-Overlapping Temp
9	11	7	10	6	10	11	11	12	13	0.89776	100/100	Non-Overlapping Temp
9	7	14	17	14	8	6	8	5	12	0.10879	98/100	Non-Overlapping Temp
9	8	10	11	15	10	6	6	10	15	0.45594	99/100	Non-Overlapping Temp
11	9	10	15	5	9	11	12	8	10	0.71975	100/100	Non-Overlapping Temp
10	7	10	12	11	12	16	6	5	11	0.38383	99/100	Non-Overlapping Temp
15	10	8	12	9	9	7	9	14	7	0.63712	99/100	Non-Overlapping Temp
9	11	12	11	7	13	4	10	9	14	0.55442	100/100	Non-Overlapping Temp
10	8	13	9	12	6	14	11	8	9	0.77919	99/100	Non-Overlapping Temp
5	13	10	10	10	7	10	12	11	12	0.81654	100/100	Non-Overlapping Temp
7	11	14	11	6	12	8	7	14	10	0.57490	100/100	Non-Overlapping Temp
10	7	13	6	10	10	7	13	11	13	0.71975	100/100	Non-Overlapping Temp
12	7	9	13	13	7	10	14	6	9	0.59555	99/100	Non-Overlapping Temp
11	12	10	10	8	9	10	9	8	13	0.98345	100/100	Non-Overlapping Temp
4	10	11	4	10	17	12	11	12	9	0.15376	100/100	Non-Overlapping Temp
6	12	14	15	7	9	5	8	11	13	0.27571	100/100	Non-Overlapping Temp
8	10	12	18	8	14	9	6	9	6	0.18156	98/100	Non-Overlapping Temp
11	5	16	7	12	9	9	12	11	8	0.47499	98/100	Non-Overlapping Temp
5	10	10	8	15	15	8	9	9	11	0.47499	100/100	Non-Overlapping Temp
8	10	11	7	9	7	9	12	9	18	0.40120	99/100	Non-Overlapping Temp
15	13	13	12	10	12	9	9	5	2	0.11539	99/100	Non-Overlapping Temp
8	6	11	10	19	9	12	9	7	9	0.22482	99/100	Non-Overlapping Temp
12	9	12	9	9	15	12	7	9	6	0.67869	100/100	Non-Overlapping Temp
9	8	14	7	12	10	9	12	5	14	0.53415	98/100	Non-Overlapping Temp
12	9	11	9	11	12	8	12	6	10	0.93572	99/100	Non-Overlapping Temp
12	12	9	6	5	11	13	14	10	8	0.53415	100/100	Non-Overlapping Temp
10	13	14	12	3	10	10	9	12	7	0.41902	97/100	Non-Overlapping Temp
13	5	15	8	11	15	5	10	11	7	0.19169	99/100	Non-Overlapping Temp
3	12	8	11	14	5	8	10	16	13	0.09658	100/100	Non-Overlapping Temp
13	9	10	7	8	9	9	16	8	11	0.67869	98/100	Overlapping Temp
14	13	8	11	12	7	11	6	8	10	0.69931	99/100	Maurer’s Universal
13	11	5	11	8	18	4	12	11	7	0.08052	100/100	Approximate Entropy
5	5	6	0	8	6	10	6	8	6	0.32418	60/60	Random Excursions
7	3	6	6	6	4	3	5	10	10	0.40709	60/60	Random Excursions
0	5	4	10	7	7	7	8	4	8	0.21331	60/60	Random Excursions
2	5	7	8	7	10	6	3	4	8	0.40709	60/60	Random Excursions
2	4	7	7	4	10	7	6	6	7	0.60246	60/60	Random Excursions
2	8	7	11	5	11	2	4	6	4	0.06688	60/60	Random Excursions
3	5	4	13	7	4	4	5	7	8	0.16261	60/60	Random Excursions
6	8	10	5	6	8	6	7	1	3	0.35049	60/60	Random Excursions
5	3	8	9	5	7	8	6	5	4	0.77276	60/60	Random Excursions V
5	6	7	4	9	7	8	4	4	6	0.86234	60/60	Random Excursions V
5	7	4	5	8	5	6	8	6	6	0.97606	60/60	Random Excursions V
5	3	7	6	8	1	6	12	7	5	0.16261	59/60	Random Excursions V
7	1	7	7	8	2	5	7	3	13	0.03517	59/60	Random Excursions V
4	5	4	7	7	5	8	6	6	8	0.94960	59/60	Random Excursions V
5	6	3	6	6	5	4	10	5	10	0.53415	60/60	Random Excursions V
6	6	4	5	5	6	7	7	6	8	0.99147	60/60	Random Excursions V
5	4	11	5	5	11	5	2	8	4	0.13469	60/60	Random Excursions V
7	2	5	8	10	5	7	6	3	7	0.50093	59/60	Random Excursions V
6	7	9	2	9	7	5	4	7	4	0.56806	60/60	Random Excursions V
5	4	2	5	9	7	6	5	8	9	0.56806	60/60	Random Excursions V
5	2	5	5	6	4	5	11	7	10	0.27571	60/60	Random Excursions V
4	5	5	5	5	3	6	8	6	13	0.23276	60/60	Random Excursions V
4	4	6	4	9	6	5	6	8	8	0.83431	60/60	Random Excursions V

5	2	5	10	7	6	9	6	3	7	0.43727	60/60	Random Excursions V
5	3	6	7	6	6	6	7	9	5	0.93195	60/60	Random Excursions V
4	4	9	4	5	7	9	8	7	3	0.56806	60/60	Random Excursions V
14	9	9	12	12	10	10	10	9	5	0.81654	100/100	Serial
11	11	15	9	10	10	11	7	7	9	0.85138	99/100	Serial
8	11	11	8	7	10	9	16	11	9	0.75976	98/100	Linear Complexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 57 for a sample size = 60 binary sequences.

Πίνακας II.5: Αναλυτικός πίνακας αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα unpredictability128_n16.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\unpredictability128_n16.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
6	16	10	14	9	6	8	12	13	6	0.22482	100/100	Frequency
9	6	9	9	13	12	7	14	12	9	0.71975	99/100	Block Frequency
8	8	9	14	13	8	10	12	10	8	0.86769	100/100	Cumulative Sums
7	10	14	13	10	13	8	10	7	8	0.73992	100/100	Cumulative Sums
12	11	7	11	6	8	15	11	13	6	0.47499	98/100	Runs
10	5	10	12	10	13	9	10	9	12	0.88317	99/100	Longest Run
8	10	12	9	8	9	16	9	9	10	0.81654	100/100	Rank
14	10	16	7	13	9	8	6	10	7	0.35049	99/100	DFT
9	6	10	14	11	5	10	9	15	11	0.47499	99/100	Non-Overlapping Temp
12	13	14	9	10	8	8	11	7	8	0.81654	97/100	Non-Overlapping Temp
10	7	11	8	14	5	14	11	8	12	0.53415	100/100	Non-Overlapping Temp
14	9	6	8	10	10	9	9	11	14	0.77919	99/100	Non-Overlapping Temp
6	9	9	13	10	11	13	9	11	9	0.91141	100/100	Non-Overlapping Temp
11	10	12	7	10	12	6	10	8	14	0.79814	100/100	Non-Overlapping Temp
12	7	11	10	9	10	11	10	13	7	0.94631	100/100	Non-Overlapping Temp
15	12	15	8	9	4	10	11	8	8	0.31908	99/100	Non-Overlapping Temp
11	8	8	12	13	11	9	10	12	6	0.88317	98/100	Non-Overlapping Temp
9	9	8	17	11	7	7	17	7	8	0.13728	100/100	Non-Overlapping Temp
10	11	8	8	13	10	8	12	14	6	0.75976	100/100	Non-Overlapping Temp
9	17	4	7	14	8	13	6	14	8	0.06688	100/100	Non-Overlapping Temp
11	13	9	13	7	10	9	10	8	10	0.94631	99/100	Non-Overlapping Temp
7	11	17	10	9	9	9	12	5	11	0.41902	99/100	Non-Overlapping Temp
11	10	9	9	10	9	12	5	11	14	0.83431	100/100	Non-Overlapping Temp
9	10	11	11	10	8	12	10	7	12	0.98345	99/100	Non-Overlapping Temp
10	17	9	6	10	8	10	12	12	6	0.40120	99/100	Non-Overlapping Temp
13	8	14	14	8	12	6	8	6	11	0.43727	99/100	Non-Overlapping Temp
11	9	10	8	7	16	7	10	11	11	0.71975	100/100	Non-Overlapping Temp
9	12	13	10	4	9	13	8	11	11	0.67869	99/100	Non-Overlapping Temp
8	9	14	10	11	13	10	12	8	5	0.69931	99/100	Non-Overlapping Temp
9	11	8	16	5	12	14	8	8	9	0.38383	98/100	Non-Overlapping Temp
11	10	5	7	7	11	13	12	13	11	0.65793	99/100	Non-Overlapping Temp
16	10	8	12	10	10	10	5	10	9	0.63712	99/100	Non-Overlapping Temp
7	14	11	17	9	9	5	8	11	9	0.28967	100/100	Non-Overlapping Temp
5	8	9	11	8	12	13	12	6	16	0.31908	99/100	Non-Overlapping Temp
8	8	11	8	10	16	9	11	11	8	0.77919	99/100	Non-Overlapping Temp
10	12	12	6	13	7	13	9	8	10	0.77919	98/100	Non-Overlapping Temp
13	6	10	13	10	8	16	12	7	5	0.26225	99/100	Non-Overlapping Temp
6	11	9	10	4	10	14	18	14	4	0.02882	100/100	Non-Overlapping Temp
10	16	10	6	8	15	9	17	5	4	0.02355	99/100	Non-Overlapping Temp
6	8	11	11	7	7	8	14	11	17	0.27571	98/100	Non-Overlapping Temp
10	9	8	13	10	6	15	11	9	9	0.75976	97/100	Non-Overlapping Temp

10	9	6	11	10	6	14	12	12	10	0.75976	100/100	Non-Overlapping Temp
14	6	5	5	9	13	12	17	6	13	0.04872	98/100	Non-Overlapping Temp
7	5	12	8	8	12	10	12	15	11	0.53415	100/100	Non-Overlapping Temp
5	6	11	13	12	9	9	14	12	9	0.55442	99/100	Non-Overlapping Temp
9	10	10	9	10	9	17	12	6	8	0.57490	98/100	Non-Overlapping Temp
11	11	10	11	11	7	11	11	10	7	0.98345	99/100	Non-Overlapping Temp
7	11	10	8	18	12	10	6	8	10	0.33454	99/100	Non-Overlapping Temp
6	15	7	8	16	11	7	4	13	13	0.08052	100/100	Non-Overlapping Temp
11	12	8	8	8	8	14	10	11	10	0.92408	99/100	Non-Overlapping Temp
13	7	10	16	10	7	9	9	10	9	0.67869	99/100	Non-Overlapping Temp
14	13	8	12	8	12	5	12	9	7	0.53415	99/100	Non-Overlapping Temp
10	8	11	5	16	10	8	15	9	8	0.35049	98/100	Non-Overlapping Temp
9	7	7	8	15	8	6	13	9	18	0.11539	99/100	Non-Overlapping Temp
9	10	5	9	13	8	10	10	12	14	0.73992	97/100	Non-Overlapping Temp
13	14	10	9	10	5	8	11	9	11	0.75976	99/100	Non-Overlapping Temp
10	10	14	9	8	8	12	9	7	13	0.85138	99/100	Non-Overlapping Temp
8	10	10	9	13	8	16	10	7	9	0.69931	100/100	Non-Overlapping Temp
8	14	14	13	7	12	4	8	14	6	0.16261	99/100	Non-Overlapping Temp
10	10	10	9	12	6	11	17	7	8	0.49439	98/100	Non-Overlapping Temp
8	11	14	13	8	11	11	12	6	6	0.61631	100/100	Non-Overlapping Temp
13	7	11	10	12	8	7	16	10	6	0.45594	98/100	Non-Overlapping Temp
10	5	15	7	8	9	10	12	16	8	0.28967	100/100	Non-Overlapping Temp
7	11	7	13	12	9	8	10	13	10	0.86769	100/100	Non-Overlapping Temp
7	9	5	15	13	7	8	15	9	12	0.26225	100/100	Non-Overlapping Temp
9	10	9	10	10	11	13	16	8	4	0.45594	100/100	Non-Overlapping Temp
7	13	14	8	6	9	11	12	10	10	0.73992	99/100	Non-Overlapping Temp
9	4	6	11	8	9	12	12	12	17	0.21331	97/100	Non-Overlapping Temp
7	16	11	8	10	11	12	12	8	5	0.45594	100/100	Non-Overlapping Temp
11	9	8	16	13	9	6	9	10	9	0.63712	99/100	Non-Overlapping Temp
9	8	9	9	12	11	14	12	9	7	0.89776	100/100	Non-Overlapping Temp
20	6	10	9	9	7	6	10	16	7	0.02695	96/100	Non-Overlapping Temp
9	9	7	16	6	10	7	11	14	11	0.43727	98/100	Non-Overlapping Temp
8	10	12	9	12	10	7	14	7	11	0.85138	100/100	Non-Overlapping Temp
6	16	10	11	10	10	8	9	10	10	0.75976	100/100	Non-Overlapping Temp
10	13	10	9	9	10	8	8	11	12	0.98345	99/100	Non-Overlapping Temp
14	4	11	7	10	16	9	7	11	11	0.27571	99/100	Non-Overlapping Temp
11	10	5	10	6	8	10	15	13	12	0.49439	97/100	Non-Overlapping Temp
7	13	5	11	7	15	10	8	13	11	0.41902	99/100	Non-Overlapping Temp
10	6	17	14	11	11	11	9	6	5	0.18156	98/100	Non-Overlapping Temp
9	10	6	16	9	10	6	7	8	19	0.05898	98/100	Non-Overlapping Temp
8	6	9	9	12	9	8	16	10	13	0.57490	100/100	Non-Overlapping Temp
9	6	10	14	11	5	10	9	15	11	0.47499	99/100	Non-Overlapping Temp
12	9	8	12	7	16	11	8	7	10	0.61631	100/100	Non-Overlapping Temp
14	9	7	11	10	4	8	7	13	17	0.14533	98/100	Non-Overlapping Temp
12	15	7	8	12	8	9	11	9	9	0.79814	96/100	Non-Overlapping Temp
11	7	7	13	15	14	15	5	7	6	0.10879	99/100	Non-Overlapping Temp
11	10	13	8	10	13	13	3	14	5	0.20227	99/100	Non-Overlapping Temp
10	13	7	6	10	12	15	10	8	9	0.65793	98/100	Non-Overlapping Temp
12	11	12	12	6	9	5	12	8	13	0.61631	98/100	Non-Overlapping Temp
14	12	8	9	15	5	12	11	6	8	0.35049	98/100	Non-Overlapping Temp
7	11	13	5	3	14	10	12	14	11	0.16261	100/100	Non-Overlapping Temp
7	12	12	6	10	10	15	9	10	9	0.73992	99/100	Non-Overlapping Temp
10	5	6	10	9	11	13	6	17	13	0.18156	100/100	Non-Overlapping Temp
11	16	8	10	4	13	8	9	10	11	0.41902	99/100	Non-Overlapping Temp
10	8	4	10	16	9	9	11	11	12	0.49439	100/100	Non-Overlapping Temp
20	11	12	12	4	8	4	13	3	13	0.00276	98/100	Non-Overlapping Temp
13	6	13	14	4	10	9	8	15	8	0.21331	98/100	Non-Overlapping Temp
11	11	10	7	6	15	10	12	10	8	0.73992	100/100	Non-Overlapping Temp
10	18	9	7	9	12	11	6	9	9	0.36692	99/100	Non-Overlapping Temp
8	13	13	12	12	6	8	3	14	11	0.23681	99/100	Non-Overlapping Temp
10	15	10	11	5	9	8	9	11	12	0.71975	100/100	Non-Overlapping Temp
13	14	7	7	12	7	7	10	14	9	0.51412	99/100	Non-Overlapping Temp

12	8	11	11	11	8	12	4	12	11	0.73992	100/100	Non-Overlapping Temp
9	8	8	8	14	10	15	12	9	7	0.65793	100/100	Non-Overlapping Temp
12	11	7	8	8	14	7	6	15	12	0.41902	98/100	Non-Overlapping Temp
6	8	13	7	6	10	12	13	12	13	0.53415	99/100	Non-Overlapping Temp
12	9	11	6	12	11	11	10	9	9	0.96430	100/100	Non-Overlapping Temp
11	11	9	9	9	11	10	6	12	12	0.96430	99/100	Non-Overlapping Temp
13	16	6	12	11	9	7	11	6	9	0.40120	100/100	Non-Overlapping Temp
11	11	10	8	7	10	13	10	8	12	0.95584	98/100	Non-Overlapping Temp
11	8	6	3	9	14	13	11	15	10	0.20227	100/100	Non-Overlapping Temp
15	10	10	11	17	6	4	11	9	7	0.12962	100/100	Non-Overlapping Temp
10	8	8	11	8	7	13	16	9	10	0.65793	100/100	Non-Overlapping Temp
9	11	11	6	13	5	11	10	14	10	0.63712	99/100	Non-Overlapping Temp
11	10	7	10	10	8	12	10	13	9	0.97170	97/100	Non-Overlapping Temp
5	9	11	14	10	14	8	7	12	10	0.57490	100/100	Non-Overlapping Temp
8	11	13	10	10	10	9	9	9	11	0.99425	99/100	Non-Overlapping Temp
10	15	4	10	10	12	6	7	12	14	0.27571	100/100	Non-Overlapping Temp
12	5	8	15	7	12	17	10	8	6	0.12233	99/100	Non-Overlapping Temp
17	12	6	9	7	12	12	8	9	8	0.38383	100/100	Non-Overlapping Temp
10	12	9	10	14	9	6	10	10	10	0.92408	98/100	Non-Overlapping Temp
9	13	10	8	9	13	12	13	7	6	0.71975	98/100	Non-Overlapping Temp
9	8	14	9	11	16	13	7	5	8	0.30413	100/100	Non-Overlapping Temp
11	11	15	9	10	8	12	13	7	4	0.43727	99/100	Non-Overlapping Temp
16	10	10	8	11	8	8	12	10	7	0.71975	99/100	Non-Overlapping Temp
10	13	10	9	8	17	6	9	11	7	0.43727	100/100	Non-Overlapping Temp
9	6	11	10	12	14	11	11	7	9	0.83431	98/100	Non-Overlapping Temp
6	14	8	8	11	16	10	8	12	7	0.40120	100/100	Non-Overlapping Temp
9	13	7	5	9	10	11	7	17	12	0.28967	99/100	Non-Overlapping Temp
11	9	8	14	10	14	14	6	3	11	0.21331	100/100	Non-Overlapping Temp
6	10	17	9	6	10	15	10	7	10	0.23681	99/100	Non-Overlapping Temp
5	13	9	16	10	13	9	9	6	10	0.36692	100/100	Non-Overlapping Temp
19	8	9	8	11	7	8	11	6	13	0.16261	97/100	Non-Overlapping Temp
12	10	8	10	13	11	10	11	5	10	0.88317	100/100	Non-Overlapping Temp
9	15	10	10	4	6	16	10	10	10	0.24928	97/100	Non-Overlapping Temp
15	5	14	14	10	5	10	3	11	13	0.05536	98/100	Non-Overlapping Temp
11	12	9	11	13	7	14	10	8	5	0.63712	99/100	Non-Overlapping Temp
20	6	11	15	12	4	7	11	8	6	0.01179	99/100	Non-Overlapping Temp
13	8	13	13	3	12	12	6	11	9	0.30413	100/100	Non-Overlapping Temp
10	7	11	9	7	8	12	10	11	15	0.79814	98/100	Non-Overlapping Temp
18	8	6	9	9	14	8	8	9	11	0.26225	100/100	Non-Overlapping Temp
17	7	14	10	9	6	12	5	9	11	0.20227	99/100	Non-Overlapping Temp
12	10	10	6	9	12	11	12	8	10	0.94631	98/100	Non-Overlapping Temp
8	10	12	11	10	11	11	14	7	6	0.81654	100/100	Non-Overlapping Temp
9	6	10	13	8	13	10	8	11	12	0.85138	98/100	Non-Overlapping Temp
14	8	10	16	9	12	12	6	8	5	0.27571	99/100	Non-Overlapping Temp
10	12	12	12	9	10	10	8	12	5	0.86769	99/100	Non-Overlapping Temp
8	11	16	7	11	9	7	8	11	12	0.63712	98/100	Non-Overlapping Temp
11	10	8	13	13	8	7	14	10	6	0.65793	97/100	Non-Overlapping Temp
14	10	10	5	9	10	13	5	14	10	0.41902	98/100	Non-Overlapping Temp
7	6	13	10	15	8	7	10	7	17	0.16261	99/100	Non-Overlapping Temp
12	6	11	10	11	10	11	8	11	10	0.97170	99/100	Non-Overlapping Temp
7	12	9	7	12	10	12	9	13	9	0.89776	99/100	Non-Overlapping Temp
10	11	11	12	10	9	7	6	16	8	0.61631	99/100	Non-Overlapping Temp
8	6	9	9	12	9	8	16	10	13	0.57490	100/100	Non-Overlapping Temp
2	8	9	8	7	17	14	13	11	11	0.07118	100/100	Overlapping Temp
12	3	16	10	11	15	7	10	9	7	0.14533	97/100	Maurer’s Universal
10	10	16	13	9	11	7	4	11	9	0.40120	99/100	Approximate Entropy
7	5	3	10	5	8	7	7	9	9	0.73992	70/70	Random Excursions
4	1	6	6	9	10	11	10	4	9	0.12233	70/70	Random Excursions
2	8	9	3	6	12	4	10	7	9	0.14415	69/70	Random Excursions
9	5	6	6	8	8	7	4	10	7	0.89162	70/70	Random Excursions
6	7	6	5	10	8	8	6	9	5	0.92919	68/70	Random Excursions
8	13	8	5	7	4	8	6	7	4	0.45056	68/70	Random Excursions

9	6	8	8	5	5	9	7	9	4	0.86996	68/70	Random Excursions
10	8	6	7	8	5	4	9	10	3	0.56318	68/70	Random Excursions
6	3	8	6	5	11	7	10	7	7	0.65199	69/70	Random Excursions V
4	5	6	6	9	8	8	12	5	7	0.62225	70/70	Random Excursions V
4	4	9	6	9	8	6	11	6	7	0.68164	70/70	Random Excursions V
4	6	6	11	7	9	7	6	5	9	0.76814	70/70	Random Excursions V
3	7	5	6	11	8	7	10	8	5	0.59259	70/70	Random Excursions V
1	4	8	9	6	8	11	7	6	10	0.26604	70/70	Random Excursions V
2	5	7	8	9	11	6	8	8	6	0.56318	70/70	Random Excursions V
4	7	6	10	4	10	8	10	6	5	0.59259	70/70	Random Excursions V
5	6	7	6	9	10	2	10	8	7	0.56318	70/70	Random Excursions V
10	10	7	5	5	10	7	5	6	5	0.71102	70/70	Random Excursions V
10	7	11	7	7	7	5	4	10	2	0.32785	69/70	Random Excursions V
7	10	10	8	7	8	6	6	4	4	0.76814	70/70	Random Excursions V
8	7	10	6	14	6	5	3	8	3	0.12233	70/70	Random Excursions V
6	7	9	9	6	6	8	10	5	4	0.84658	70/70	Random Excursions V
7	7	7	7	8	8	4	9	5	8	0.96969	70/70	Random Excursions V
6	6	9	6	8	8	9	9	5	4	0.89162	70/70	Random Excursions V
5	7	8	5	15	7	6	4	8	5	0.18298	70/70	Random Excursions V
7	7	8	7	10	3	6	9	4	9	0.71102	70/70	Random Excursions V
15	9	15	6	8	14	8	8	11	6	0.26225	99/100	Serial
8	8	14	16	9	9	9	12	7	8	0.53415	99/100	Serial
13	6	14	10	5	13	5	14	7	13	0.14533	99/100	Linear Complexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 66 for a sample size = 70 binary sequences.

Πίνακας II.6: Αναλυτικός πίνακας αποτελεσμάτων, όπως αυτός προκύπτει από την εφαρμογή όλων των ελέγχων του πακέτου NIST, επί ενός αρχείου δεδομένων με όνομα unpredictability64_n2.txt και μέγεθος 100Mbit, το οποίο αποτελείται από 100 ακολουθίες 1Mbit έκαστη.

RESULTS FOR THE UNIFORMITY OF P-VALUES AND THE PROPORTION OF PASSING SEQUENCES

generator is <d:\unpredictability64_n2.txt>

C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	P-VALUE	PROPORTION	STATISTICAL TEST
18	10	10	15	9	13	11	4	5	5	0.02882	92/100*	Frequency
3	7	9	12	6	18	13	11	15	6	0.02200	99/100	Block Frequency
19	7	12	14	9	6	6	11	8	8	0.08559	93/100*	Cumulative Sums
17	11	11	13	11	5	9	6	10	7	0.26225	94/100*	Cumulative Sums
11	9	13	3	14	6	10	12	15	7	0.16261	100/100	Runs
11	13	2	9	10	5	11	13	15	11	0.13728	99/100	Longest Run
10	8	10	12	11	9	8	14	12	6	0.83431	99/100	Rank
10	10	14	3	7	9	10	18	8	11	0.10879	98/100	DFT
10	11	14	9	11	8	11	10	9	7	0.94631	100/100	Non-Overlapping Temp
10	11	13	11	10	10	7	10	10	8	0.98345	99/100	Non-Overlapping Temp
8	7	12	16	11	13	3	12	9	9	0.22482	99/100	Non-Overlapping Temp
10	10	15	8	10	9	8	9	9	12	0.91141	99/100	Non-Overlapping Temp
12	5	9	16	5	8	16	9	13	7	0.09094	98/100	Non-Overlapping Temp
16	10	10	10	9	13	6	9	7	10	0.61631	95/100*	Non-Overlapping Temp
10	9	13	12	6	12	8	10	8	12	0.86769	100/100	Non-Overlapping Temp
10	8	17	8	8	4	6	12	13	14	0.11539	98/100	Non-Overlapping Temp
10	10	12	8	7	7	15	12	7	12	0.65793	100/100	Non-Overlapping Temp
17	8	10	4	10	13	11	10	9	8	0.31908	99/100	Non-Overlapping Temp
15	12	7	8	12	6	11	8	11	10	0.65793	98/100	Non-Overlapping Temp
10	8	5	6	20	11	13	7	14	6	0.02055	99/100	Non-Overlapping Temp
8	11	15	7	9	15	6	7	10	12	0.40120	99/100	Non-Overlapping Temp
8	12	9	17	18	15	3	3	9	6	0.00190	100/100	Non-Overlapping Temp
7	11	4	12	9	15	12	12	10	8	0.45594	100/100	Non-Overlapping Temp
12	9	13	10	9	9	9	12	10	7	0.96430	99/100	Non-Overlapping Temp

10	7	12	6	17	6	9	14	11	8	0.23681	100/100	Non-Overlapping Temp
8	8	18	9	10	11	7	8	9	12	0.41902	98/100	Non-Overlapping Temp
16	10	17	10	6	10	6	7	9	9	0.17187	99/100	Non-Overlapping Temp
8	13	8	10	5	13	12	11	10	10	0.77919	100/100	Non-Overlapping Temp
6	12	7	14	4	15	12	15	7	8	0.09658	100/100	Non-Overlapping Temp
2	10	11	13	12	12	3	12	12	13	0.09658	100/100	Non-Overlapping Temp
9	7	10	17	9	15	6	6	14	7	0.11539	99/100	Non-Overlapping Temp
3	7	10	14	12	7	19	9	5	14	0.01265	100/100	Non-Overlapping Temp
8	8	11	4	11	8	9	16	13	12	0.35049	100/100	Non-Overlapping Temp
13	12	14	8	9	12	11	4	8	9	0.53415	98/100	Non-Overlapping Temp
11	10	9	11	9	16	10	8	10	6	0.73992	100/100	Non-Overlapping Temp
9	10	13	6	7	12	11	15	7	10	0.59555	100/100	Non-Overlapping Temp
11	9	15	8	13	9	7	10	12	6	0.63712	98/100	Non-Overlapping Temp
12	11	7	10	15	9	10	10	6	10	0.77919	98/100	Non-Overlapping Temp
11	10	8	14	11	12	13	4	9	8	0.57490	99/100	Non-Overlapping Temp
10	9	4	16	10	12	15	12	10	2	0.04872	98/100	Non-Overlapping Temp
11	9	9	6	14	10	12	12	9	8	0.85138	99/100	Non-Overlapping Temp
10	8	7	15	12	9	6	9	11	13	0.63712	100/100	Non-Overlapping Temp
9	10	10	10	11	11	12	6	7	14	0.85138	100/100	Non-Overlapping Temp
9	6	12	7	12	11	9	11	12	11	0.89776	100/100	Non-Overlapping Temp
12	15	10	8	17	8	7	7	6	10	0.21331	98/100	Non-Overlapping Temp
10	12	8	12	11	12	12	6	10	7	0.86769	100/100	Non-Overlapping Temp
6	11	6	7	12	10	13	13	14	8	0.49439	99/100	Non-Overlapping Temp
9	13	8	9	8	11	11	12	10	9	0.97807	100/100	Non-Overlapping Temp
7	6	5	10	11	12	13	10	15	11	0.43727	98/100	Non-Overlapping Temp
15	14	11	10	7	10	9	9	6	9	0.63712	96/100	Non-Overlapping Temp
6	10	6	14	8	15	8	10	10	13	0.43727	98/100	Non-Overlapping Temp
7	8	12	9	11	12	15	8	10	8	0.77919	98/100	Non-Overlapping Temp
5	9	10	6	13	17	6	13	8	13	0.12962	100/100	Non-Overlapping Temp
5	13	6	10	9	13	9	14	9	12	0.51412	99/100	Non-Overlapping Temp
11	11	17	5	6	7	11	11	8	13	0.23681	99/100	Non-Overlapping Temp
7	15	9	12	9	8	6	9	10	15	0.47499	100/100	Non-Overlapping Temp
12	10	4	11	11	6	9	9	13	15	0.40120	99/100	Non-Overlapping Temp
8	12	13	7	10	8	9	17	4	12	0.21331	98/100	Non-Overlapping Temp
14	8	14	12	8	10	8	5	12	9	0.55442	98/100	Non-Overlapping Temp
10	17	7	9	13	6	13	6	4	15	0.04872	99/100	Non-Overlapping Temp
13	7	15	4	12	9	9	8	10	13	0.36692	98/100	Non-Overlapping Temp
6	13	10	5	7	15	12	12	11	9	0.40120	100/100	Non-Overlapping Temp
12	10	11	19	3	4	8	13	9	11	0.02882	98/100	Non-Overlapping Temp
12	11	7	11	14	10	7	9	10	9	0.89776	99/100	Non-Overlapping Temp
7	16	8	6	9	11	5	14	11	13	0.22482	100/100	Non-Overlapping Temp
10	7	9	16	4	8	7	15	15	9	0.10253	98/100	Non-Overlapping Temp
7	12	11	12	7	6	14	9	12	10	0.69931	99/100	Non-Overlapping Temp
9	12	10	13	8	6	15	4	6	17	0.06688	100/100	Non-Overlapping Temp
9	11	13	7	11	7	9	11	14	8	0.81654	99/100	Non-Overlapping Temp
13	13	13	12	8	10	8	10	5	8	0.65793	98/100	Non-Overlapping Temp
11	10	9	12	14	12	4	8	12	8	0.59555	100/100	Non-Overlapping Temp
8	16	15	8	7	10	13	10	7	6	0.26225	98/100	Non-Overlapping Temp
9	6	11	17	9	10	9	11	7	11	0.53415	99/100	Non-Overlapping Temp
10	8	12	8	8	6	13	10	11	14	0.75976	98/100	Non-Overlapping Temp
7	8	8	9	8	9	10	14	11	16	0.57490	100/100	Non-Overlapping Temp
13	8	13	7	8	8	12	12	10	9	0.85138	98/100	Non-Overlapping Temp
8	4	7	15	17	13	10	11	9	6	0.09094	100/100	Non-Overlapping Temp
13	9	10	10	4	13	12	9	9	11	0.71975	100/100	Non-Overlapping Temp
12	10	6	8	10	12	9	13	14	6	0.63712	99/100	Non-Overlapping Temp
12	7	10	9	11	5	5	16	13	12	0.24928	99/100	Non-Overlapping Temp
18	11	6	9	7	7	11	10	9	12	0.30413	99/100	Non-Overlapping Temp
11	12	9	9	8	10	13	5	12	11	0.83431	98/100	Non-Overlapping Temp
10	11	14	9	11	9	10	10	9	7	0.96430	100/100	Non-Overlapping Temp
7	11	9	10	10	8	13	14	7	11	0.83431	99/100	Non-Overlapping Temp
7	8	10	11	12	9	11	8	12	12	0.95584	100/100	Non-Overlapping Temp
13	11	10	5	9	7	17	5	7	16	0.05898	100/100	Non-Overlapping Temp

11	9	11	6	7	12	4	13	14	13	0.33454	99/100	Non-Overlapping Temp
7	17	11	8	16	3	14	8	9	7	0.03757	99/100	Non-Overlapping Temp
8	14	14	9	6	12	7	14	9	7	0.41902	99/100	Non-Overlapping Temp
9	18	6	8	7	11	10	10	14	7	0.21331	100/100	Non-Overlapping Temp
9	10	10	12	11	11	6	15	6	10	0.69931	100/100	Non-Overlapping Temp
8	16	12	6	10	11	10	14	10	3	0.18156	100/100	Non-Overlapping Temp
9	8	9	15	10	11	6	8	15	9	0.55442	100/100	Non-Overlapping Temp
7	17	6	4	10	7	15	11	11	12	0.09094	100/100	Non-Overlapping Temp
12	10	14	5	12	6	11	10	8	12	0.59555	100/100	Non-Overlapping Temp
11	13	8	14	7	11	8	7	14	7	0.55442	98/100	Non-Overlapping Temp
8	13	7	9	12	18	7	9	13	4	0.10253	100/100	Non-Overlapping Temp
12	12	9	7	8	5	11	7	13	16	0.33454	97/100	Non-Overlapping Temp
9	13	16	10	10	7	10	6	9	10	0.61631	98/100	Non-Overlapping Temp
14	14	11	6	10	6	7	9	9	14	0.41902	99/100	Non-Overlapping Temp
13	6	11	9	14	10	13	8	9	7	0.67869	99/100	Non-Overlapping Temp
10	8	12	13	11	9	12	10	7	8	0.93572	100/100	Non-Overlapping Temp
8	7	15	8	4	8	11	12	16	11	0.19169	99/100	Non-Overlapping Temp
12	14	7	6	10	9	16	9	9	8	0.45594	99/100	Non-Overlapping Temp
13	7	17	12	14	5	11	5	11	5	0.05898	98/100	Non-Overlapping Temp
10	12	14	8	8	5	9	12	5	17	0.15376	98/100	Non-Overlapping Temp
8	19	14	7	10	8	8	9	6	11	0.13728	100/100	Non-Overlapping Temp
9	11	16	11	9	11	7	9	7	10	0.73992	100/100	Non-Overlapping Temp
10	14	10	14	5	11	9	11	10	6	0.57490	99/100	Non-Overlapping Temp
7	6	12	14	7	11	7	14	11	11	0.51412	99/100	Non-Overlapping Temp
4	9	11	9	20	14	4	11	9	9	0.02200	98/100	Non-Overlapping Temp
8	10	18	10	9	7	7	9	7	15	0.20227	99/100	Non-Overlapping Temp
8	3	13	7	9	11	9	14	15	11	0.23681	100/100	Non-Overlapping Temp
8	9	8	13	8	10	14	9	10	11	0.91141	99/100	Non-Overlapping Temp
12	12	13	8	14	9	6	10	8	8	0.71975	96/100	Non-Overlapping Temp
10	14	8	10	9	8	14	8	11	8	0.83431	97/100	Non-Overlapping Temp
14	13	5	10	9	8	17	7	9	8	0.22482	100/100	Non-Overlapping Temp
10	12	11	9	12	10	11	7	12	6	0.91141	100/100	Non-Overlapping Temp
8	13	11	11	8	9	8	10	13	9	0.94631	100/100	Non-Overlapping Temp
5	12	14	9	11	12	16	10	5	6	0.17187	100/100	Non-Overlapping Temp
8	13	6	11	6	13	15	6	12	10	0.35049	99/100	Non-Overlapping Temp
11	10	7	9	11	11	16	11	5	9	0.57490	99/100	Non-Overlapping Temp
11	12	12	8	12	12	11	7	9	6	0.85138	96/100	Non-Overlapping Temp
10	6	8	13	13	9	6	9	12	14	0.57490	99/100	Non-Overlapping Temp
8	9	10	14	7	9	10	12	10	11	0.93572	98/100	Non-Overlapping Temp
5	13	6	7	8	13	12	14	12	10	0.38383	100/100	Non-Overlapping Temp
12	7	9	14	15	13	5	11	8	6	0.27571	98/100	Non-Overlapping Temp
11	9	7	17	11	12	10	10	8	5	0.40120	100/100	Non-Overlapping Temp
11	10	10	9	9	12	11	7	10	11	0.99425	99/100	Non-Overlapping Temp
8	12	12	11	8	12	10	10	6	11	0.92408	100/100	Non-Overlapping Temp
9	5	8	4	11	9	13	16	12	13	0.18156	100/100	Non-Overlapping Temp
9	9	10	15	14	9	6	7	16	5	0.16261	100/100	Non-Overlapping Temp
9	6	11	13	14	10	6	9	8	14	0.53415	100/100	Non-Overlapping Temp
12	4	10	16	11	12	10	5	8	12	0.24928	97/100	Non-Overlapping Temp
10	9	7	8	11	13	11	12	11	8	0.94631	100/100	Non-Overlapping Temp
8	11	8	17	12	10	6	12	9	7	0.41902	99/100	Non-Overlapping Temp
10	11	10	9	7	11	9	11	14	8	0.94631	100/100	Non-Overlapping Temp
10	10	10	9	8	7	11	12	15	8	0.85138	99/100	Non-Overlapping Temp
9	9	11	9	7	11	3	11	12	18	0.15376	99/100	Non-Overlapping Temp
13	9	7	11	14	10	7	9	11	9	0.85138	97/100	Non-Overlapping Temp
8	4	10	16	13	11	8	12	9	9	0.38383	100/100	Non-Overlapping Temp
6	13	12	6	5	12	11	14	11	10	0.41902	100/100	Non-Overlapping Temp
14	14	14	15	5	6	10	7	6	9	0.12233	100/100	Non-Overlapping Temp
11	9	11	4	10	13	15	6	8	13	0.33454	98/100	Non-Overlapping Temp
8	7	13	10	5	10	9	13	10	15	0.51412	99/100	Non-Overlapping Temp
6	11	13	17	8	11	7	12	6	9	0.27571	100/100	Non-Overlapping Temp
11	13	6	9	9	4	14	12	5	17	0.07118	100/100	Non-Overlapping Temp
7	6	15	22	7	12	10	8	5	8	0.00430	98/100	Non-Overlapping Temp

7	8	16	8	6	11	9	13	10	12	0.49439	100/100	Non-Overlapping Temp
15	8	9	17	6	10	8	8	4	15	0.05898	99/100	Non-Overlapping Temp
11	8	9	10	11	6	15	9	11	10	0.83431	98/100	Non-Overlapping Temp
15	9	5	6	10	7	12	13	8	15	0.22482	97/100	Non-Overlapping Temp
13	8	10	13	9	7	10	8	12	10	0.91141	100/100	Non-Overlapping Temp
5	6	7	13	10	14	8	10	15	12	0.28967	100/100	Non-Overlapping Temp
8	9	17	4	12	9	13	10	11	7	0.24928	100/100	Non-Overlapping Temp
11	12	9	9	8	10	13	5	12	11	0.83431	98/100	Non-Overlapping Temp
9	6	12	7	7	13	9	17	12	8	0.30413	98/100	Overlapping Temp
4	9	11	16	12	9	13	7	7	12	0.27571	99/100	Maurer’s Universal
10	7	10	9	6	11	10	11	12	14	0.85138	99/100	Approximate Entropy
3	4	4	6	8	11	6	11	3	3	0.02200	58/59	Random Excursions
2	1	14	8	5	6	7	8	4	4	0.00190	59/59	Random Excursions
6	7	8	5	5	6	4	6	6	6	0.92408	58/59	Random Excursions
5	3	8	5	7	6	4	9	3	9	0.27571	58/59	Random Excursions
10	11	10	3	3	9	4	2	1	6	0.00120	59/59	Random Excursions
10	3	4	8	5	8	3	3	5	10	0.06282	57/59	Random Excursions
3	3	9	7	6	5	6	5	3	12	0.05536	59/59	Random Excursions
6	4	6	8	12	3	5	4	6	5	0.14533	59/59	Random Excursions
4	4	3	8	6	8	7	3	8	8	0.33454	59/59	Random Excursions V
3	7	4	3	7	6	8	9	7	5	0.40120	59/59	Random Excursions V
2	9	2	6	10	4	3	4	8	11	0.00827	59/59	Random Excursions V
0	10	5	7	9	4	8	3	5	8	0.02882	59/59	Random Excursions V
3	7	4	10	5	3	11	5	4	7	0.07118	59/59	Random Excursions V
4	5	7	5	5	7	7	7	5	7	0.89776	59/59	Random Excursions V
6	1	7	6	6	4	12	7	5	5	0.08052	59/59	Random Excursions V
4	6	6	7	7	6	6	5	7	5	0.94631	58/59	Random Excursions V
5	6	8	9	2	5	7	4	10	3	0.12962	59/59	Random Excursions V
7	10	8	4	6	5	5	5	4	5	0.51412	57/59	Random Excursions V
10	9	4	8	6	4	4	4	4	6	0.24928	59/59	Random Excursions V
6	8	6	7	6	7	4	7	5	3	0.75976	59/59	Random Excursions V
6	8	6	5	6	10	5	2	8	3	0.22482	59/59	Random Excursions V
5	6	8	6	7	4	7	3	9	4	0.51412	57/59	Random Excursions V
6	8	4	4	8	10	3	5	6	5	0.33454	58/59	Random Excursions V
7	6	6	7	5	8	4	7	4	5	0.83431	58/59	Random Excursions V
10	6	5	2	6	5	6	8	7	4	0.33454	58/59	Random Excursions V
8	9	5	3	4	5	3	9	7	6	0.27571	57/59	Random Excursions V
8	9	8	10	7	7	12	16	13	10	0.57490	99/100	Serial
9	7	13	12	7	9	13	8	12	10	0.83431	98/100	Serial
7	6	8	13	12	8	15	15	7	9	0.30413	100/100	Linear Complexity

The minimum pass rate for each statistical test with the exception of the random excursion (variant) test is approximately = 96 for a sample size = 100 binary sequences. The minimum pass rate for the random excursion (variant) test is approximately = 56 for a sample size = 59 binary sequences.

ΑΝΑΦΟΡΕΣ

[1] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, and S. Ioannidis, “Two-factor Authentication : Is the World Ready ? Quantifying 2FA Adoption Categories and Subject Descriptors,” in *EuroSec ’15 Proceedings of the Eighth European Workshop on System Security*, 2014, no. October.

[2] C. W. O’Donnell, G. E. Suh, and S. Devadas, “PUF-Based Random Number Generation,” *MIT CSAIL CSG Technical Memo 481*, 2004.

[3] R. Pappu, “Physical One-Way Functions,” PhD Thesis, Massachusetts Institute of Technology, 2001.

[4] D. Lim, J. W. Lee, B. Gassend, E. G. Suh, M. van Dijk, and S. Devadas, “Extracting secret keys from integrated circuits.,” in *Very Large Scale Integration (VLSI) Systems, IEEE Transactions*, 2005, vol. 13, no. 10, pp. 1081–1085.

[5] S. S. Kumar, J. Guajardo, R. Maes, G. J. Schrijen, and P. Tuyls, “The Butterfly PUF protecting IP on every FPGA,” in *Proc. of the IEEE International Workshop on Hardware-Oriented Security and Trust (HOST)*, 2008, no. 71369, pp. 67–70.

[6] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, “Enhancing RFID Security and Privacy by Physically Unclonable Functions,” in *Towards Hardware-Intrinsic Security: Foundations and Practice*, A.-R. Sadeghi and D. Naccache, Eds. Springer, 2010, pp. 281–305.

[7] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, “Design and Implementation of PUF-Based ‘Unclonable’ RFID ICs for Anti-Counterfeiting and Security Applications,” in *Proc. of the IEEE International Conference on RFID*, 2008, pp. 58–64.

[8] F. Armknecht, R. Maes, A. R. Sadeghi, F. X. Standaert, and C. Wachsmann, “A formal foundation for the security features of physical functions,” in *Proceedings - IEEE Symposium on Security and Privacy*, 2011, pp. 397–412.

[9] T. McGrath, I. E. Bagci, Z. M. Wang, U. Roedig, and R. J. Young, “A PUF taxonomy,” *Appl. Phys. Rev.*, vol. 6, no. 11303, 2019.

[10] U. Rührmair, F. Sehnke, J. S ölter, G. Dror, S. Devadas, and J. Ü. Schmidhuber, “Modeling attacks on physical unclonable functions,” in *Proc. of the 17th ACM conference on Computer and communications security - CCS ’10*, 2010, p. 237.

[11] F. Sehnke, C. Osendorfer, J. Sölter, J. Schmidhuber, and U. Rührmair, “Policy gradients for cryptanalysis,” in *Artificial Neural Networks – ICANN 2010. ICANN 2010. Lecture Notes in Computer Science*, 2010, vol. 6354, pp. 168–177.

[12] U. Ruhrmair, J. Solter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, “PUF modeling attacks on simulated and silicon data,” *IEEE Trans. Inf. Forensics Secur.*, vol. 8, no. 11, pp. 1876–1891, 2013.

[13] U. Ruhrmair and J. Solter, “PUF modeling attacks: An introduction and overview,” in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014, pp. 1–6.

[14] P. H. Nguyen, D. P. Sahoo, R. S. Chakraborty, and D. Mukhopadhyay, “Efficient attacks on robust ring oscillator PUF with enhanced challenge-response set,” in *2015 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2015, pp. 641–646.

[15] J. Delvaux and I. Verbauwhede, “Side channel modeling attacks on 65nm arbiter PUFs exploiting CMOS device noise,” in *Proc. of the 2013 IEEE Int. Symposium on Hardware-Oriented Security and Trust (HOST)*, 2013, pp. 137–142.

[16] U. Rührmair, X. Xu, J. Sölter, A. Mahmoud, M. Majzoobi, F. Koushanfar, and W. Burleson, “Efficient Power and Timing Side Channels for Physical Unclonable Functions,” *Cryptogr. Hardw. Embed. Syst.*, no. 8731, pp. 476–492, 2014.

[17] S. Tajik, F. Ganji, J. P. Seifert, H. Lohrke, and C. Boit, “Laser fault attack on physically unclonable functions,” in *Proc. of 2015 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2016, pp. 85–96.

[18] A. Fratalocchi, A. Fleming, C. Conti, and A. Di Falco, “NIST-certified secure key generation via deep learning of physical unclonable functions in silica aerogels,” *Nanophotonics*, vol. 10, no. 1, pp. 457–464, 2020.

[19] Y. Wan, P. Wang, F. Huang, J. Yuan, D. Li, K. Chen, J. Kang, Q. Li, T. Zhang, S. Sun, Z. Qiu, and Y. Yao, “Bionic optical physical unclonable functions for authentication and encryption,” *J. Mater. Chem. C*, vol. 9, no. 38, pp. 13200–13208, 2021.

[20] M. S. Kim, G. J. Lee, J. W. Leem, S. Choi, Y. L. Kim, and Y. M. Song, “Revisiting silk: a lens-free optical physical unclonable function,” *Nat. Commun.*, vol. 13, no. 1, 2022.

[21] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, “Physical One-Way Functions,” *Science (80-.).*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[22] S. Shariati, F.-X. Standaert, L. Jacques, and B. Macq, “Analysis and experimental evaluation of image-based PUFs,” *J. Cryptogr. Eng.*, vol. 2, no. 3, pp. 189–206, 2012.

[23] J. D. R. Buchanan, R. P. Cowburn, A.-V. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K.

Fenton, D. a Allwood, and M. T. Bryan, “Forgery: ‘fingerprinting’ documents and packaging.,” *Nature*, vol. 436, no. 7050, p. 475, 2005.
[24] U. Rührmair, C. Hilgers, and S. Urban, “Optical PUFs Reloaded,” *Eprint.Iacr.Org*, 2013.
[25] U. Rührmair, S. Urban, A. Weiershäuser, and B. Forster, “Revisiting Optical Physical Unclonable Functions,” *Cryptol. ePrint Arch.*, vol. 215, pp. 1–11, 2013.
[26] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York: McGraw - Hill, 1988.
[27] E. Hecht, *Optics*, 5th ed. Harlow: Pearson Education Limited, 2017.
[28] D. Voelz, *Computational Fourier Optics - A MATLAB tutorial*, 1st ed. Bellingham, Washington: SPIE Press, 2011.
[29] M. Ramamurthy and V. Lakshminarayanan, “Human Vision and Perception,” in *Handbook of Advanced Lighting Technology*, 1st ed., R. Karlicek, C.-C. Sun, G. Zissis, and R. Ma, Eds. Springer Publishing Company, Incorporated, 2017, pp. 754–787.
[30] “ASTM E308-15, Standard Practice for Computing the Colors of Objects by Using the CIE System.”
[31] M. Anderson, R. Motta, S. Chandrasekar, and M. Stokes, “Proposal for a standard default color space for the Internet - sRGB,” *Proc. Color Imaging Conf. Color Sci. Syst. Appl.*, pp. 238–246, 1997.
[32] D. D. Duncan and S. J. Kirkpatrick, “Algorithms for simulation of speckle (laser and otherwise),” in *Proceedings of SPIE - The International Society for Optical Engineering*, 2008, no. January 2008, p. 685505.
[33] J. W. Goodman, “Laser Speckle and Related Phenomena,” in *Topics in Applied Physics*, vol. 9, Berlin: Springer-Verlag, 1975.
[34] J. C. Dainty, “The statistics of speckle patterns,” in *Progress in Optics*, E. Wolf, Ed. Elsevier, 1977, pp. 1–46.
[35] J. W. Goodman, *Speckle Phenomena in Optics: Theory and Applications*, 2nd ed., no. 1. Washington USA: SPIE, 2020.
[36] E. Collett, *Field Guide to Polarization*, 1st ed. Washington USA: SPIE, 2005.
[37] K. Perlin, “Image Synthesizer,” *Comput. Graph.*, vol. 19, no. 3, pp. 287–296, 1985.
[38] K. Perlin, “Improving Noise,” *ACM Trans. Graph.*, vol. 21, no. 3, pp. 681–682, 2002.
[39] K. Okamoto, *Fundamentals of Optical Waveguides*, 2nd ed. Oxford: Elsevier, 2006.
[40] A. Yariv and P. Yeh, *Photonics: Optical Electronics in Modern Communications*, 6th ed. New York: Oxford University Press, 2007.
[41] E. Grivas, N. Raptis, and D. Syvridis, “An Optical Mode Filtering Technique for the Improvement of the Large Core,” *J. Light. Technol.*, vol. 28, no. 12, pp. 1796–1801, 2010.
[42] D. Gloge, “Weakly Guiding Fibers,” *Appl. Opt.*, vol. 10, no. 10, pp. 2252–2258, 1971.
[43] M. Greenberg, M. Nazarathy, and M. Orenstein, “Data Parallelization by Optical MIMO Transmission Over Multimode Fiber with Intermodal Coupling,” *J. Light. Technol.*, vol. 25, no. 6, pp. 1503–1514, 2007.
[44] R. Paschotta, “Noise in Laser Technology,” *Opt. Photonik*, vol. 5, no. 1, pp. 55–57, 2010.
[45] U. Jain, “Characterization of CMOS Image Sensor,” Delft University of Technology, 2016.
[46] J.-G. Dumas, J.-L. Roch, E. Tannier, and S. Varrette, *Foundations Of Coding: Compression, Encryption, Error Correction*, 1st ed. New Jersey: Wiley & Sons Inc, 2015.
[47] G. Tzimpragos, C. Kachris, I. B. Djordjevic, M. Cvijetic, D. Soudris, and I. Tomkos, “A Survey on FEC Codes for 100G and Beyond Optical Networks,” *IEEE Commun. Surv. Tutorials*, vol. 18, no. 1, pp. 209–221, 2014.
[48] I. S. Reed and X. Chen, *Error - Control Coding for Data Networks*. Springer Science & Business Media, 1999.
[49] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data,” *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.
[50] R. Sobti and G. Geetha, “Cryptographic Hash Functions : A Review,” *Int. J. Comput. Sci. Issues*, vol. 9, no. 2, 2012.
[51] P. Koeberl, J. Li, A. Rajan, and W. Wu, “Entropy Loss in PUF-based Key Generation Schemes : The Repetition Code Pitfall,” in *2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST)*, 2014, pp. 44–49.
[52] A. Juels and M. Wattenberg, “A fuzzy commitment scheme,” in *Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28–36.
[53] L. Xudong, “Robust Digital Image Hashing Algorithms for Image Identification,” University of British Columbia, 2013.
[54] C. Harris and M. Stephens, “A Combined Corner and Edge Detector,” in *Proceedings of the 4th Alvey Vision Conference*, 1988, pp. 147–152.
[55] A. Alahi, R. Ortiz, and P. Vandergheynst, “FREAK: Fast Retina Keypoint,” in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2012, pp. 510–517.
[56] Κ. Μουστάκας, Ι. Παλιόκας, Α. Τσακίρης, and Δ. Τζοβάρας, *Γραφικά Και Εικονική Πραγματικότητα*. ΣΕΑΒ, ΚΑΛΛΙΠΟΣ, 2015.

[57] D. Coltuc and P. Bolon, “Strict Ordering on Discrete Images and Applications,” in *Procs of the 1999 International Conference on Image Processing*, 1999, no. 2, pp. 150–153.
[58] D. Coltuc, P. Bolon, and J. Chassery, “Exact Histogram Specification,” *IEEE Trans. Image Process.*, vol. 15, no. 5, pp. 1143–1152, 2006.
[59] E. J. Candès and M. B. Wakin, “An Introduction To Compressive Sampling,” *IEEE Signal Process. Mag.*, vol. 25, no. 2, pp. 21–30, 2008.
[60] K. Li and S. Cong, “State of the art and rospects of Structured Sensing matrices in Sompressed Sensing,” *Front. Comput. Sci.*, vol. 9, no. 5, pp. 665–677, 2015.
[61] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 4th ed. Pearson, 2008.
[62] F. M. Naini, R. Gribonval, L. Jacques, and P. Vandergheynst, “Compressive Sampling of Pulse Trains: Spread the Spectrum!,” in *IEEE International Conference on Acoustics Speech Signal Processing*, 2009, pp. 2877–2880.
[63] T. T. Do, L. Gan, N. H. Nguyen, and T. D. Tran, “Fast and Efficient Compressive Sensing Using Structurally Random Matrices,” *IEEE Trans. Signal Process.*, vol. 60, no. 1, pp. 139–154, 2012.
[64] N. H. Παπαμάρκος, *Ψηφιακή Επεξεργασία & Ανάλυση Εικόνας*. Ξάνθη, Ελλάδα: Κρίκος, 2010.
[65] R. A. Sadek, “SVD Based Image Processing Applications : State of The Art , Contributions and Research Challenges,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 3, no. 7, pp. 26–34, 2012.
[66] L. Cao, “Singular Value Decomposition Applied To Digital Image Processing,” Arizona State University Polytechnic Campus Mesa, Arizona.
[67] S. S. Kozat, R. Venkatesan, and M. K. Mihcak, “Robust perceptual image hashing via matrix invariants,” in *International Conference on Image Processing (ICIP)*, 2004, pp. 3443–3446.
[68] V. Monga and M. K. Mıhçak, “Robust and Secure Image Hashing via Non-Negative Matrix Factorizations,” *IEEE Trans. Inf. Forensics Secur.*, vol. 2, no. 3, pp. 376–390, 2007.
[69] F. Armknecht, D. Moriyama, and A. Sadeghi, “Towards a Unified Security Model for Physically Unclonable Functions,” in *The Cryptographers’ Track at the RSA Conference*, 2016, pp. 271–287.
[70] R. Maes and I. Verbauwhede, “Physically Unclonable Functions: A Study on the State of the Art and Future Research Directions,” in *Towards Hardware-Intrinsic Security*, 2010, pp. 3–37.
[71] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray, and S. Vo, “A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.” 2010.
[72] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
[73] S. J. Kirkpatrick, D. D. Duncan, and E. M. Wells-Gray, “Detrimental effects of speckle-pixel size matching in laser speckle contrast imaging,” *Opt. Lett.*, vol. 33, no. 24, p. 2886, 2008.
[74] U. Maurer, R. Renner, and S. Wolf, *Security with Noisy Data: On Private Biometrics, Secure Key Storage and Anti-Counterfeiting.* Springer Science & Business Media, 2007.
[75] P. Ping, Y. Mao, X. Lv, F. Xu, and G. Xu, “An image scrambling algorithm using discrete Henon map,” in *2015 IEEE International Conference on Information and Automation, ICIA 2015 - In conjunction with 2015 IEEE International Conference on Automation and Logistics*, 2015, no. August, pp. 429–432.
[76] I. Atakhodjaev, “Machine Learning Attacks on Optical Physical Unclonable Functions,” Johns Hopkins University, 2018.
[77] G. E. Lio, S. Nocentini, L. Pattelli, E. Cara, D. S. Wiersma, U. Rührmair, and F. Riboli, “Quantifying the Sensitivity and Unclonability of Optical Physical Unclonable Functions,” *Adv. Photonics Res.*, vol. 4, no. 2, p. 2200225, 2023.
[78] B. Bougher, “Introduction to compressed sensing,” *Lead. Edge*, vol. 34, no. 10, pp. 936–937, 2015.
[79] E. Zisselman, A. Adler, and M. Elad, “Chapter 1- Compressed Learning for Image Classification : A Deep Neural Network Approach,” in *Handbook of Numerical Analysis*, 1st ed., vol. 19, R. Kimmel and X.-C. Tai, Eds. Elsevier B.V., 2018, pp. 3–17.
[80] Y. C. Eldar and G. Kutyniok, *Compressed Sensing, Theory and Applications*, 1st ed. New York: Cambridge University Press, 2012.
[81] D. L. Donoho and X. Huo, “Uncertainty Principles and Ideal Atomic Decomposition,” *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2845–2862, 2001.
[82] S. Qaisar, R. M. Bilal, W. Iqbal, M. Naureen, and S. Lee, “Compressive Sensing : From Theory to Applications , A Survey,” *J. Commun. Networks*, vol. 15, no. 5, pp. 443–456, 2013.