ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Φυσικές Μη Αναπαράξιμες Λειτουργίες

Πασχάλης Μ. Βαλσαμάκης

Επιβλέπων: **Δημήτριος Συβρίδης,** Καθηγητής

ΑΘΗΝΑ

ΝΟΕΜΒΡΙΟΣ 2021

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Φυσικές Μη Αναπαράξιμες Λειτουργίες

Πασχάλης Μ. Βαλσαμάκης
Α.Μ.: 1115201700011

ΕΠΙΒΛΕΠΩΝ: **Δημήτριος Συβρίδης,** Καθηγητής

ΠΕΡΙΛΗΨΗ

Η φυσική μη αναπαράξιμη λειτουργία (PUF), η οποία αποτελεί βασικό αντικείμενο μελέτης της παρούσας πτυχιακής, ορίζεται ως μια συσκευή που εκμεταλλεύεται την εγγενή τυχαιότητα που εισήχθη κατά την κατασκευή για να δώσει σε μια φυσική οντότητα ένα μοναδικό «δακτυλικό αποτύπωμα». Ακόμη, η αυθεντικοποίηση επιβεβαιώνει την ταυτότητα των μερών κατά τη διάρκεια των επικοινωνιών. Επίσης, οι έννοιες PUF για ηλεκτρονικές εφαρμογές είναι πολλές και δύνανται εύκολα να ενσωματωθούν και να ψηφιοποιηθούν. Επιπροσθέτως, αναλύεται ένα ευέλικτο και οπτικό σύστημα ελέγχου ταυτότητας βασισμένο σε φυσικές απροσδιόριστες λειτουργίες (PUF), ενώ παρουσιάζεται ένα σχήμα οπτικής ιεραρχικής πιστοποίησης βασισμένο στην αρχή της παρεμβολής και τη συνάρτηση κατακερματισμού. Τέλος, αναλύεται το πλαίσιο μηχανικής μάθησης που περιλαμβάνει στοιχεία για τον εντοπισμό επιθέσεων που μπορούν να αξιοποιήσουν την εποπτευόμενη, ημι-εποπτευόμενη και χωρίς επίβλεψη μάθηση για τον εντοπισμό επιθέσεων και, κατά περίπτωση, τον προσδιορισμό του τύπου και της έντασής τους.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Προστασία Φυσικού Επιπέδου

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: PUF, επεκτάσεις, αυθεντικοποίηση, κρυπτογράφηση, μηχανική μάθηση

ABSTRACT

Physical unclonable function (PUF), which is the main subject of this dissertation, is defined as a device that takes advantage of the inherent randomness introduced during construction to give a physical entity a unique "fingerprint. Also, authentication confirms the identity of the parties during communications. Apart from that, PUF concepts for electronic applications are many and can be easily integrated and digitized. In addition, a flexible and optical authentication system based on physical indeterminate functions (PUF) is analyzed, while a visual hierarchical certification scheme based on the principle of interference and the hash function was presented. Finally, the machine learning framework is analyzed which includes elements for detecting attacks that can utilize supervised, semi-supervised and unsupervised learning to detect attacks and, where appropriate, determine their type and intensity.

SUBJECT AREA: Physical Layer Security

KEYWORDS: PUF, extensions, authentication, encryption, machine learning

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΡΟΛΟΓΟΣ

Η παρούσα Πτυχιακή Εργασία εκπονήθηκε στην Αθήνα από τον Μάιο του 2021 μέχρι και τον Νοέμβριο του 2021. Αποτελεί αναπόσπαστο κομμάτι για την απόκτηση του πτυχίου και διεξήχθη κατά το τελευταίο έτος της φοίτησής μου ως προπτυχιακός φοιτητής στο Τμήμα Πληροφορικής και Τηλεπικοινωνιών του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών. Για τη διεκπεραίωσή της, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Δημήτριο Συβρίδη για τη συνεργασία και την πολύτιμη συμβολή του στην ολοκλήρωσή της.

ΕΙΣΑΓΩΓΗ

Μια φυσική μη αναπαράξιμη λειτουργία (PUF) είναι μια συσκευή που εκμεταλλεύεται την εγγενή τυχαιότητα που εισήχθη κατά την κατασκευή για να δώσει σε μια φυσική οντότητα ένα μοναδικό «δακτυλικό αποτύπωμα». Αυτές οι συσκευές μπορούν να χρησιμοποιηθούν σε διάφορες εφαρμογές από την παραχάραξη, την ταυτοποίηση, τον έλεγχο ταυτότητας και τη δημιουργία κλειδιών έως προηγμένα πρωτόκολλα, όπως η ανταλλαγή κλειδιών (Willers et al, 2016).

Η αυθεντικοποίηση επιβεβαιώνει την ταυτότητα των μερών κατά τη διάρκεια των επικοινωνιών. Για λόγους ασφαλείας, είναι σημαντικό αυτές οι ταυτότητες να είναι πολύπλοκες, προκειμένου να είναι δύσκολο να κλωνοποιηθούν ή να μαντευθούν. Τα τελευταία χρόνια, εμφανίστηκαν φυσικά μη αναπαράξιμες λειτουργίες (PUF), στις οποίες οι ταυτότητες ενσωματώνονται σε δομές και δεν αποθηκεύονται σε στοιχεία μνήμης. Οι PUF παρέχουν «ψηφιακά δακτυλικά αποτυπώματα», όπου οι πληροφορίες διαβάζονται συνήθως από τη στατική εντροπία ενός συστήματος, αντί να έχουν τεχνητά προγραμματισμένη ταυτότητα, εμποδίζοντας ένα κακόβουλο μέρος να κάνει ένα αντίγραφο για κακόβουλη χρήση αργότερα. Πολλές έννοιες για τη φυσική πηγή της μοναδικότητας αυτών των PUF έχουν αναπτυχθεί για πολλές διαφορετικές εφαρμογές (McGrath et al, 2019).

Παρόλο που ορισμένοι τύποι PUF έχουν λάβει μεγάλη προσοχή, άλλες υποσχόμενες προτάσεις τείνουν να αγνοηθούν. Στο πλαίσιο της παρούσας πτυχιακής, παρουσιάζεται μια ανασκόπηση που επιδιώκει να καταγράψει και να παρέχει ένα οργανωτικό σχήμα προς τις προτεινόμενες έννοιες για PUF. Πιο συγκεκριμένα, αναλύεται η αυθεντικοποίηση, η μελέτη ευέλικτου και επικυρωμένου συστήματος οπτικού ελέγχου ταυτότητας βασισμένο σε PUFs, το σχέδιο οπτικής κρυπτογράφησης και ελέγχου ταυτότητας βασισμένο σε συμβολόμετρο μετατόπισης φάσης, η οπτική ιεραρχική πιστοποίηση σχετικά με την παρεμβολή και τη λειτουργία κατακερματισμού (hash function), η εκμετάλλευση τυχαίων προτύπων οπτικά αναγνώσιμων υλικών για την διασφάλιση του ελέγχου ταυτότητας εγγράφων, μέσων και υποστρωμάτων αλλά και η μηχανική μάθηση για την ασφάλεια οπτικού δικτύου (McGrath et al, 2019).

1. ΚΕΦΑΛΑΙΟ 1

1.1 Ορισμός PUF

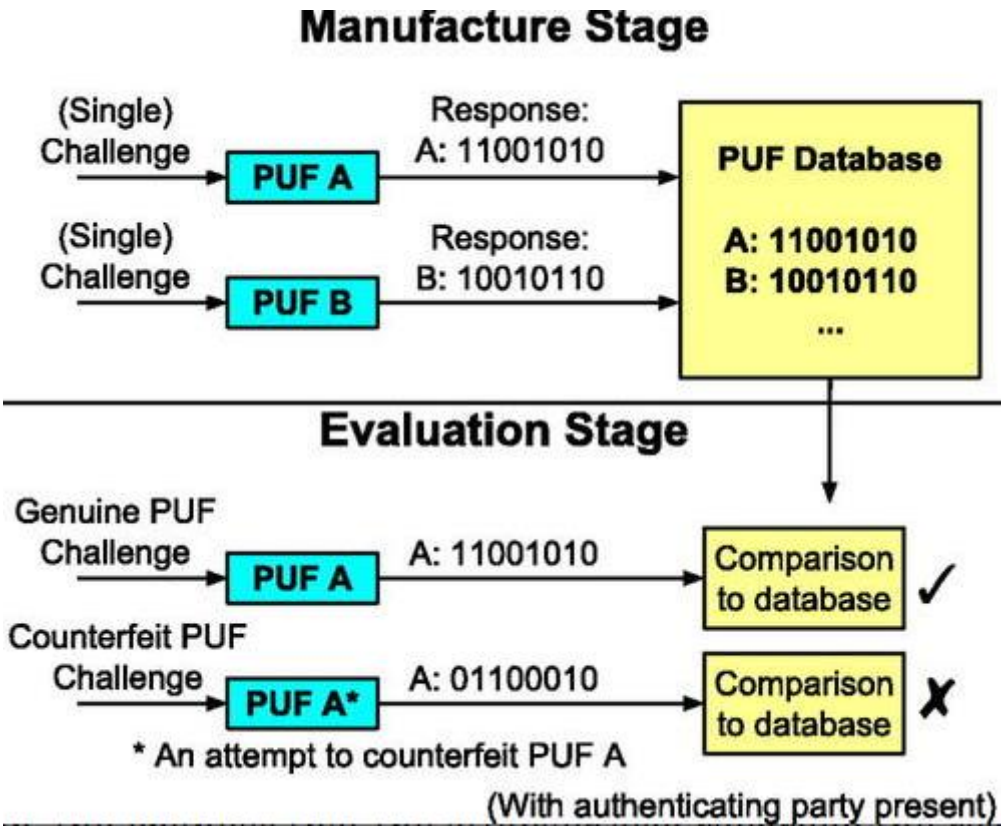
Οι Φυσικές Μη Αναπαράξιμες Λειτουργίες (Physically Unclonable Functions (PUF)) αποτελούν θεμελιώδη στοιχεία ασφάλειας υλικού που μεταφράζουν μια πρόκληση εισόδου σε απόκριση εξόδου μέσω ενός φυσικού συστήματος με τρόπο που είναι συγκεκριμένο για την ακριβή παρουσία υλικού (μοναδικό) και δεν είναι δυνατό να αναπαραχθεί (μη κλωνοποιήσιμο). Αυτό επιτρέπει στο σύστημα, και κατ 'επέκταση σε οποιοδήποτε αντικείμενο ή συσκευή που είναι προσαρτημένα ή ενσωματωμένα μέσα, να πιστοποιούνται με μοναδικό τρόπο. Στο σημείο κατασκευής, το σύστημα υπόκειται σε μία ή περισσότερες προκλήσεις και η απάντηση σε αυτές τις προκλήσεις λαμβάνεται και καταγράφεται. Από εκεί και πέρα, είναι γνωστό ότι εάν μια πρόκληση επαναληφθεί σε οποιοδήποτε σημείο και επαληθευτεί η αναμενόμενη απάντησή της, η συσκευή είναι απαραίτητο να είναι η ίδια με αυτή που χαρακτηρίστηκε προηγουμένως. Τα χαρακτηριστικά μιας PUF είναι απαραίτητο να είναι σταθερά με την πάροδο του χρόνου, μοναδικά (οπότε καμία PUF δεν είναι ίδια), ενώ θα πρέπει να είναι εύκολο να αξιολογηθεί (να εφαρμοστεί εφικτά), δύσκολο να αναπαραχθεί (έτσι η PUF δεν μπορεί να αντιγραφεί) και πολύ δύσκολο ή αδύνατο να προβλεφθεί (McGrath et al, 2019).

Πολλές έννοιες έχουν υποβληθεί ως υποψήφιες για PUF. Ορισμένα, όπως η Arbiter PUF, έχουν καθιερωθεί με μεγάλο αριθμό παραλλαγών. Άλλα, όπως το MEMS PUF ή το BoardPUF, δεν φαίνεται να έχουν σημαντική τρέχουσα εστίαση στον κλάδο. Ενώ υπάρχουν έγγραφα που παρέχουν πληροφορίες και οργάνωση σε μια επιλογή προτεινόμενων PUF, κανένα έγγραφο δεν προβλέπει την παροχή πλήρους ανασκόπησης και σχεδίου οργάνωσης για όλες τις προτεινόμενες PUF σε επίπεδο ιδέας και άνω (Willers et al, 2016).

1.2 Ισχύς των PUF

Στη συνέχεια βλέπετε ένα παράδειγμα παράθεσης σχήματος, με την αντίστοιχη λεζάντα. Η Μια βασική διακριτική ιδιότητα των PUF είναι αυτό που περιγράφεται ως η ισχύς της εφαρμογής τους. Υπάρχουν δύο επίπεδα ισχύος PUF - αδύναμο και ισχυρό. Η ισχύς της PUF εξαρτάται από τον αριθμό των ζευγών απόκρισης πρόκλησης (CRP) που μπορούν να δημιουργηθούν από μία μόνο συσκευή. Αυτή, με τη σειρά της, αντιστοιχεί συνήθως στο πώς ο αριθμός των CRP αυξάνεται με το αυξανόμενο μέγεθος συσκευής (Reuhrmair et al, 2010).

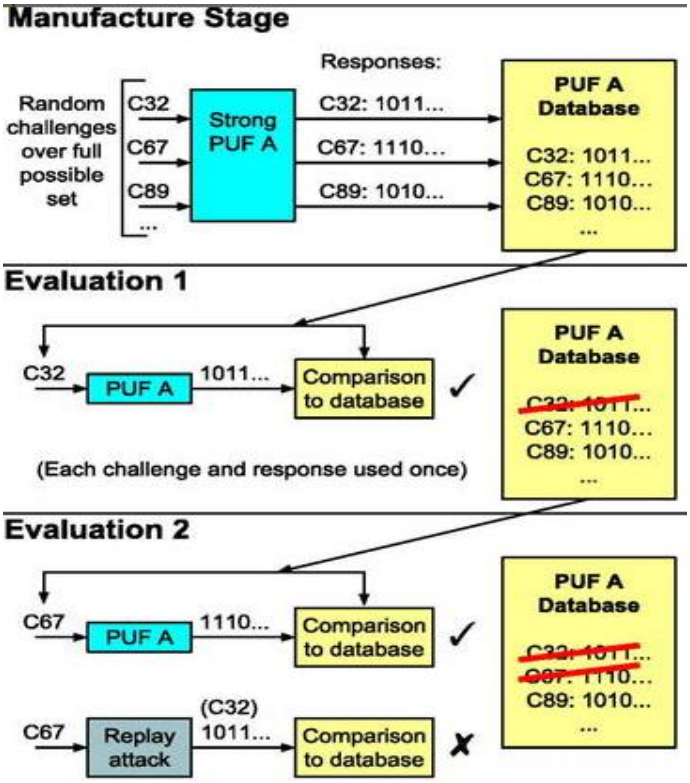
Οι αδύναμες PUF υποστηρίζουν έναν σχετικά μικρό αριθμό CRP, συνήθως ως συνέπεια ενός χαμηλού βαθμού κλιμάκωσης. Αυτό σημαίνει ότι το πλήρες σύνολο αυτών των ζευγαριών μπορεί να διαβαστεί από τη συσκευή εάν ένας εισβολέας αποκτήσει φυσική πρόσβαση στη PUF για κάθε δεδομένη στιγμή. Παρόλο που δεν θα ήταν δυνατό να αντιγραφεί η ίδια η φυσική PUF, με γνώση των CRP της PUF, ένας εισβολέας θα μπορούσε να απαντήσει πειστικά σε ερώτημα σαν να είχε ακόμη τη συσκευή - πολύ μετά την εγκατάλειψη της συσκευής. Οι αδύναμες PUF μπορούν να χρησιμοποιηθούν για ασφαλή αποθήκευση κλειδιών και τεχνικές ελέγχου ταυτότητας οντοτήτων, για παράδειγμα, χρησιμοποιώντας το πρωτόκολλο που παρουσιάζεται στην Εικόνα 1. Ωστόσο, για σκοπούς ελέγχου ταυτότητας, η PUF πρέπει να εξεταστεί σε περιβάλλον όπου υπάρχει μέρος ελέγχου ταυτότητας για να διασφαλιστεί ότι η ίδια η PUF αξιολογείται (Reuhrmair et al, 2010).



Εικόνα 1: **Μια απλή εφαρμογή της αδύναμης PUF. Η απόκριση οποιασδήποτε απόπειρας απομίμησης θα διέφερε ανιχνεύσιμα σε σύγκριση με την απόκριση που καταγράφηκε από τη γνήσια PUF (McGrath et al, 2019).**

Οι ισχυρές PUF, από την άλλη πλευρά, κλιμακώνονται με τρόπο ώστε να υποστηρίζουν ένα πολύ μεγαλύτερο σύνολο CRP. Ο αριθμός αυτών των ζευγαριών είναι τόσο μεγάλος, στην πραγματικότητα, που ακόμη και αν ένας εισβολέας έχει πρόσβαση στη PUF δεν μπορεί να τα καταγράψει όλα. Εάν στο στάδιο κατασκευής ληφθεί τυχαία ένα δείγμα αυτών των CRP, οι πιθανότητες ο επιτιθέμενος να καταγράψει επίσης την

απάντηση στην ίδια πρόκληση μπορεί να είναι αμελητέες. Αυτό έχει ως αποτέλεσμα ένα σύστημα όπου ακόμη και αν ο εισβολέας είχε πρόσβαση στη PUF σε ένα συγκεκριμένο σημείο, μόνο ο χρήστης με φυσική πρόσβαση στη PUF τη στιγμή της πρόκλησης έχει την ικανότητα να δώσει τη σωστή απάντηση και να γίνει έλεγχος ταυτότητας. Επιπλέον, μια τόσο μεγάλη ποικιλία CRP σημαίνει ότι κάθε ζεύγος απόκρισης σε πρόκληση χρειάζεται να χρησιμοποιηθεί μόνο μία φορά. Αυτό προστατεύει από την υποκλοπή και μπορεί να διευκολύνει ασφαλή πρωτόκολλα επικοινωνίας χρησιμοποιώντας τη PUF. Ένα απλό παράδειγμα ενός ισχυρού πρωτοκόλλου ελέγχου ταυτότητας PUF παρουσιάζεται στην Εικόνα 2 (McGrath et al, 2019).



Εικόνα 2: Μια απλή εφαρμογή μιας ισχυρής PUF. Εδώ, ακόμη και αν η PUF παραβιαστεί, ένας επιτιθέμενος δεν θα γνώριζε τις σχετικές προκλήσεις για εγγραφή (McGrath et al, 2019).

1.3 Εσωτερική και εξωτερική αξιολόγηση

Πέρα από τη διάκριση μεταξύ μιας PUF με πηγές τυχαιότητας, μια συσκευή είναι πιθανό να ταξινομηθεί σε εγγενείς και μη εγγενείς ποικιλίες αξιολόγησης. Μια εγγενής PUF έχει τυχαιότητα και αξιολογείται εσωτερικά. Ως αποτέλεσμα, τα μέσα μέτρησης ή ανίχνευσης της PUF είναι ενσωματωμένα ή εγγενή στην ίδια τη συσκευή. Εάν αυτές οι δύο προϋποθέσεις δεν πληρούνται, για παράδειγμα, στην περίπτωση μιας μη ολοκληρωμένης πηγής τυχαιότητας, η PUF περιγράφεται ως μη εγγενής ή εξωγενής. Επί του παρόντος, αυτή η εγγενής ιδιότητα είναι πιθανό να κατέχεται μόνο από όλες τις ηλεκτρονικές PUF, καθώς ο μόνος τρόπος για να αξιολογηθεί μια PUF και να δώσει

ηλεκτρονική ανάγνωση αυτή τη στιγμή είναι μέσω ενός ηλεκτρονικού μηχανισμού αξιολόγησης (Verbauwhede et al, 2012). Οι μηχανισμοί εσωτερικής αξιολόγησης είναι πιο επιθυμητοί από την εξωτερική αξιολόγηση, καθώς επιτρέπουν την περαιτέρω επεξεργασία (για παράδειγμα τον κατακερματισμό) χωρίς να έχει εκτεθεί η αρχική απόκριση PUF στο εξωτερικό του εσωτερικού κυκλώματος της PUF. Αυτή η ενσωμάτωση της πηγής τυχαίοτητας και του κυκλώματος αξιολόγησης βοηθά πολύ να αντισταθεί ο άνθρωπος στις μεσαίες και πλευρικές επιθέσεις καναλιών μεταξύ των δύο στοιχείων. Οι μηχανισμοί αξιολόγησης που είναι εσωτερικοί στη PUF, τείνουν επίσης να είναι πιο ακριβείς, ευκολότεροι στη χρήση και λιγότερο επιρρεπείς σε παρεμβολές κακοποιών (Verbauwhede et al, 2012).

1.4 Εφαρμογές και επεκτάσεις PUF

Ενώ η πιο συνηθισμένη χρήση φυσικών μη αναπαράξιμων συναρτήσεων (PUF) είναι για έλεγχο ταυτότητας, υπάρχουν πολλές πρόσθετες εφαρμογές. Βασικά, η αδύναμη PUF μπορεί να περιγραφεί ως ένας μηχανισμός για την παραγωγή και την αποθήκευση ενός (ή μικρού αριθμού) κρυπτογραφικών κλειδιών. Αυτό το κλειδί μπορεί στη συνέχεια να συγκριθεί με μια εξωτερική βάση δεδομένων για αναγνώριση ή έλεγχο ταυτότητας ή να χρησιμοποιηθεί ως μέρος άλλων πρωτοκόλλων, όπως ασφαλής επικοινωνία ή κρυπτογράφηση μνήμης (McGrath et al, 2019).

Όπως και με τα πρωτόκολλα ελέγχου ταυτότητας που περιγράφηκαν προηγουμένως, ο αριθμός των κλειδιών που αποθηκεύονται είναι μικρός, οπότε ένας εισβολέας θα μπορούσε να έχει πρόσβαση στη PUF με τέτοιο τρόπο ώστε να καθορίζει αυτά τα κλειδιά, καθιστώντας το σύστημα στη συνέχεια μη ασφαλές. Αυτό θα ήταν το ίδιο με έναν εισβολέα να ανακαλύψει τον κωδικό πρόσβασης ή το κλειδί για την επικοινωνία ή την κρυπτογράφηση σε ένα πιο συμβατικό σύστημα (McGrath et al, 2019).

Η ισχυρή PUF τείνει επίσης να χρησιμοποιηθεί για τις ίδιες εφαρμογές και μπορεί να θεωρηθεί ως ένας μηχανισμός για τη δημιουργία μεγάλου αριθμού κλειδιών που θα αποθηκευτούν στη συνέχεια. Όπως και στο ισχυρό πρωτόκολλο ελέγχου ταυτότητας PUF, αυτό σημαίνει ότι τα κλειδιά μπορούν να χρησιμοποιηθούν περιττά, αυξάνοντας την ασφάλεια (McGrath et al, 2019).

Επιπλέον, εάν το κλειδί επιλέγεται τυχαία από το μεγάλο δυνατό σύνολο, η πρόσβαση στη PUF είναι απαραίτητο να πραγματοποιείται ταυτόχρονα με τον έλεγχο ταυτότητας, την επικοινωνία ή την αποκρυπτογράφηση, καθώς ο προσδιορισμός του κλειδιού που

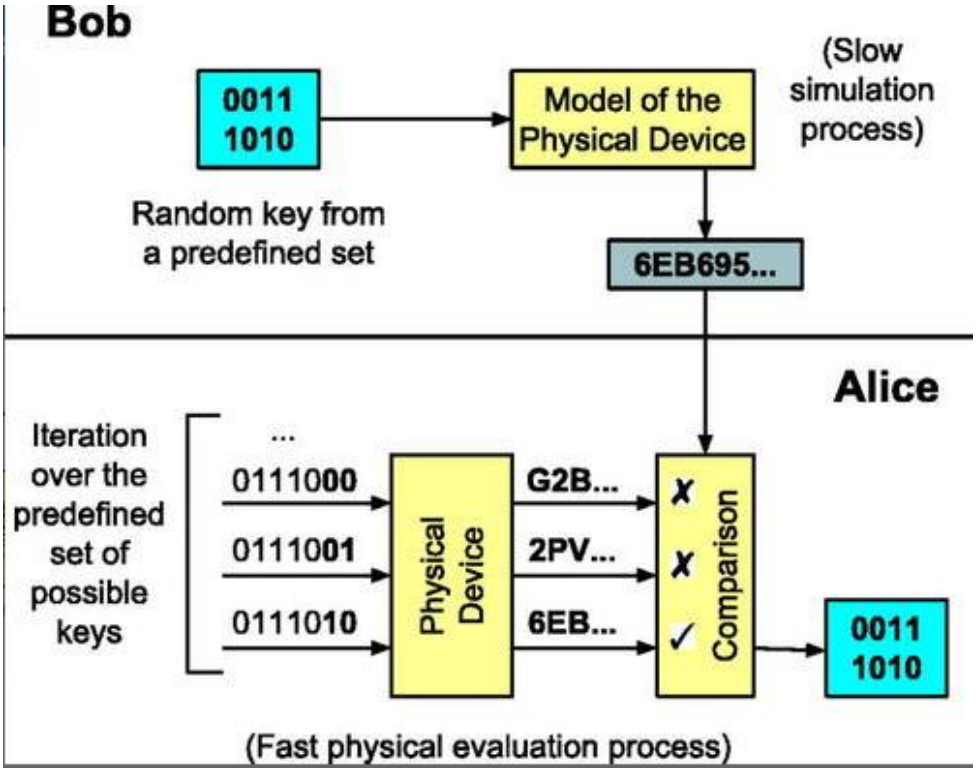
είναι απαραίτητο για την εγγραφή και την επανάληψη δεν θα ήταν δυνατό εκ των προτέρων (Lenstra et al, 2016).

Υπάρχει επίσης μια σειρά πρόσθετων ή εναλλακτικών επεκτάσεων στις έννοιες των PUF, οι οποίες μπορούν να επεκτείνουν τη λειτουργικότητα και την ικανότητά τους. Τα δύο πιο αξιοσημείωτα από αυτά είναι η επαναδιαμορφώσιμη PUF (rPUF) και η δημόσια PUF (PPUF). Η rPUF είναι μια συσκευή που μπορεί να αλλάξει σκόπιμα την απόκριση της στην ίδια πρόκληση εισόδου. Αυτό επιτρέπει την ενημέρωση νέων ζευγών απόκρισης πρόκλησης, την ανάκληση προηγούμενων CRP και επιτρέπει την επαναφορά μιας PUF, για παράδειγμα, για την εκ νέου ανάθεση της συσκευής σε νέο σκοπό ή χρήστη. Είναι σημαντικό να ληφθεί μέριμνα ώστε να εξασφαλιστεί ότι η νέα απόκριση, η επαναφορά στο πεδίο, είναι τόσο μοναδική και απρόβλεπτη όσο και οι απαντήσεις που δημιουργήθηκαν αρχικά στη φάση της κατασκευής. Ένα παράδειγμα μηχανισμού για αυτή τη PUF περιλαμβάνει τήξη οπτικών μέσων ως μέρος μιας PUF ή ελεγχόμενη ανανέωση ενός κελιού μη πτητικής μνήμης, όπως η PCM (Phase Change Memory) RAM (McGrath et al, 2019).

Η PPUF, γνωστή αλλιώς ως σύστημα SIMPL (Simulation Possible but Laborious), είναι πιο πολύπλοκη. Εδώ, η PUF μπορεί να διαμορφωθεί από τις παραμέτρους σε μια χρονοβόρα διαδικασία. Αυτό σημαίνει ότι κάποιος με πρόσβαση στις παραμέτρους μπορεί, δεδομένου χρόνου, να αντλήσει ένα ή περισσότερα από τα ζεύγη απόκρισης πρόκλησης που υπάρχουν στην ίδια τη φυσική PUF (Lenstra et al, 2016).

Μια απλή εφαρμογή μιας PPUF για ανταλλαγή μυστικών κλειδιών παρουσιάζεται στο στην Εικόνα 3. Σε αυτό το σχήμα, ο Bob έχει πρόσβαση σε ένα δημόσια διαθέσιμο μοντέλο του φυσικού PPUF της Alice. Αυτό το μοντέλο μπορεί να μεταφράσει μια πρόκληση (εδώ μια τυχαία πρόκληση από ένα καθορισμένο σύνολο) στην αναμενόμενη απάντηση της PUF σε ένα όχι ασήμαντο χρονικό πλαίσιο. Αυτή η απάντηση μπορεί στη συνέχεια να σταλεί στην Alice μέσω οποιουδήποτε δημόσιου ή ιδιωτικού καναλιού. Η Alice μπορεί στη συνέχεια να επαναλάβει το πλήρες σύνολο των πιθανών προκλήσεων μέχρι να βρει την απάντηση που ταιριάζει με αυτήν που στάλθηκε από τον Bob. Αυτή η επανάληψη μπορεί να γίνει μόνο με τη φυσική συσκευή λόγω χρονικών περιορισμών στη μοντελοποίηση της. Επομένως, μόνο η Alice (ο κάτοχος της φυσικής συσκευής) μπορεί να μεταφράσει την απάντηση πίσω για να βρει το αρχικό μυστικό κλειδί. Αυτό το πρωτόκολλο είναι παρόμοιο με την κρυπτογράφηση ασύμμετρου κλειδιού στην κρυπτογραφία δημόσιου κλειδιού, όπου το μοντέλο PPUF λειτουργεί ως δημόσιο κλειδί της Alice και η επαναλαμβανόμενη φυσική συσκευή λειτουργεί ως ιδιωτικό κλειδί της

Alice. Ωστόσο, αξίζει να σημειωθεί εδώ ότι αυτό το σύστημα υποθέτει ότι αυτό το έργο που είναι βαρύ για υπολογισμούς θα διαρκεί πάντα τόσο ώστε να εμποδίζει τη συλλογή μεγάλου αριθμού αυτών των ζευγαριών και να αναδημιουργήσει το PUF. Τα βήματα προς τα εμπρός στη συμβατική ισχύ υπολογιστή και στον κβαντικό υπολογισμό θα μπορούσαν επομένως να ακυρώσουν ή να αποδυναμώσουν τα συστήματα PPUF, με τον ίδιο τρόπο όπως τα μήκη κλειδιών παραγοντοποίησης RSA στην κρυπτογραφία δημοσίου κλειδιού (Lenstra et al, 2016).



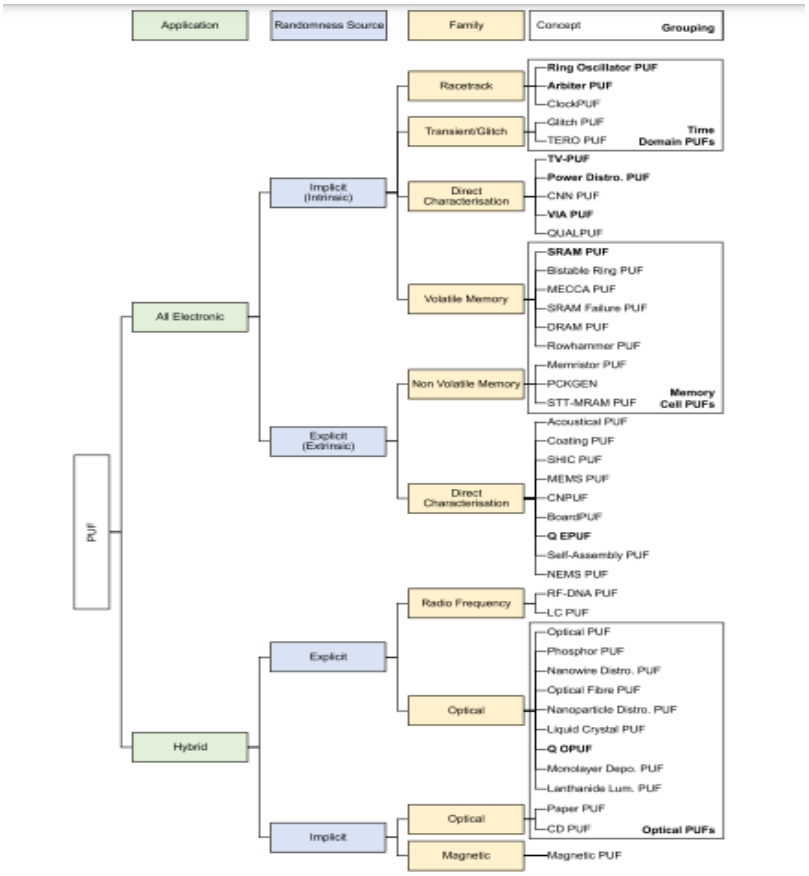
Εικόνα 3: Ένα διάγραμμα που δείχνει μια απλή εφαρμογή του PPUF για ανταλλαγή μυστικών κλειδιών. Η μονόδρομη λειτουργία μπορεί να αντιστραφεί μόνο μέσω της επανάληψης της φυσικής συσκευής, λόγω περιορισμών ταχύτητας στη διαδικασία προσομοίωσης (McGrath et al, 2019).

1.5 Συστήματα κατάταξης

Υπάρχουν πολλές έννοιες και παραλλαγές μη αναπαράξιμων συναρτήσεων και ακόμη περισσότερες έχουν προταθεί τόσο για τον χαρακτηρισμό κυκλωμάτων όσο και για φυσικά αντικείμενα. Εδώ, παρουσιάζονται 3 διαφορετικά σχήματα οργάνωσης. Αυτά περιγράφονται ως οργανική (με γνώμονα την ιδιότητα), παραμετρική (με παράμετρο) και χρονολογική ταξινόμηση (McGrath et al, 2019).

1.5.1 Οργανικό σύστημα

Το πρώτο σύστημα, που παρουσιάζεται στην Εικόνα 4**,** χωρίζει το σύνολο των PUF σε ομάδες σε 6 επίπεδα. Αυτά τα επίπεδα ξεκινούν με την Εφαρμογή, την Πηγή Τυχαιότητας, την Οικογένεια και την Έννοια - μαζί με δύο επιπλέον επίπεδα και μια ομάδα εννοιών. Αυτά τα επιπλέον επίπεδα δεν περιλαμβάνονται στα ακόλουθα διαγράμματα σχεδίων οργάνωσης και σχετίζονται με τη συγκεκριμένη παραλλαγή και εφαρμογή μιας PUF, για τον μοναδικό προσδιορισμό οποιασδήποτε συσκευής στο μικρότερο δυνατό επίπεδο (McGrath et al, 2019).



Εικόνα 4: Γράφημα του "οργανικού" σχήματος οργάνωσης για φυσικά μη ασύρματες συναρτήσεις (McGrath et al, 2019).

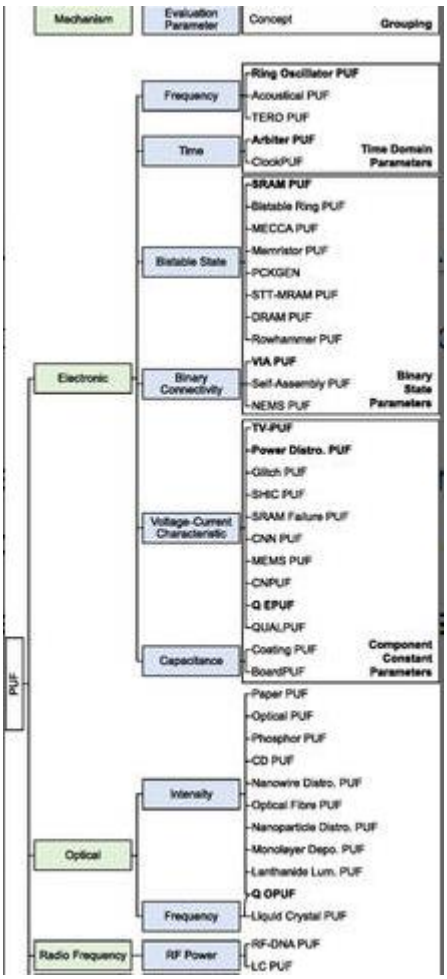
Το οργανικό σύστημα ομαδοποίησης είναι πιο αυθαίρετο και όχι τόσο συγκεκριμένο όσο το παραμετρικό ή χρονολογικό σχήμα οργάνωσης, αλλά φαίνεται πιο διαισθητικό (McGrath et al, 2019).

1.5.2 Παραμετρικό σύστημα

Το δεύτερο σχήμα οργάνωσης είναι το παραμετρικό σχήμα, που φαίνεται στην Εικόνα 5**.** Αυτό χωρίζει το σύνολο των εννοιών PUF σε δύο επίπεδα. Το πρώτο από αυτά τα επίπεδα, ο μηχανισμός αξιολόγησης, οργανώνει με ποιο μέσο υπάρχουν τα σήματα που αξιολογούν την PUF, όπως ένα ηλεκτρονικό σήμα, μια δέσμη φωτός ή λέιζερ, ηλεκτρομαγνητικά κύματα ραδιοσυχνοτήτων ή μαγνητική ακτινοβολία κοντά στο πεδίο. Το δεύτερο επίπεδο, η παράμετρος αξιολόγησης, ταξινομεί τις PUF στη συγκεκριμένη και κύρια παράμετρο της αξιολογούμενης ιδιότητας που εξετάζεται (McGrath et al, 2019).

Είναι πιθανό ότι μια PUF μπορεί να εξετάσει περισσότερες από μία παραμέτρους, όπως μια οπτική PUF που εξετάζει τη φωτεινότητα μιας εικόνας (οπτική ένταση) και το χρώμα (οπτική συχνότητα). Αυτό είναι ένα σπάνιο φαινόμενο, καθώς προσθέτει μια άλλη διάσταση πολυπλοκότητας στη διαδικασία εξαγωγής PUF. Σε αυτές τις περιπτώσεις, μια παρόμοια PUF μπορεί να υπάρχει σε δύο ή περισσότερες από αυτές τις κατηγορίες (McGrath et al, 2019).

Οι έννοιες των PUF είναι ιδέες υψηλότερου επιπέδου για το πώς να σχεδιαστεί και να δημιουργηθεί μια PUF από ένα συγκεκριμένο φυσικό ή ηλεκτρονικό σύστημα και περιλαμβάνουν τα Arbiter PUF, Glitch PUF, SRAM failure PUF, STT-MRAM PUF κ.ο.κ. Πέραν του επιπέδου έννοιας, προτείνεται να είναι τα επίπεδα παραλλαγής και εφαρμογής. Η παραλλαγή θα αντιπροσωπεύει τις πολλές διαφορετικές ποικιλίες της ίδιας έννοιας PUF, για παράδειγμα, προσπάθειες να γίνει μια PUF πιο ασφαλής ή να προσαρμόσει τη συνολική αρχιτεκτονική της PUF σε συγκεκριμένη εφαρμογή. Αυτές οι παραλλαγές δεν ξεφεύγουν από την αρχική ιδέα αρκετά για να κάνουν τη δική τους κατηγορία εννοιών και υπάρχουν ως διαφορετικές «γεύσεις» του υψηλότερου εννοιολογικού επιπέδου (McGrath et al, 2019).



Εικόνα 5: Γράφημα για την εμφάνιση του «παραμετρικού» οργανωτικού σχήματος για μια σειρά PUF. Σημειώστε ότι το Q OPUF έχει παραμέτρους αξιολόγησης συχνότητας και έντασης φωτός (McGrath et al, 2019).

1.5.3 Χρονολογικό σύστημα

Το τελικό σχέδιο οργάνωσης είναι το χρονολογικό. Όπως υποδηλώνει το όνομα, σε αυτό το σχέδιο απλώς παραγγέλλεται μέχρι την ημερομηνία της πρώτης πρότασης της ιδέας. Αυτές οι έννοιες χωρίζονται στον ηλεκτρονικό μηχανισμό με χρονικό πεδίο, κύτταρο μνήμης και άμεσο χαρακτηρισμό και στις ομαδοποιήσεις από το οργανικό σχήμα οργάνωσης. Οι υβριδικοί μηχανισμοί PUF ομαδοποιούνται σε οπτικά και μη οπτικά PUF. Αυτή η διαίρεση σε ξεχωριστά κομμάτια ενεργεί για τη λεπτομέρεια της συσσώρευσης εννοιών σε κάθε μία από αυτές τις μεγάλες σχολές σκέψης και την εξέλιξη των νέων PUF που προτείνονται με την πάροδο του χρόνου (McGrath et al, 2019).

2. ΚΕΦΑΛΑΙΟ 2

2.1 Διαδικασία αυθεντικοποίησης

Η διαδικασία αυθεντικοποίησης χρησιμοποιείται από έναν διακομιστή όταν ο διακομιστής είναι απαραίτητο να γνωρίζει ακριβώς ποιος έχει πρόσβαση στις πληροφορίες ή στον ιστότοπό του (Tabbara et al, 2019).

Ακόμη, χρησιμοποιείται από έναν πελάτη όταν ο πελάτης πρέπει να γνωρίζει ότι ο διακομιστής είναι το σύστημα που ισχυρίζεται ότι είναι. Κατά τον έλεγχο ταυτότητας, ο χρήστης ή ο υπολογιστής είναι απαραίτητο να αποδείξει την ταυτότητά του στον διακομιστή ή τον πελάτη. Συνήθως, ο έλεγχος ταυτότητας από διακομιστή συνεπάγεται τη χρήση ονόματος χρήστη και κωδικού πρόσβασης. Άλλοι τρόποι ελέγχου ταυτότητας είναι πιθανό να είναι μέσω καρτών, σαρώσεων αμφιβληστροειδούς, αναγνώρισης φωνής και δακτυλικών αποτυπωμάτων (Tabbara et al, 2019).

Η διαδικασία αυθεντικοποίησης από έναν πελάτη συνήθως περιλαμβάνει τον διακομιστή να δίνει ένα πιστοποιητικό στον πελάτη στο οποίο ένα αξιόπιστο τρίτο μέρος, όπως το Verisign ή το Thawte, δηλώνει ότι ο διακομιστής ανήκει στην οντότητα (όπως μια τράπεζα) στην οποία αναμένει ο πελάτης. Ο έλεγχος ταυτότητας δεν καθορίζει ποιες εργασίες δύναται να κάνει το άτομο ή ποια αρχεία μπορεί να δει το άτομο. Ο έλεγχος ταυτότητας απλώς προσδιορίζει και επαληθεύει ποιο είναι το άτομο ή το σύστημα (Tabbara et al, 2019).

2.2 Δημιουργία οπτικών προτύπων

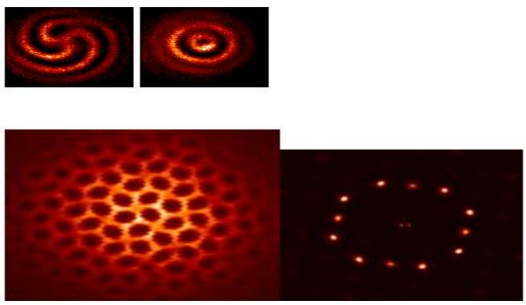
Μη γραμμικά εφέ εμφανίζονται σε πολλά μέσα και σε πολλές διαφορετικές διαμορφώσεις. Όσον αφορά το μέσο, η εστίαση αφορά πειράματα με χρήση ατμών νατρίου. Η μη γραμμικότητα οφείλεται στην οπτική άντληση. Εκτός από τεχνικά πλεονεκτήματα (υψηλή οπτική ποιότητα, εύκολη παραλλαγή παραμέτρων σε μεγάλο εύρος, υψηλή συντονιστική μη γραμμικότητα) το όφελος από τη χρήση ατομικού ατμού είναι ότι οι εξισώσεις που διέπουν την αλληλεπίδραση φωτός-ύλης μπορούν να προκύψουν απευθείας από την κβαντομηχανική μέσω της προσέγγισης μήτρας πυκνότητας. Όσον αφορά τις διαμορφώσεις που ερευνήθηκαν, έχουν διεξαχθεί έρευνες στις περισσότερες περιπτώσεις στις οποίες είναι γνωστό ότι συμβαίνουν χωρικές οπτικές δομές (Tabbara et al, 2019).

Τα πειράματα οδήγησαν στην πρώτη επίδειξη μιας δευτερογενούς αστάθειας ενός εξαγωνικού σχεδίου λόγω ενός δισδιάστατου συντονισμού κυματοδιανυσμάτων στο sqrt (3) του αρχικού αριθμού κυμάτων. Ακόμη, στα αποτελέσματα ανήκει η πρώτη

λεπτομερής διερεύνηση και ερμηνεία των προτύπων πόλωσης και η επίδειξη προτύπων έντασης σπειροειδούς και στόχου σε ένα περιστροφικά συμμετρικό σύστημα αλλά με ακτινικά μεταβαλλόμενες παραμέτρους ελέγχου (Optical Pattern Formation – EQOP Group @ Strathclyde Physics, 2021).

Επίσης, αποδείχθηκε ότι υπάρχει ένα πεπερασμένο εύρος κλειδώματος εάν τα μοτίβα προκαλούνται από μια κλίση του καθρέφτη ανάδρασης και την ερμηνεία του. Ακόμη, προέκυψαν αυθόρμητα υποπεριοδικά μοτίβα με συμμετρία περιστροφής δώδεκα και οκτώ με αυθόρμητο σπάσιμο της περιστροφικής συμμετρίας (Εικόνα 6) (Optical Pattern Formation – EQOP Group @ Strathclyde Physics, 2021).

Επιπρόσθετα, προέκυψε η επίδειξη ενός νέου τύπου αυτοοργανωμένου υπερπλέγματος και μια προσεκτική ανάλυση των ιδιοτήτων των διαλυτικών σολιτονίων, δηλ. αυτο-εντοπισμένων δομών. Συγκεκριμένα, δόθηκαν τα πρώτα πειραματικά στοιχεία για την ύπαρξη πολλαπλών, διακριτών αποστάσεων σε συστάδες διαλυτικών σολιτονίων λόγω αλληλεπιδράσεων μέσω ταλαντευόμενων ουρών. Ακόμη, στα αποτελέσματα ανήκει και η πρώτη πειραματική επίδειξη μιας διακριτής οικογένειας υψηλών τάξεων διαλυτικών σολιτονίων. Τέλος, προέκυψε η πρώτη πειραματική επίδειξη ενός αναπτυξιακού νόμου για τη χονδροποίηση των τομέων ισοδύναμων καταστάσεων που φωλιάζουν μεταξύ τους και πώς αυτά κλειδώνουν για να σχηματίσουν εντοπισμένες δομές (Optical Pattern Formation – EQOP Group @ Strathclyde Physics, 2021).



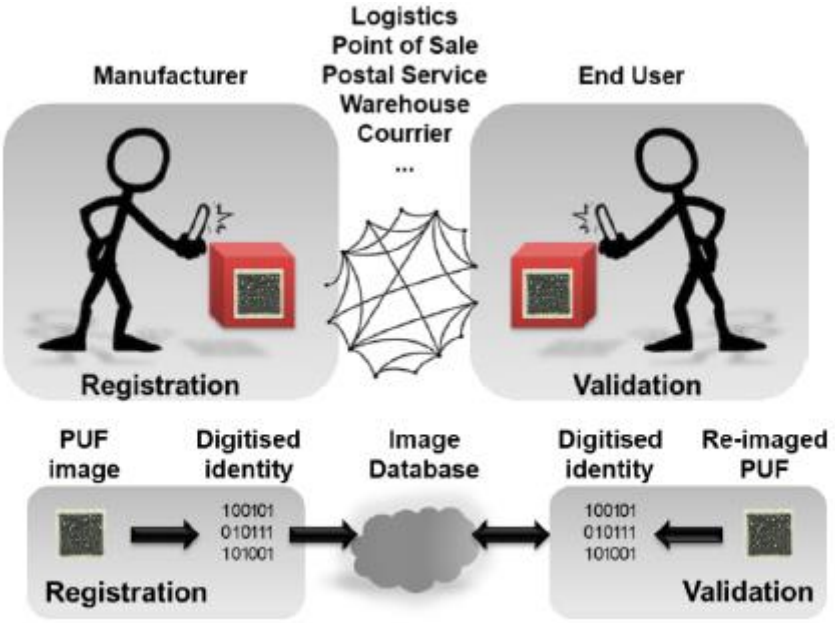
Εικόνα 6: Οπτικά πρότυπα (Optical Pattern Formation – EQOP Group @ Strathclyde Physics, 2021).

2.3 Μελέτη ευέλικτου και επικυρωμένου συστήματος οπτικού ελέγχου ταυτότητας βασισμένο σε PUFs

Η κυκλοφορία των πλαστών προϊόντων δημιουργεί μεγάλες κοινωνικές προκλήσεις. Τα πλαστά καταναλωτικά αγαθά και τα προϊόντα πολυτελείας προκάλεσαν οικονομικές

απώλειες δισεκατομμυρίων δολαρίων, ενώ τα ψεύτικα ιατρικά προϊόντα και τα πλαστά φάρμακα αποτελούν πραγματική απειλή για την ευημερία, ιδιαίτερα στις αναπτυσσόμενες χώρες, την παγκοσμιοποίηση του εμπορίου και τη μετατόπιση των καταναλωτικών συνηθειών. Οι καταναλωτές δεν έχουν πλέον ισχυρούς δεσμούς με το σημείο πώλησης και το σημείο πώλησης δεν έχει πλήρη γνώση της ιστορίας των προϊόντων. Τα πλαστά αγαθά μπορεί εύκολα να εισέλθουν στην αγορά απαρατήρητα. Για να μην συμβεί αυτό, ο κατασκευαστής εφαρμόζει συχνά αντικλεπτικά χαρακτηριστικά, τα οποία συχνά υπόκεινται στην παραποίηση τους (Arppe et al, 2017).

Στην καταπολέμηση της παραχάραξης, οι καθιερωμένες τεχνολογίες χρησιμοποιούν ετικέτες που είναι αποτέλεσμα μιας ντετερμινιστικής διαδικασίας. Έχουν εμφανιστεί ετικέτες τύπου PUF, ενώ οι κυρίαρχες τεχνολογίες κατά της παραποίησης ή απομίμησης βασίζονται σε περιορισμένη πρόσβαση σε ασφαλές μελάνι ή ασφαλή τεχνολογία εκτύπωσης. Το οπτικό σύστημα γνησιότητας που παρουσιάζεται εδώ έχει διαφορετικό χαρακτήρα καθώς κάθε ετικέτα είναι πραγματικά μοναδική και δεν μπορεί ποτέ να αναπαραχθεί ούτε από τον κατασκευαστή, πόσο μάλλον από τους παραχαράκτες (Arppe et al, 2017).



Εικόνα 7: Η έννοια του ελέγχου ταυτότητας με τη χρήση μοναδικών αναγνωριστικών (πάνω): καθώς κάθε προϊόν φέρει μια μοναδική αδιάβροχη ετικέτα PUF, όλα τα προϊόντα μπορούν πάντα να επικυρωθούν και η προέλευση να εξασφαλιστεί. Ο μηχανισμός λειτουργίας (κάτω) του συστήματος οπτικής πιστοποίησης παρουσιάζεται εδώ (Tabbara et al, 2019).

Το πρόβλημα που επιδιώχθηκε να λυθεί στην μελέτη των Tabbara et al, 2019 απεικονίζεται στην Εικόνα 7. Για την περιγραφής της έννοιας PUF χρησιμοποιήθηκαν ιόντα λανθανίδης παγιδευμένα σε ζεόλιθους που διαβάζονται χρησιμοποιώντας ένα

εξελιγμένο μικροσκόπιο φθορισμού. Εδώ, φαίνεται ότι η έννοια PUF είναι βιώσιμη ακόμη και όταν χρησιμοποιείται διασπορά ή απορρόφηση μικροσωματιδίων που διαβάζονται από smartphone εξοπλισμένο με φακό μακροεντολής. Έτσι, η προέλευση οποιουδήποτε προϊόντος μπορεί να επικυρωθεί όταν ο κατασκευαστής τοποθετήσει μια ετικέτα PUF απόδειξης παραβίασης στα προϊόντα (Liao et al, 2015).

Σημειώνεται ότι η ετικέτα PUF είναι μοναδική για το μεμονωμένο προϊόν και ο τελικός χρήστης είναι πιθανό πάντα να επιβεβαιώσει ότι το προϊόν είναι γνήσιο. Καθώς όλα τα προϊόντα είναι εξοπλισμένα με μια μοναδική ετικέτα PUF που καταχωρείται όταν το προϊόν εγκαταλείπει τη γραμμή παραγωγής, είναι δυνατή η αξιολόγηση σε οποιοδήποτε σημείο μέχρι τον τελικό χρήστη. Αυτό εξασφαλίζει επίσης ότι κάθε προϊόν είναι πιθανό να προσδιοριστεί μοναδικά σε όλη την αλυσίδα εφοδιασμού. Καθώς το PUF είναι ικανό να συνδυαστεί με οποιαδήποτε μορφή γραμμικού κώδικα, όπως ένας κωδικός QR, το μέτρο καταπολέμησης της παραχάραξης συνδυάζεται εύκολα με την υπάρχουσα σειριοποίηση. Το οπτικό σύστημα ελέγχου ταυτότητας βασίζεται σε μια βάση δεδομένων ψηφιακών ταυτοτήτων που αποτελεί πλήρη αναπαράσταση κάθε ετικέτας PUF. Κάθε επικύρωση διαμορφώνεται από την αξιόπιστη αρχή έναντι της ψηφιακής ταυτότητας, δεν υπάρχει μείωση δεδομένων μεταξύ του τελικού χρήστη και της αξιόπιστης δημιουργίας και σε καμία περίπτωση η καταχωρημένη ψηφιακή ταυτότητα δεν μοιράζεται με τον τελικό χρήστη (Liao et al, 2015).

Ακόμη, φαίνεται ότι οι ετικέτες PUF μπορούν να δημιουργηθούν από μια ποικιλία υλικών χρησιμοποιώντας τις πιο κοινές τεχνολογίες εκτύπωσης. Επικυρώνεται το σύστημα παραποίησης ή απομίμησης χρησιμοποιώντας 10.000 μοναδικές ετικέτες και διαπιστώνεται ότι το οπτικό σύστημα ελέγχου ταυτότητας σε αυτήν τη μορφή προκαλεί μηδενικά ψευδώς θετικά και έχει ικανότητα κωδικοποίησης 2,5 * (10^120). Αυτό το όριο είναι ο αριθμός των διαφορετικών ετικετών PUF που είναι πιθανό να διαφοροποιηθούν από το σύστημα και όχι ο αριθμός των πιθανών μοτίβων που δημιουργούνται στο αυτοκόλλητο PUF (Tabbara et al, 2019).

2.4 Υλικά και ανάπτυξη PUF για το σύστημα οπτικού ελέγχου ταυτότητας

Το βασικό μελάνι για το σύστημα οπτικού ελέγχου ταυτότητας αναπτύχθηκε με τη δημιουργία εναιωρήματος μικροσωματιδίων σε 1 % (weight/volume) πολυ βινυλική αλκοόλη (PVA, Sigma-Aldrich) με μοριακό βάρος 13000-23000. Τα μικροσωματίδια περιλάμβαναν σκόνη οξειδίου τιτανίου (IV). Όλα τα μελάνια παρασκευάστηκαν χρησιμοποιώντας αναλογία 1 g σκόνης μικροσωματιδίων σε 1% διαλύματος PVA (Tabbara et al, 2019).

Οι κωδικοί QR εκτυπώθηκαν είτε σε ανακυκλωμένο χαρτί ποιότητας γραφείου (80 g/m^2) είτε σε λευκές ετικέτες πολλαπλών χρήσεων Lyreco χρησιμοποιώντας πέντε διαφορετικούς εκτυπωτές, συμπεριλαμβανομένου ενός εκτυπωτή λέιζερ και τεσσάρων εκτυπωτών inkjet. Οι PUF δημιουργήθηκαν με αερογράφο μελάνης στο υπόστρωμα χρησιμοποιώντας αερογράφο Iwata Eclipse HP-CS 0,35 mm. Η τελική ετικέτα PUF πλαστικοποιήθηκε στη συνέχεια χρησιμοποιώντας γυαλιστερές σακούλες πλαστικοποίησης (Fellowes) και ένα Leitz 7474 ILAM Touch Laminator (Tabbara et al, 2019).

Ακόμη, ένα iPhone 7 χρησιμοποιήθηκε ως αναγνώστης εγγραφής. Για την επικύρωση χρησιμοποιήθηκαν τηλέφωνα iPhone 7, iPhone 6, iPhone 4C, iPhone SE, Huawei P9, Samsung Galaxy 6, Samsung Galaxy J3, Oneplus 5t και Oneplus 3t. Με κάθε τηλέφωνο χρησιμοποιήθηκε ένας φακός μακροεντολής Lieqi 15x clip-on (LQ-046) (Tabbara et al, 2019).

Ως φωτεινός αναγνώστης ετικετών, χρησιμοποιήθηκε ένα μικροσκόπιο Olympus IX71 με Olympus 10X, στόχο 0,3 NA CPlanFLN και πηγή διέγερσης X-Cite 120Q (Excelitas Technologies) για την ανάγνωση των φωτεινών ετικετών. Οι φωτεινές ετικέτες απεικονίστηκαν επίσης για σκέδαση χρησιμοποιώντας μικροσκόπιο Nurugo για κινητά τηλέφωνα και iPhone 7 (Tabbara et al, 2019).

Πίνακας 1: Συνδυασμοί υλικών που χρησιμοποιήθηκαν για τη δημιουργία ετικετών φυσικών ασυμβίβαστων λειτουργιών και οι δύο αναγνώστες που χρησιμοποιήθηκαν για την εγγραφή και την επικύρωσή τους (Tabbara et al, 2019).

Tag					Reader
Ink			Substrate	Application method	1: White light 15x lens Camera
Carrier material	Particles	Contrast type			
PVA	ZnO	Scattering	Paper	Spray coating	
Epoxy	TiO2	Scattering	Glass	Knife coating	
Molyol	Silicon carbide	Absorption	Polymer	Stamping	
Glue	Eu^{3+}/Tb^{3+}-phosphors	Scattering/Luminescence	Tape	Painting	2: Microscope filters 10x Camera
	$Tb(acac)_3$	Luminescence		Transfer	
	Carbon powder	Absorption			

2.5 Εγγραφή, αντιστοίχιση και επικύρωση

Όπως αναφέρθηκε, για την επικύρωση του συστήματος οπτικής ταυτοποίησης επιλέχθηκε η χρήση ενός εκτυπωμένου με λέιζερ κωδικού QR σε ανακυκλωμένο χαρτί ποιότητας γραφείου (80 g/m^2) ως υπόστρωμα. Η ετικέτα PUF δημιουργήθηκε με επίστρωση με ψεκασμό διοξειδίου του τιτανίου με μελάνι PVA πάνω στο υποστρώμα χαρτιού. Όλες οι ετικέτες PUF πλαστικοποιήθηκαν με μια θήκη σάρωσης 80 μm για

βελτίωση της ανθεκτικότητας. Η Εικόνα 8 δείχνει την εικόνα εγγραφής μιας αντιπροσωπευτικής ετικέτας PUF που λαμβάνεται με μακροεντολικό φακό 15 ιντσών προσαρτημένο σε iPhone 7. Αυτή η ετικέτα PUF διαβάζεται μέσω της αντίθεσης που παρέχεται από το διάσπαρτο φως από το οξείδιο του τιτάνιου στο τυπωμένο μαύρο φόντο (Tabbara et al, 2019).

Ένας ιδιόκτητος αλγόριθμος χρησιμοποιήθηκε για την καταχώριση της ετικέτας PUF στο μητρώο ετικετών, δημιουργώντας έτσι μια ψηφιακή ταυτότητα ή ένα ψηφιακό δίδυμο του επισημασμένου αντικειμένου. Η Εικόνα 8 δείχνει τα βήματα που εμπλέκονται στη διαδικασία δημιουργίας της ψηφιακής ταυτότητας της ετικέτας PUF (Tabbara et al, 2019).

1. Η εικόνα αποκτάται με μια κάμερα τηλεφώνου και μετατρέπεται σε εικόνα PNG. Τα ενσωματωμένα οπτικά trains που βρίσκονται συνήθως στα σύγχρονα κινητά τηλέφωνα είναι συσκευές CMOS συστήματος σε τσιπ με μετατροπείς αναλογικού σε ψηφιακό 12-bit. (Tabbara et al, 2019).

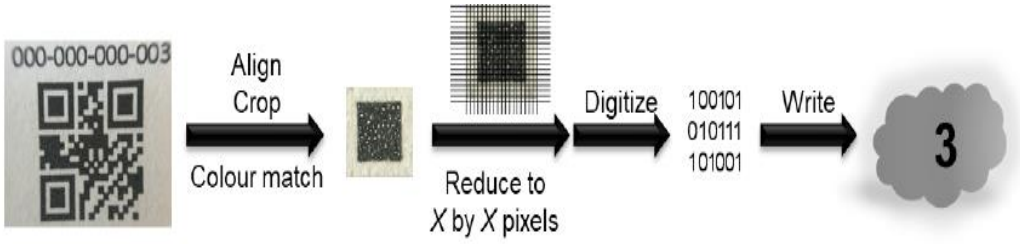
2. Η εικόνα υφίσταται μετασχηματισμό μορφολογίας σε περικοπή, περιστροφή, κλίμακα και διόρθωση αποκλίσεων, αποδίδοντας μια εικόνα με τυπική γεωμετρία που ταιριάζει με αυτήν της ετικέτας αναφοράς με την υπόθεση ότι το υπόστρωμα ετικέτας είναι μια ορθογώνια περιοχή. Ο μετασχηματισμός χρησιμοποιεί το γεγονός ότι υπάρχει ένας μη εκφυλισμένος συγγενικός μετασχηματισμός από τις τέσσερις γωνίες οποιουδήποτε τετράπλευρου σε οποιοδήποτε άλλο τετράπλευρο. Τέλος, το αντίστροφο του συσχετιζόμενου μετασχηματισμού εφαρμόζεται σε ολόκληρη την εικόνα για να παραχθεί μια εικόνα με την ίδια κλίμακα και μορφολογία με την αναφορά (Tabbara et al, 2019).

3. Εφαρμόζονται μη γραμμικά φίλτρα για την ενίσχυση της αντίθεσης και την απομάκρυνση του παραπλανητικού θορύβου από την εικόνα (Tabbara et al, 2019).

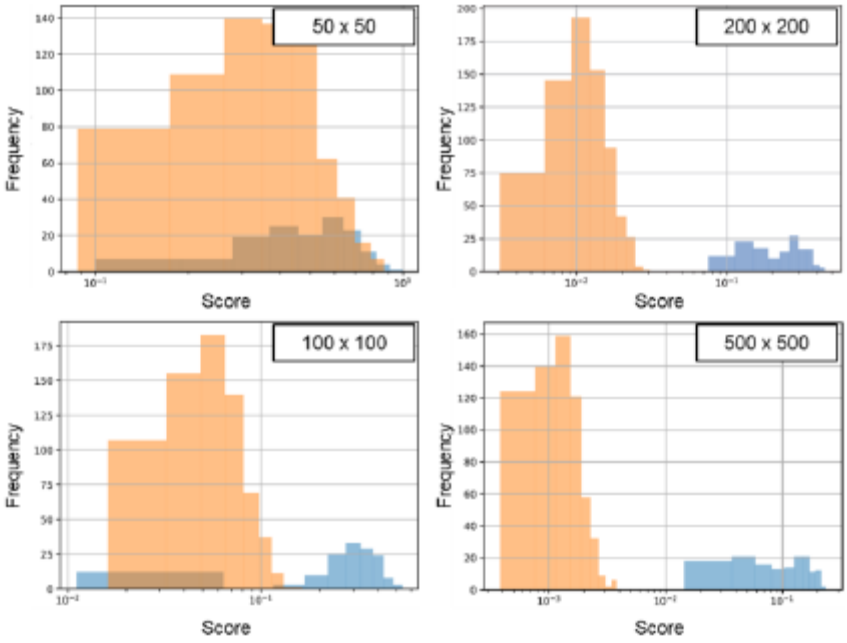
4. Η επεξεργασμένη εικόνα γράφεται στη βάση δεδομένων και αποτελεί την ψηφιακή ταυτότητα που χρησιμοποιείται ως αναφορά για αντιστοίχιση (Tabbara et al, 2019).

Αντί να βασίζεται στην αντιστοίχιση εικονοστοιχείων για εικονοστοιχεία, η αντιστοίχιση πραγματοποιείται με τη σύγκριση βασικών χαρακτηριστικών της αναφοράς και της αποκτηθείσας εικόνας, η οποία είναι αρκετά ισχυρή στο θόρυβο και τις μικρές διαφορές στη μορφολογία. Σε αντίθεση με τους τυπικούς αλγόριθμους εξαγωγής χαρακτηριστικών που χρησιμοποιούνται στην όραση υπολογιστή, τα χαρακτηριστικά που ταιριάζουν δεν διακρίνονται από το θόρυβο. Οι ιδιότητες των ετικετών που τα καθιστούν δύσκολα

πλαστά, καθιστούν επίσης δύσκολη την αναπαράστασή τους χρησιμοποιώντας μια αναπαράσταση χαρακτηριστικών χαμηλών διαστάσεων (Tabbara et al, 2019).



Εικόνα 8: Σχήμα των λειτουργιών που εκτελούνται κατά τη δημιουργία μιας ψηφιακής ταυτότητας για κάθε φυσική μη αναπαράξιμη λειτουργία (Tabbara et al, 2019).

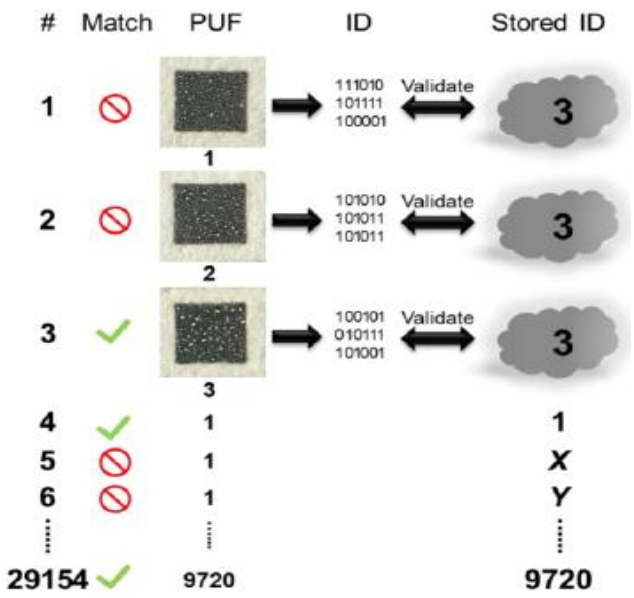


Εικόνα 9: Ο διαχωρισμός μεταξύ πραγματικών (μπλε) και ψευδών (πορτοκαλί) αντιστοιχιών σε έναν αυθαίρετο άξονα βαθμολογίας αντιστοίχισης ως συνάρτηση του μεγέθους της ψηφιακής ταυτότητας (x επί x pixel) (Tabbara et al, 2019).

Οι εικόνες τυποποιήθηκαν σε 200 × 200 εικονοστοιχεία στην άσκηση αξιολόγησης, αποδίδοντας πάνω από 10^1178 μοναδικά μοτίβα bit. Η Εικόνα 9 δείχνει ότι ένας πίνακας 200 × 200 εικονοστοιχείων διασφαλίζει ότι κάθε ετικέτα PUF αναγνωρίζεται ως μοναδική. Χαμηλότερες αναλύσεις όπως 100 × 100 εικονοστοιχεία δημιουργούν ψευδώς θετικά αποτελέσματα, ενώ υψηλότερη ανάλυση π.χ. 500 × 500 έχει ως αποτέλεσμα μεγαλύτερα αρχεία και πιο αργή αντιστοίχιση. Η γεωμετρία 200 × 200 ταιριάζει καλά με το μέγεθος των σωματιδίων, προσφέροντας έναν υψηλό δυναμικό και

λογικό χρόνο διεργασίας για τις ετικέτες PUF που έγιναν για την επικύρωση. Χρησιμοποιώντας έναν πίνακα 200 × 200 εικονοστοιχείων, μια θετική επικύρωση απαιτεί το αποτελέσμα αντιστοίχισης να είναι 0,05 ή υψηλότερο (Tabbara et al, 2019).

Για να εξασφαλιστεί η σταθερότητα των ετικετών PUF, τοποθετήθηκαν σε πλαστικοποίηση. Με τα δεδομένα εγγραφής στη θέση τους, πραγματοποιήθηκε η επικύρωση της αντιστοίχισης της ψηφιακής ταυτότητας με νέες εικόνες των 9.720 ετικετών PUF χρησιμοποιώντας διαφορετικούς αναγνώστες κινητών τηλεφώνων. Κάθε ετικέτα επικυρώθηκε έναντι των αντίστοιχων δεδομένων μητρώου και δύο τυχαία επιλεγμένων καταχωρήσεων από τη βάση δεδομένων. Η διαδικασία επικύρωσης φαίνονται στην Εικόνα 10. Τα αποτελέσματα συγκεντρώνονται στον Πίνακα 2. Η πρόχειρη επιθεώρηση του Πίνακα 2 δείχνει ότι ο ψευδώς θετικός ρυθμός από το δείγμα είναι μικρότερος από έναν στις δέκα χιλιάδες. Για να αποδειχθεί ότι είναι ακόμη χαμηλότερος θα απαιτούσε να δημιουργηθούν, να καταχωρηθούν και να επικυρωθούν τουλάχιστον 100.000 ετικέτες PUF. Το σχετικά υψηλό ποσοστό ψευδώς αρνητικών οφείλεται στην ποιότητα της εικόνας επικύρωσης. Η βρωμιά στην επιφάνεια ή οι εικόνες εκτός εστίασης δεν μπορούν να χρησιμοποιηθούν στη διαδικασία αξιολόγησης. Καθώς η επικύρωση δοκιμάστηκε σε πραγματικό περιβάλλον, με διάφορους τύπους smartphone και διαφορετικά άτομα που εκτελούν την απεικόνιση, μια εύλογη υπόθεση είναι ότι μία στις πέντε επικυρώσεις απαιτεί περισσότερες από μία εικόνες. Αυτό εφαρμόζεται εύκολα σε μια εφαρμογή λογισμικού που ελέγχει την ποιότητα της εικόνας πριν ξεκινήσει η αντιστοίχιση. Για τον τελικό χρήστη, αυτό δεν θα αντιμετωπιστεί καθώς η εφαρμογή θα αποκτήσει απλώς εικόνες έως ότου επιτευχθεί μια κατάλληλη εικόνα. Είναι πιθανό να είναι απαραίτητη μια προτροπή που ζητά από τον τελικό χρήστη να διατηρήσει το τηλέφωνο σταθερό (Tabbara et al, 2019).



Εικόνα 10: Γραφική απεικόνιση της διαδικασίας επικύρωσης του συστήματος οπτικού ελέγχου ταυτότητας (Tabbara et al, 2019).

Πίνακας 2: Δοκιμή αλγορίθμου επικύρωσης στη χρήση εικόνων εγγραφής και ελεγχόμενων αναγνώσεων (Tabbara et al, 2019).

	Registration	Reread [a]
Total number of PUF patterns	1,081	1,081
Total number of matching events	3,240 [b]	3,240 [b]
Correct validations	100.0%	99.63% [c]
Rate of false positives	0.000%	0.000%
Rate of false negatives	0.000%	0.370% [d]
Average match score of true matches	1.00±0.0	0.19±0.079
Average match score of non-matches	0.017±0.006	0.016±0.006

[a] The validation was run twice, the false negatives were identical. [b] 33% true events, 66% false events. [c] The remainder are false negatives (image quality). [d] False negatives were due to poor validation image quality e.g. out of focus.

3. ΚΕΦΑΛΑΙΟ 3

3.1 Σχέδιο οπτικής κρυπτογράφησης και ελέγχου ταυτότητας βασισμένο σε συμβολόμετρο μετατόπισης φάσης

Με την ευρεία ανάπτυξη και χρήση του υπολογιστή και του διαδικτύου, διαφορετικές τεχνικές κρυπτογράφησης για τη μετάδοση ασφαλών πληροφοριών μέσω ψηφιακών καναλιών επικοινωνίας έχουν προσελκύσει αυξανόμενο ενδιαφέρον. Σε σύγκριση με τις τεχνικές ψηφιακής κρυπτογράφησης, οι τεχνικές κρυπτογράφησης οπτικής εικόνας έχουν αξιοσημείωτα πλεονεκτήματα, όπως η παράλληλη επεξεργασία υψηλής ταχύτητας και οι πολυδιάστατες δυνατότητες. Ένα πρωτοποριακό έργο στον τομέα της οπτικής κρυπτογράφησης, που ονομάζεται κωδικοποίηση διπλής τυχαίας φάσης (Double Random Phase Encoding, DRPE), προτάθηκε από τους Refregier και Javidi το 1995. Στο κλασικό σύστημα DRPE, μια εικόνα εισόδου μετατρέπεται σε στάσιμο λευκό θόρυβο χρησιμοποιώντας στατιστικά ανεξάρτητες τυχαίες μάσκες μόνο φάσης (Random Phase-Only Mask, RPM) αντίστοιχα που βρίσκονται στα επίπεδα εισόδου και στα επίπεδα Fourier. Διαδοχικά, ο αλγόριθμος DRPE επεκτάθηκε από τον τομέα Fourier σε άλλους τομείς, όπως κλασματικός Fourier, για περαιτέρω βελτίωση της ασφάλειας του παραδοσιακού συστήματος DRPE χρησιμοποιώντας παραμέτρους δομής ως πρόσθετα ιδιωτικά κλειδιά για μεγέθυνση του χώρου των κλειδιών. Εκτός από τα προαναφερθέντα έργα, η κρυπτοανάλυση είναι σημαντική και απαραίτητη για οποιοδήποτε σύστημα ασφαλείας συμπεριλαμβανομένου του DRPE. Το σύστημα DRPE έχει αποδειχθεί ότι είναι ευάλωτο σε διάφορες επιθέσεις λόγω της εγγενούς γραμμικότητας που εισάγει ο μετασχηματισμός Fourier (Xiong et al, 2020).

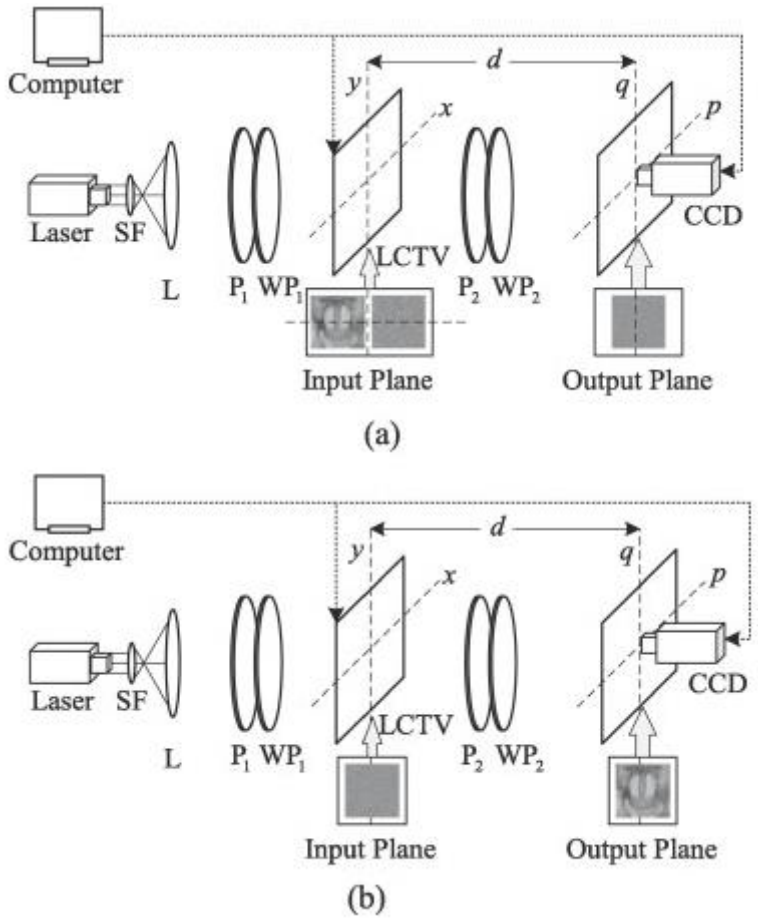
Επιπλέον, δεδομένου ότι η κρυπτογραφημένη εικόνα που λαμβάνεται με χρήση του συστήματος DRPE είναι πολύπλοκη μήτρα που περιλαμβάνει πληροφορίες πλάτους και φάσης, τα κρυπτογραφημένα δεδομένα πρέπει να καταχωρούνται ολογραφικά. Αυτό σημαίνει ότι το σύστημα DRPE απαιτεί ακριβή οπτική ευθυγράμμιση, η οποία στην πράξη είναι δύσκολο να επιτευχθεί. Για την ανακούφιση αυτού του περιορισμού, το JTC εισήχθη στη δομή DRPE. Στο κρυπτοσύστημα που βασίζεται στο JTC, το απλό κείμενο που συνδέεται με ένα RPM τοποθετείται δίπλα-δίπλα με το κλειδί κρυπτογράφησης στο επίπεδο εισόδου και την κατανομή έντασης του φάσματος ισχύος (JPS) καθώς τα κρυπτογραφημένα δεδομένα μπορούν να καταγραφούν χρησιμοποιώντας ένα κοινό αισθητήρα ισχύος, όπως μια συσκευή με ζεύξη φορτίου (CCD). Κατά συνέπεια, έχουν

προταθεί διάφορα σχήματα κρυπτογράφησης που βασίζονται σε JTC (Chen et al, 2019).

Από την άλλη πλευρά, έχουν προταθεί επίσης διάφορα σχήματα ελέγχου ταυτότητας που βασίζονται σε οπτικές τεχνικές. Σε σύγκριση με τα παραδοσιακά σχήματα κρυπτογράφησης στα οποία οι πληροφορίες των απλών κειμένων είναι άμεσα ορατές από αποκωδικοποιημένες εικόνες που λαμβάνονται με σωστά ιδιωτικά κλειδιά, οι αποκωδικοποιημένες εικόνες δεν μπορούν να δώσουν οπτικά πληροφορίες σχετικά με τα απλά κείμενα στα σχήματα ελέγχου ταυτότητας. Στη συνέχεια, παρουσιάζονται μέθοδοι οπτικού ελέγχου ταυτότητας με χωριστή ή απομακρυσμένη βάση δεδομένων όπου αποθηκεύονται περαιτέρω κείμενα για περαιτέρω επαλήθευση αποκωδικοποιημένων εικόνων. Δεδομένου ότι η διεπαφή της βάσης δεδομένων παρέχεται μόνο σε εξουσιοδοτημένους χρήστες, δημιουργείται ένα επιπλέον επίπεδο ασφαλείας για να αντισταθεί στις πιθανές επιθέσεις. Διάφορες επιθέσεις έχουν προταθεί για να σπάσουν τα συστήματα κρυπτογράφησης που βασίζονται σε JTC ενώ λίγες επιθέσεις έχουν ερευνηθεί για να σπάσουν τα σχήματα ελέγχου ταυτότητας που βασίζονται σε JTC (Chen et al, 2019).

3.2 Μελέτη κρυπτοσυστήματος και σκοπιμότητα της προτεινόμενης μεθόδου για την ανάπτυξη σχεδίου οπτικής κρυπτογράφησης

Το σχηματικό διάγραμμα του οπτικού κρυπτοσυστήματος που βασίζεται στο JTC για κρυπτογράφηση δυαδικών δεδομένων που προτείνεται στο φαίνεται στην Εικόνα 11.



Εικόνα 11: Σχηματικό διάγραμμα του συστήματος για (α) διαδικασίες κρυπτογράφησης και (β) αποκρυπτογράφησης. Τα SF και L είναι χωρικά φίλτρα και φακοί, αντίστοιχα. Τα P1 και P2 είναι πολωτικά ενώ τα WP1 και WP2 είναι κυματοειδείς πλάκες. Η προγραμματιζόμενη οθόνη υγρών κρυστάλλων (LCTV) χρησιμοποιείται για την εμφάνιση σημάτων εισόδου και την επίτευξη αλλαγής φάσης. Ο υπολογιστής χρησιμοποιείται για την οδήγηση ενός LCTV και μιας συσκευής που συνδέεται με φόρτιση (CCD) (Xiong et al, 2020).

Σημειώνεται ότι υπάρχουν κάποια εγγενή μειονεκτήματα στο κρυπτοσύστημα. Στη διαδικασία κρυπτογράφησης, το κρυπτοσύστημα μπορεί να επιτύχει κρυπτογράφηση μόνο για δυαδικά απλά κείμενα. Επιπλέον, σε άλλες μελέτες ισχυρίστηκαν ότι το δυαδικό απλό κείμενο απαιτείται για να ληφθούν τα πρότυπα έντασης από PST στο

πρώτο στάδιο εξαγωγής της διαδικασίας αποκρυπτογράφησης. Ωστόσο, στην πρακτική περίπτωση, μόνο τα κρυπτογραφημένα κείμενα και τα κλειδιά αποκρυπτογράφησης δίνονται στους εξουσιοδοτημένους δέκτες. Στη συνέχεια, χρησιμοποιώντας τα σωστά κλειδιά αποκρυπτογράφησης, οι πληροφορίες των αρχικών εικόνων είναι δυνατό να ανακτηθούν από την κωδικοποιημένη εικόνα. Ως εκ τούτου, φαίνεται αδύνατο να ληφθούν οι πληροφορίες των απλών κειμένων πριν επιτευχθεί η διαδικασία αποκρυπτογράφησης με σωστά ιδιωτικά κλειδιά. Κατά συνέπεια, φαίνεται αδύνατο να ληφθούν τα πρότυπα έντασης χρησιμοποιώντας τη διαδικασία εξαγωγής πρώτης φάσης χωρίς καμία γνώση των απλών κειμένων. Από την άλλη πλευρά, εάν τα τρία πρότυπα έντασης αποκτήθηκαν στη διαδικασία κρυπτογράφησης, ένα δυαδικό απλό κείμενο αντιστοιχεί σε τρία πρότυπα έντασης που πρέπει να καταγράφονται ως κρυπτογραφημένα κείμενα και να διαβιβάζονται στους εξουσιοδοτημένους δέκτες. Αυτή η διαδικασία θα επιβαρύνει το πρόβλημα μετάδοσης (Xiong et al, 2020).

3.3 Οπτική ιεραρχική πιστοποίηση σχετικά με την παρεμβολή και τη λειτουργία κατακερματισμού (hash function)

Την τελευταία δεκαετία, οι θεωρίες και οι τεχνολογίες της ασφάλειας των πληροφοριών με οπτικά μέσα, ως νέα διεπιστημονική μέθοδος, έχουν προσελκύσει μεγάλη προσοχή παγκοσμίως λόγω των εγγενών πλεονεκτημάτων της, όπως η ικανότητα παράλληλης επεξεργασίας δεδομένων και η ελευθερία σχεδιασμού πολλαπλών διαστάσεων. Μέχρι τώρα, έχει μελετηθεί και αναπτυχθεί μια σειρά σχετικών έργων. Επικεντρώνονται κυρίως στις πτυχές της κρυπτογράφησης εικόνας, της απόκρυψης εικόνας, της ψηφιακής υδατοσήμανσης και της οπτικής κρυπτανάλυσης. Εν τω μεταξύ, θα άξιζε τον κόπο να επισημανθεί ότι τα περισσότερα από αυτά επικεντρώνονται πάντα στη θεωρητική ανάλυση και στις προσομοιώσεις υπολογιστών και όχι σε πρακτικά πειράματα, επειδή μπλοκάρονται από τη χαμηλότερη ακρίβεια των σημερινών οπτικών εξαρτημάτων. Παρ 'όλα αυτά, πολλοί ερευνητές εξακολουθούν να διατηρούν μια προσεκτικά αισιόδοξη στάση για το μέλλον της ασφάλειας των οπτικών πληροφοριών (He et al, 2012).

Στην μελέτη των Zhang et al, 2008 παρουσίασαν μια προσέγγιση για την κρυπτογράφηση εικόνας βασισμένη σε παρεμβολές δύο δοκών, στην οποία μια μυστική εικόνα χωρίστηκε σε δύο POMs μέσω αναλυτικής προέλευσης. Λίγο αργότερα, ανέπτυξαν ξανά μια μέθοδο για την απόκρυψη δύο εικόνων εισάγοντας έναν επιπλέον αλγόριθμο ανάκτησης φάσης (Zhang et al, 2008).

Πιο πρόσφατα, άλλες μελέτες έδειξαν ανεξάρτητα τα πειραματικά αποτελέσματα για να επαληθεύσουν την αποτελεσματικότητα της κρυπτογράφησης οπτικής εικόνας βάσει παρεμβολών. Οι Yang et al εισήγαγαν την έννοια της κρυπτογράφησης ροής για την κωδικοποίηση των μυστικών εικόνων σε δύο POMs με βάση το συμβολόμετρο Michelson, στα οποία το ένα POM χρησιμεύει ως κλειδί κρυπτογράφησης, ενώ το άλλο θεωρείται ως κρυπτογραφημένο κείμενο. Οι He et al, 2012 ανέφεραν δύο είδη μεθόδων απόκρυψης εικόνας για μία εικόνα και πολλαπλές εικόνες ξεχωριστά με βάση την παρεμβολή δύο δοκών. Ωστόσο, τα περισσότερα από τα προαναφερθέντα σχήματα κρυπτογράφησης εικόνας είναι αρκετά κατάλληλα για να εξηγηθούν ως σύστημα ελέγχου ταυτότητας (He et al, 2012).

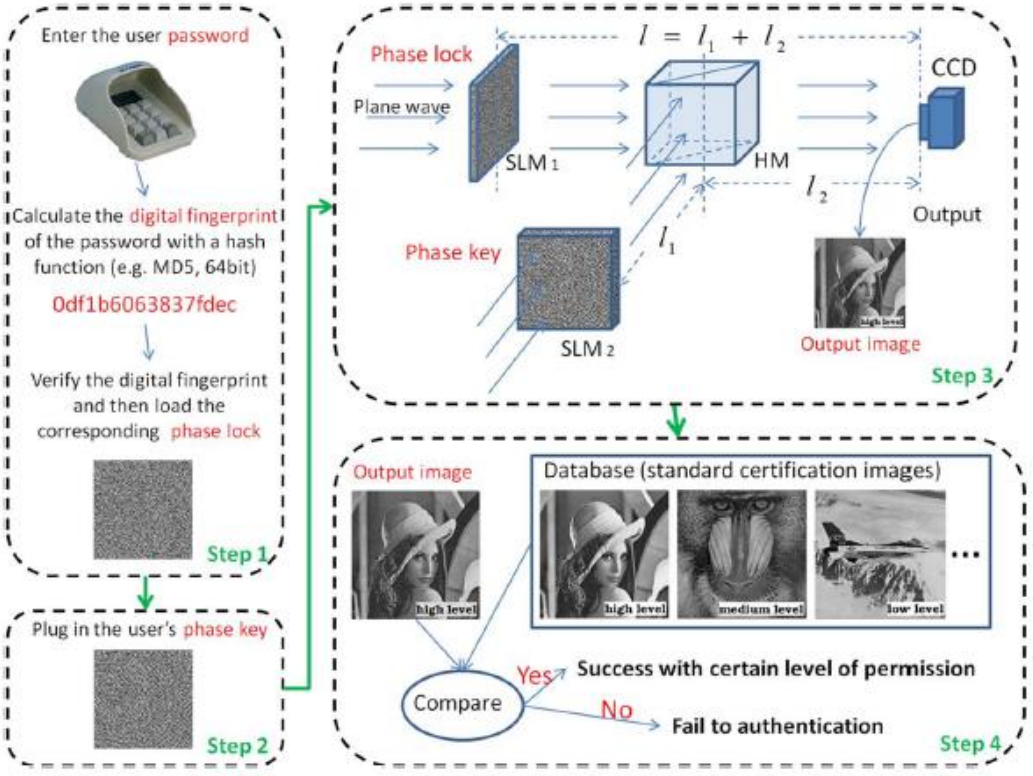
3.4 Αποτελέσματα προσομοίωσης για την οπτική ιεραρχική πιστοποίηση

Μια συνάρτηση κατακερματισμού (hash function) είναι επίσης γνωστή ως μονόδρομο κρυπτοσύστημα. Σε αντίθεση με τα παραδοσιακά συμμετρικά ή ασύμμετρα κρυπτοσυστήματα, είναι ένα ιδιαίτερο είδος κρυπτοσυστήματος χωρίς τη διαδικασία αποκρυπτογράφησης. Επιπλέον, το μυστικό κλειδί για μια λειτουργία κατακερματισμού είναι ακόμη επιλέξιμο και οι πιο διάσημες συναρτήσεις κατακερματισμού, όπως οι MD5 και SHA-1, χρησιμοποιούνται ευρέως χωρίς μυστικό κλειδί. Μια συνάρτηση κατακερματισμού, H (M), λειτουργεί σε ένα προ-κωδικοποιημένο μήνυμα αυθαίρετου μήκους και επιστρέφει μια τιμή κατακερματισμού σταθερού μήκους (He et al, 2012).

Λόγω των προαναφερθέντων χαρακτηριστικών, η τιμή κατακερματισμού ενός μηνύματος είναι λογικό να θεωρείται ως το «ψηφιακό αποτύπωμα (DF)» του μηνύματος. Η πιο κοινή εφαρμογή των συναρτήσεων κατακερματισμού είναι για τον έλεγχο της ορθότητας των μηνυμάτων που μεταδίδονται μέσω των δημόσιων διαύλων επικοινωνίας. Ας γίνει η υπόθεση ότι δύο μέρη (A και B) επικοινωνούν μέσω ενός ανασφαλούς καναλιού, ένα μέρος είναι σημαντικό να επαληθεύσει ότι η ακεραιότητα του μηνύματος προήλθε από το άλλο μέρος για λόγους ασφαλείας. Σε αυτήν την περίπτωση, το μέρος A στέλνει ένα μήνυμα που σχετίζεται με την τιμή κατακερματισμού του, h, στο μέρος B. Στο τέλος του δέκτη, το μέρος B υπολογίζει εκ νέου το ληφθέν μήνυμα χρησιμοποιώντας την ίδια συνάρτηση κατακερματισμού για να δημιουργήσει μια άλλη τιμή κατακερματισμού. Μόνο εάν $h = h'$ μπορεί να ειπωθεί ότι το ληφθέν μήνυμα δεν έχει παραποιηθεί ή παραποιηθεί όταν μεταδίδεται από το μέρος A στο μέρος B. Εν τω μεταξύ, μια άλλη τυπική χρήση της λειτουργίας κατακερματισμού είναι η αποθήκευση των κωδικών πρόσβασης των χρηστών για πολλά συστήματα ασφαλείας ή στις ιστοσελίδες διαδικτύου. Χάρη στη μη αναστρέψιμη ιδιότητα της συνάρτησης

κατακερματισμού, είναι σχεδόν αδύνατο για έναν επιτιθέμενο να αποκτήσει τον κωδικό πρόσβασης του χρήστη, ακόμη και αν μπορεί να λάβει το DF του κωδικού πρόσβασης μέσω εισβολής στο σύστημα. Αυτό το χαρακτηριστικό της συνάρτησης κατακερματισμού ταιριάζει ακριβώς με το ενδιαφέρον μας σε αυτό το έγγραφο (He et al, 2012).

Ο χρήστης εισάγει τον ιδιωτικό κωδικό πρόσβασης μέσω εξωτερικής συσκευής. Το DF του εισαγόμενου κωδικού πρόσβασης θα υπολογιστεί αμέσως με τη βοήθεια μιας συνάρτησης κατακερματισμού. Προσδιορίζοντας αν υπάρχει αντιστοιχία μεταξύ του δημιουργούμενου DF και όλων των DF που έχουν προηγηθεί στη βάση δεδομένων, το σύστημα μπορεί έτσι να πραγματοποιήσει μια προκαταρκτική επαλήθευση: εάν δεν υπάρχει αντιστοίχιση, αυτό σημαίνει ότι ένας μη εξουσιοδοτημένος χρήστης προσπαθεί να επισκεφθεί το σύστημα. Εάν φαίνεται να υπάρχει αντιστοίχιση, στη συνέχεια, φορτώνεται ένα αντίστοιχο κλείδωμα φάσης και γράφεται στον διαμορφωτή χώρου φωτός SLM1 για μετέπειτα χρήση. Μετά την επιβεβαίωση, ο χρήστης υποδεικνύεται ότι συνδέει τη φάση του κλειδιού, το οποίο είναι γραμμένο στο SLM2 για επόμενη χρήση σε μια εικόνα εξόδου (He et al, 2012).



Εικόνα 12: Διαδικασία ελέγχου ταυτότητας χρήστη (He et al, 2012).

4. ΚΕΦΑΛΑΙΟ 4

4.1 Εκμετάλλευση τυχαίων προτύπων οπτικά αναγνώσιμων υλικών για την διασφάλιση του ελέγχου ταυτότητας εγγράφων, μέσων και υποστρωμάτων

Ορισμένες τεχνολογίες προσπάθησαν να διασφαλίσουν την αυθεντικότητα των αντικειμένων βάζοντας κωδικοποιημένα ή μη κωδικοποιημένα σημάδια στα προϊόντα. Μόλις σπάσει ο κώδικας, ωστόσο, δηλαδή, όταν ένας παραχαράκτης μαθαίνει να αντιγράφει μια "υπογραφή", αυτή η μέθοδος χάνει αξία στον έλεγχο ταυτότητας. Έχουν επίσης επιχειρηθεί μέθοδοι δισδιάστατου ελέγχου ταυτότητας. Αυτές οι μέθοδοι είναι χρήσιμες, αλλά μπορούν επίσης να ξεπεραστούν. Έχουν επίσης χρησιμοποιηθεί άλλα, προ-βαθμονομημένα τρισδιάστατα δεδομένα (δηλ. Ολογράμματα). Παρ 'όλα αυτά, στο βαθμό που τα ολόγραμμα είναι προκαθορισμένα, είναι πιθανό επίσης να αντιγραφούν. Οι μηχανισμοί προσδιορισμού της ταυτότητας είναι εγγενώς ευάλωτοι στην παραχάραξη, καθώς ο παραχαράκτης έχει έναν «σταθερό» στόχο (Fraser, 2008).

Η λύση του Tracer εκμεταλλεύεται τυχαία μοτίβα διακριτικών και μοναδικών οπτικών ινών φθορισμού (ή άλλων οπτικά αναγνώσιμων υλικών) και παρέχει έναν συνεχώς «κινούμενο» και μη επαναλαμβανόμενο στόχο, μειώνοντας δραστικά, αν όχι μαθηματικά εξαλείφοντας, την πιθανότητα αντιγραφής. Μια μοναδική αριθμητική τιμή ή κώδικας που παράγεται αλγοριθμικά εκχωρείται και εκτυπώνεται σε κάθε άρθρο και εμφανίζεται σε κοντινή απόσταση από το τυχαίο μοτίβο ινών που είναι πιθανό να ταιριάζει με το μοτίβο για επικύρωση. Αυτός ο συνεχώς «κινούμενος» και μη επαναλαμβανόμενος στόχος καθιστά την αντιγραφή πρακτικά αδύνατη (Fraser, 2008).

Τα προϊόντα ανίχνευσης του Tracer δρουν αποτελεσματικά και δραστικά ενισχύοντας την προστασία και τα επίπεδα ασφάλειας για τον εντοπισμό πλαστών προϊόντων. Το ActivElementsTM επιτρέπει την εύκολη ανίχνευση πλαστών προϊόντων ή εγγράφων από κατασκευαστές ή κυβερνητικούς επιθεωρητές που μπορούν να ελέγξουν την αυθεντικότητα εγγράφων ή προϊόντων σε πραγματικό χρόνο χρησιμοποιώντας τον αναγνώστη του Tracer ή έναν καθολικό αναγνώστη στον οποίο έχει ενσωματωθεί το οπτικό σύστημα ανάγνωσης του Tracer (Fraser, 2008).

Η πιθανότητα εμφάνισης διπλών κωδικών είναι στατιστικά απίθανη (λιγότερο από 1 στα 10^15). Περαιτέρω, ένας κακοβουλος θα είναι σημαντικό ταυτόχρονα να αντιγράψει το υλικό των ινών, τα οπτικά χαρακτηριστικά των ινών και είναι απαραίτητο να χρησιμοποιήσει τα ίδια οπτικά για να σπάσει το σύστημα. Τέλος, η σάρωση των ινών είναι απαραίτητο να πραγματοποιηθεί στη σωστή θέση στο έγγραφο και η εικόνα που προκύπτει πρέπει να ταιριάζει με τον σχετικό κώδικα. Το αποτέλεσμα είναι η άμεση

πιστοποίηση οποιουδήποτε εγγράφου ή αντικειμένου που προστατεύεται από αυτήν την τεχνολογία (Fraser, 2008).

Τα προϊόντα του Tracer παρέχουν μια μοναδική, οικονομικά αποδοτική μέθοδο για τον εντοπισμό πλαστών και εκτροπών προϊόντων. Η ανίχνευση πλαστών αντικειμένων από κατασκευαστές ή κρατικούς επιθεωρητές είναι αναγνώσιμη από μηχανή και ως εκ τούτου, σχετικά εύκολη στην αλυσίδα εφοδιασμού (Fraser, 2008).

4.2 Μηχανική μάθηση για την ασφάλεια οπτικού δικτύου

Τα οπτικά δίκτυα, ως η μόνη βιώσιμη τεχνολογία για την υποστήριξη της σταθερής αύξησης της κίνησης του δικτύου, αποτελούν κρίσιμη υποδομή επικοινωνίας, της οποίας η ασφαλής και αξιόπιστη λειτουργία είναι θεμελιώδης για μια ποικιλία υπηρεσιών και εφαρμογών επικάλυψης. Τα τρωτά σημεία των δομικών στοιχείων οπτικών δικτύων, δηλαδή, οπτικές ίνες, ενισχυτές και διακόπτες, τείνουν να αξιοποιηθούν για την εκτέλεση επιθέσεων φυσικού επιπέδου με στόχο τη διακοπή της υπηρεσίας. Τέτοιες επιθέσεις είναι πιθανό να εκτελεστούν, για παράδειγμα, με άμεση πρόσβαση σε πάνελ ή σε μονάδες ινών που αναπτύσσονται σε μεγάλο βαθμό πέρα από μια ασφαλή περίμετρο (Furdek et al, 2020).

Οι μέθοδοι επίθεσης τείνουν να είναι πολύ διαφορετικές ως προς την πολυπλοκότητά τους, τις καταστροφικές δυνατότητες και τη δυσκολία εντοπισμού και αντιμετώπισής τους. Για παράδειγμα, το κόψιμο της ίνας είναι μια απλή επίθεση που επηρεάζει όλες τις συνδέσεις που διασχίζουν τον σύνδεσμο κοπής και είναι σχετικά εύκολο να εντοπιστεί καθώς προκαλεί απώλεια σήματος στο άκρο του δέκτη. Πιο εξελιγμένες μέθοδοι περιλαμβάνουν την εισαγωγή επιβλαβών σημάτων εμπλοκής (εντός ή εκτός ζώνης) κατά την παραβίαση των επιθεμάτων ή την παραβίαση των ινών, π.χ. με κατάχρηση γνωστής τεχνικής παρακολούθησης για τη δημιουργία προσωρινών παθητικών συζευκτών κάμπτοντας τις ίνες. Η ζημιά από τέτοιες επιθέσεις εξαρτάται από την ισχύ και τις φασματικές ιδιότητες του σήματος εμπλοκής, καθώς και από τον υποκείμενο σχεδιασμό οπτικού δικτύου. Το οπτικό στρώμα είναι πιθανό επίσης να διαταραχθεί χωρίς απαραίτητα να σπάσει η ίνα. Η πολυπλοκότητα των επιπτώσεων που έχουν οι τεχνικές επίθεσης φυσικού επιπέδου στις παραμέτρους του οπτικού καναλιού καθιστά τον εντοπισμό τους ένα πολύ δύσκολο έργο (Uematsu et al, 2017).

Προκειμένου να διατηρηθεί η εξέλιξη προς ευέλικτα, προγραμματιζόμενα και αυτόνομα συστήματα, τα οπτικά δίκτυα είναι σημαντικό να υποστηρίζουν αυτόνομη διάγνωση και λειτουργία. Η ενσωματωμένη τηλεμετρία και η ανάλυση δικτύων είναι ζωτικής σημασίας

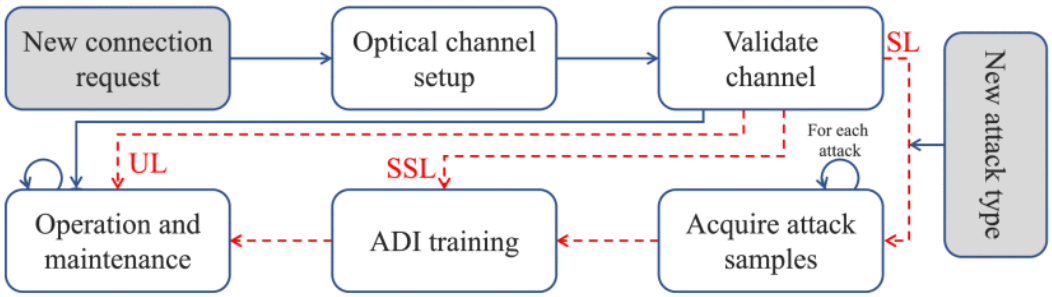
για την πραγματοποίηση του βρόχου ελέγχου Observe-Analyze-Act και τη βελτίωση της απόδοσης του δικτύου, την αποδοτικότητα κόστους και την ασφάλεια. Ο πρόσφατος πολλαπλασιασμός των τεχνικών μηχανικής μάθησης (ML) σε πολλές πτυχές της οπτικής δικτύωσης έφερε νέες και ισχυρές μεθόδους για γνωστική και αυτοματοποιημένη διαχείριση της ασφάλειας του οπτικού δικτύου. Αυτές οι τεχνικές έχουν αποδειχθεί επιτυχημένες, π.χ. στην ανίχνευση μη εξουσιοδοτημένων σημάτων στο δίκτυο ή στον εντοπισμό επιθέσεων εμπλοκής και πόλωσης. Ωστόσο, η πρακτικότητα τέτοιων λύσεων και η ενσωμάτωσή τους στα υπάρχοντα συστήματα διαχείρισης δικτύου παραμένει ανοιχτό ζήτημα. Οι προκλήσεις που σχετίζονται με την απόδοση εργαλείων που βασίζονται σε ML για διαγνωστικά επιθέσεων περιλαμβάνουν την ακρίβειά τους και τη λεπτομερή πληροφόρηση που δύνανται να παρέχουν. Οι προκλήσεις που σχετίζονται με την ενσωμάτωσή τους με τυπικά πλαίσια διαχείρισης δικτύου περιλαμβάνουν την επιλογή πρόσθετου λογισμικού που είναι απαραίτητο να ενσωματωθεί στον κύκλο ελέγχου, τις διαθέσιμες επιλογές αρχιτεκτονικής λογισμικού για την εφαρμογή τους και τις επιπτώσεις αυτών των αρχιτεκτονικών στις απαιτήσεις του συστήματος παρακολούθησης όσον αφορά τη χωρητικότητα και τα γενικά έξοδα επικοινωνίας (Uematsu et al, 2017).

4.3 Δίκτυο και προσεγγίσεις αυθεντικοποίησης

Η ανίχνευση και η ταυτοποίηση των επιθέσεων είναι πιθανό να πραγματοποιηθεί με διαφορετικές τεχνικές ML. Τα οφέλη και τα μειονεκτήματα κάθε τεχνικής ML είναι απαραίτητο να εκτιμηθούν λαμβάνοντας υπόψη όχι μόνο την ακρίβεια των μοντέλων, αλλά και τις επιπτώσεις τους στη λειτουργία του δικτύου.

Οι κύριες διαφορές μεταξύ τεχνικών μάθησης υπό επίβλεψη, ημι-επίβλεψης και χωρίς επίβλεψη βρίσκονται στις απαιτήσεις δεδομένων και στις διαδικασίες κατάρτισης. Η κατανόηση του τρόπου με τον οποίο αυτά τα μοντέλα έχουν την δυνατότητα να ενσωματωθούν στο Network Management System (NMS) είναι θεμελιώδους σημασίας για αποτελεσματική και αξιόπιστη αξιολόγηση ασφάλειας. Η Εικόνα 12 απεικονίζει τα βήματα που ενυπάρχουν στα Supervised Learning (SL), Semi-Supervised Learning (SSL) and Unsupervised Learning (UL) για να ικανοποιήσουν ένα νέο αίτημα σύνδεσης ή έναν πρόσφατα ανακαλυφθέντα τύπο επίθεσης φυσικού επιπέδου. Μια τυπική ενέργεια NMS κατά την άφιξη ενός νέου αιτήματος σύνδεσης είναι η δημιουργία ενός νέου οπτικού καναλιού, το οποίο περιλαμβάνει διάφορες εκτιμήσεις καναλιών και αποφάσεις ανάθεσης πόρων. Μόλις ρυθμιστεί το κανάλι, ένα βήμα επικύρωσης καναλιού επαληθεύει εάν οι συνθήκες φυσικού επιπέδου είναι κατάλληλες και, αν ναι,

συλλέγει ένα σύνολο δειγμάτων OPM που θεωρούνται ως κανονικές συνθήκες λειτουργίας (NOC), δηλ. Αντιπροσωπεύουν τη βασική απόδοση OCh σε συνθήκες χωρίς επίθεση. Τα δείγματα NOC χρησιμοποιούνται για εκπαίδευση σε SSL και ως βάση για SL. Εάν χρησιμοποιείται SL, ένα αντιπροσωπευτικό σύνολο δεδομένων με απόδοση καναλιού παρουσία όλων των γνωστών τεχνικών επίθεσης πρέπει επίσης να συλλεχθεί και να επισημανθεί για σκοπούς εκπαίδευσης ADI. Αυτό τείνει να προκαλέσει πολυπλοκότητες στο σχεδιασμό και την εκτέλεση των πειραμάτων και μπορεί να καθυστερήσει τη φάση λειτουργίας του OCh. Για το SSL, το βήμα συλλογής δεδομένων συγκεκριμένης επίθεσης παρακάμπτεται και το μοντέλο ξανά εκπαιδεύεται χρησιμοποιώντας μόνο τα δείγματα NOC. Το UL παραλείπει και τα δύο βήματα και προχωρά στη λειτουργία όπως πριν από τη νέα σύνδεση ή τον τύπο επίθεσης (Furdek et al, 2020).



Εικόνα 13: Βήματα που έχουν ληφθεί από SL, SSL και UL για να ικανοποιήσουν ένα νέο αίτημα σύνδεσης ή έναν τύπο επίθεσης φυσικού επιπέδου που ανακαλύφθηκε πρόσφατα. Οι συνεχείς γραμμές αντιπροσωπεύουν την παραδοσιακή διαδικασία δημιουργίας, λειτουργίας και διατήρησης μιας σύνδεσης. Οι διακεκομμένες γραμμές αντιπροσωπεύουν τα βήματα που είναι εγγενή στις τεχνικές ML (Furdek et al, 2020).

Οι κύριες ιδιότητες των τεχνικών ML που εξετάστηκαν συνοψίζονται στον Πίνακα 3 και επισημαίνονται ως θετικές, αρνητικές και κρίσιμες. Όλες οι τεχνικές απαιτούν απόκτηση δεδομένων NOC και πραγματοποιούν ανίχνευση επίθεσης, δηλαδή ταξινομούν την κατάσταση OCh μεταξύ της κανονικής και της υπό επίθεσης. Λόγω της επισήμανσης των δειγμάτων επίθεσης, μόνο τα μοντέλα SL είναι σε θέση να εκτελέσουν ταυτοποίηση επίθεσης, δηλαδή να ταξινομήσουν τη συγκεκριμένη τεχνική επίθεσης (και την έντασή της) διαταράσσοντας το OCh (Furdek et al, 2020).

Πίνακας 3: Περίληψη των πλεονεκτημάτων και των μειονεκτημάτων της εποπτευόμενης μάθησης (SL), της ημι-εποπτευόμενης μάθησης (SSL) και της μη εποπτευόμενης μάθησης (UL) για ADI (Furdek et al, 2020).

Property	SL	SSL	UL
Requires NOC data	Yes	Yes	Yes
Attack detection	Yes	Yes	Yes
Attack identification	Yes	No	No
Requires attack-specific labeled data	Yes	No	No
Training complexity	High	Low	None
Re-training for new OChs	Yes	Yes	No
Inference complexity	Low	Low	High
Requires prior samples	No	No	Yes
Supports stateless operation	Yes	Yes	Yes

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Είναι γεγονός ότι οι έννοιες PUF για ηλεκτρονικές εφαρμογές είναι πολλές και δύνανται εύκολα να ενσωματωθούν και να ψηφιοποιηθούν. Ωστόσο, θα ήταν φρόνιμο να διερευνηθούν τα πλεονεκτήματα διαφορετικών PUF και πιο σύγχρονων εννοιών, όπως οι οπτικές, για κάθε δεδομένη κατάσταση εφαρμογής πριν από τη χρήση οποιουδήποτε PUF. Η επιλογή της βέλτιστης PUF είναι σημαντικό να γίνει σε πολλά ξεχωριστά επίπεδα. Πιο συγκεκριμένα, είναι απαραίτητο να επιλεγεί η σωστή «οικογένεια» του PUF για μια συγκεκριμένη κατάσταση.

Ακόμη, στην παρούσα μελέτη αναλύεται ένα ευέλικτο και οπτικό σύστημα ελέγχου ταυτότητας βασισμένο σε φυσικές απροσδιόριστες λειτουργίες (PUF). Προσθέτοντας ένα στρώμα μικροσκοπικών σωματιδίων που σε μια στοχαστική διαδικασία σχηματίζουν ένα μοναδικό μοτίβο σε έναν κωδικό QR δείχνουν ότι οι ετικέτες PUF παράγονται εύκολα μαζικά.

Επιπρόσθετα, αποδεικνύονται μειονεκτήματα του συστήματος οπτικής κρυπτογράφησης και προτείνεται ένα προηγμένο σχήμα κρυπτογράφησης και ελέγχου ταυτότητας με βάση την ανάλυση. Παρουσιάστηκε ένα σχήμα οπτικής ιεραρχικής πιστοποίησης βασισμένο στην αρχή της παρεμβολής και τη συνάρτηση κατακερματισμού. Ένα συμβολόμετρο δύο δοκών υιοθετείται ως η κύρια μονάδα για την ολοκλήρωση της διαδικασίας ελέγχου ταυτότητας. Εν τω μεταξύ, σε σύγκριση με ορισμένα κοινά συστήματα ασφαλείας ελέγχου ταυτότητας, τα κύρια πλεονεκτήματα της προτεινόμενης μεθόδου μπορούν να συναχθούν ως εξής: δεν είναι δυνατόν να ελεγχθεί εάν ο χρήστης είναι νόμιμος, αλλά και να επαναληφθεί το επίπεδο ταυτότητάς του. Επιπλέον, οι πολλαπλοί παράγοντες που επαληθεύουν τον μηχανισμό παρέχουν σχετικά υψηλότερη δύναμη ασφάλειας.

Επίσης, αναλύεται ένα πλαίσιο βασισμένο σε μηχανική μάθηση (ML) για γνωστικά και αυτόνομα διαγνωστικά ασφάλειας της ασφάλειας φυσικού επιπέδου σε οπτικά δίκτυα. Το πλαίσιο περιλαμβάνει στοιχεία για τον εντοπισμό επιθέσεων που μπορούν να αξιοποιήσουν την εποπτευόμενη, ημι-εποπτευόμενη και χωρίς επίβλεψη μάθηση για τον εντοπισμό επιθέσεων και, κατά περίπτωση, τον προσδιορισμό του τύπου και της έντασής τους. Τέλος, σημειώνεται ότι μελλοντικά έργα και ανοιχτές ερωτήσεις περιλαμβάνουν μια βαθύτερη διερεύνηση της εύρειας πλατφόρμας παρακολούθησης σε παραλλαγές των «φυσιολογικών» συνθηκών αστοχίας (δηλαδή ικανότητα σωστής διάκρισης μεταξύ επιθέσεων και αποτυχιών).

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενόγλωσσος όρος	**Ελληνικός Όρος**
Act	Δρω
Analyze	Αναλύω
Observe	Παρακολουθώ
Inkjet	Με μελάνι
Volume	Όγκος
Weight	Βάρος
Smartphone	Έξυπνο κινητό
Hash	Κατακερματισμός
Function	Συνάρτηση

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

PUF	Physical Unclonable Function
rPUF	Reconfigurable PUF
PPUF	Public PUF
SRAM PUF	Static Random Access Memory PUF
STT-MRAM PUF	Spin-transfer-torque magnetic RAM PUF
CRP	Challenge Response Pair
PCM	Phase Change Memory
RAM	Random Access Memory
SIMPL	Simulation Possible but Laborious
RSA	Rivest-Shamir-Adleman
PVA	PolyVinyl Alcohol
g	Gram
mm	Millimetre
m^2	Meter x Meter
μm	Micrometre
CMOS	Complementary metal–oxide–semiconductor
PNG	Portable Network Graphics
DRPE	Double Random Phase Encoding
RPM	Random Phase-only Mask
JTC	Joint Transform Correlator
JPS	Joint Power Spectrum
POM	Phase-Only Mask
PST	Phase-Shifting Technique
CCD	Charge-Couple Device
SF	Spatial Filter
L	Lens
P	Polarizer
WP	Wave Plate
LCTV	Liquid-Crystal Television Display
DF	Digital Fingerprint
SLM	Spatial Light Modulator
ML	Machine Learning
NMS	Network Management System
SL	Supervised Learning

SSL	Semi-Supervised Learning
UL	Unsupervised Learning
OPM	Optical Performance Monitoring
NOC	Normal Operating Conditions
OCh	Optical Channel
ADI	Attack Detection and Identification
QR	Quick Response

ΑΝΑΦΟΡΕΣ

[1] Arppe, R.; Sørensen, T. J., Physical Unclonable Functions Generated Through Chemical Methods for Anti-Counterfeiting. Nature Reviews Chemistry 2017, 1 (4), 31.

[2] Chen, Z. Liu, L. Zhu, C. Tanougast, W. Blondel, C. Asymmetric color cryptosystem using chaotic Ushiki map and equal modulus decomposition in fractional Fourier transform domain, Opt. Lasers Eng, 2019, 7–15.

[3] Eqop.phys.strath.ac.uk. 2021. Optical Pattern Formation – EQOP Group @ Strathclyde Physics. [online] Available at: <https://eqop.phys.strath.ac.uk/nonlinear-photonics/pattern-formation/optical-pattern-formation/> [Accessed 12 October 2021].

[4] Fraser, J. "Exploiting Random Patterns of Optically Readable Materials to Ensure Authentication of Documents, Media & Substrates," 2008 IEEE Conference on Technologies for Homeland Security, 2008, pp. 438-443, doi: 10.1109/THS.2008.4534492.

[5] Furdek, C., Natalino, F., Lipp, D., Hock, A., Giglio D, Schiano, M., "Machine Learning for Optical Network Security Monitoring: A Practical Perspective," in Journal of Lightwave Technology, vol. 38, no. 11, pp. 2860-2871, 2020, doi: 10.1109/JLT.2020.2987032.

[6] He, W., Peng, X., Meng, X. and Liu, X., Optical hierarchical authentication based on interference and hash function. *Applied Optics*, 51(32), 2012, p.7750.

[7] Lenstra, K.,. Verheul, R.,“Selecting cryptographic key sizes,” J. Cryptography 14(4), 255–293,2016 .5–460.

[8] Liao, Z.; Tropiano, M.; Mantulnikovs, K.; Faulkner, S.; Vosch, T.; Just Sørensen, T., Spectrally Resolved Confocal Microscopy Using Lanthanide Centred Near-IR Emission. Chemical Communications 2015, 51 (12), 2372-2375.

[9] McGrath, T., Bagci, I., Wang, Z., Roedig, U. and Young, R., A PUF taxonomy. Applied Physics Reviews, 6(1), 2019. p.011303.

[10] Reuhrmair, H., Busch, S., Katzenbeisser, U. “Strong PUFs: Models, constructions, and security proofs,” in Proceedings of Towards Hardware-Intrinsic Security: Foundations Practice, 2010, pp. 79–96.

[11] Refregier, B. Javidi, P., Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett. 20 (7), 1995, 767–769.

[12] Tabbara, R., Tabbara, M. and Sørensen, T., Versatile and Validated Optical Authentication System Based on Physical Unclonable Functions. ACS Applied Materials & Interfaces, 11(6), 2019. pp.6475-6482.

[13] Uematsu, H., Hirota, T., Kawano, T., Kiyokura, and Manabe, T., “Design of a temporary optical coupler using fiber bending for traffic monitoring,” IEEE Photonics J., vol. 9, no. 6, pp. 1–13, Dec 2017, DOI: 10.1109/JPHOT.2017.2762662.

[14] Verbauwhede, I., Maes, R., “Physically unclonable functions: Manufacturing variability as an unclonable device identifier,” in Proceedings of the ACM Great Lakes Symposium on VLSI (GLSVLSI), 2011, pp. 4526A.

[15] Willers, O., Huth, C., Guajardo, J., Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 591–602.

[16] Xiong, J. Du, C. Quan, J. Optical encryption and authentication scheme based on phase-shifting interferometry in a joint transform correlator, Optics & Laser Technology, Volume 126, 2020.

[17] Zhang Y. and Wang, B. “Optical image encryption based on interference,” Opt. Lett. 33, 2008, pp. 2443–2445.