Μελέτη και ανάλυση των secure sketches συναρτήσεων για τη διαχείριση απόρρητων βιομετρικών δεδομένων σε κρυπτογραφικές εφαρμογές

Σοφία Σακκά

Διπλωματική Εργασία

Επιβλέπουσα: Βασιλική Λιάγκου

Άρτα, Ιούλιος 2021

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

DEPARTMENT OF UNIVERSITY OF IOANNINA


ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ Η/Υ & ΠΛΗΡΟΦΟΡΙΚΗΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

Ευχαριστίες

Θα ήθελα να ευχαριστήσω θερμά την καθηγήτριά μου κ. Βασιλική Λιάγκου για τη συνεχή καθοδήγηση και υποστήριξη καθ' όλη τη διάρκεια της εργασίας, καθώς και για την εμπιστοσύνη που μου έδειξε.

Θα ήθελα επίσης να ευχαριστήσω τους συμφοιτητές και φίλους πλέον για την αμερόληπτη βοήθειά τους σε οποιαδήποτε δυσκολία. Και, τέλος την οικογένειά μου για την υπομονή της.

Άρτα, 2021

Σοφία Σακκά

Περίληψη

Η ασφάλεια ενός χρήστη, όσον αφορά την πρόσβαση σε ένα σύστημα, βασίζεται σε ισχυρούς κωδικούς πρόσβασης. Όσο πιο τυχαίοι είναι αυτοί οι κωδικοί τόσο πιο ασφαλή καθιστούν την αυθεντικοποίηση του χρήστη . Η βιομετρία προσφέρει ένα σαφές πλεονέκτημα για τη δημιουργία τέτοιων κωδικών. Ωστόσο, η μετάδοση και η αποθήκευσή τους αποτελούν σημαντικά ζητήματα καθώς τα βιομετρικά δεδομένα είναι στενά συνδεδεμένα με την ταυτότητα του χρήστη και γι' αυτό θα πρέπει να διασφαλιστεί το απόρρητο της πληροφορίας που φέρουν. Η διπλωματική εργασία εστιάζει στα παραπάνω προβλήματα μελετώντας δύο κρυπτογραφικά σχήματα, τα ασφαλή σκίτσα (secure sketches) και τους εξαγωγείς ασάφειας (fuzzy extractors), τα οποία έχουν την ιδιότητα να μετασχηματίζουν και να κωδικοποιούν τα βιομετρικά δεδομένα ενός χρήστη με σκοπό να γίνεται η ταυτοποίησή τους χωρίς την επαναφορά τους στην αρχική μορφή. Επιπλέον, μελετάται η αρχιτεκτονική των βιομετρικών συστημάτων, καθώς και ευπάθειές τους που μπορούν να αποτελέσουν σημεία επίθεσης για κακόβουλες οντότητες. Τέλος, γίνεται εφαρμογή των παραπάνω κρυπτογραφικών σχημάτων, καθώς και επεκτάσεών τους, για τον απομακρυσμένο έλεγχο πρόσβασης.

Λέξεις Κλειδιά: κρυπτογραφία, ασφάλεια, βιομετρία, βιομετρικά δεδομένα, απομακρυσμένος έλεγχος πρόσβασης

Abstract

A user's security in accessing a system is based on strong passwords. The more random these passwords are, the more secure they are in authenticating the user. Biometrics offers a clear advantage in generating such codes. However, their transmission and storage are important issues as biometric data is closely linked to the identity of the user and therefore the confidentiality of their information should be ensured. The dissertation focuses on the above problems by studying two cryptographic schemes, secure sketches and fuzzy extractors, which can transform and encode a user's biometric data in order to identify them. without restoring them to their original form. In addition, the architecture of biometric systems is studied, as well as their vulnerabilities that can be attack points for malicious entities. Finally, the above cryptographic schemes, as well as their extensions, are applied for remote access control.

Keywords: cryptography, security, biometrics, biometric data, remote access control, secure sketches, fuzzy exctractors

Πίνακας περιεχομένων

Κεφάλαιο 1. Εισαγωγή

1.1 Αντικείμενο της διπλωματικής

Η παρούσα διπλωματική εργασία στοχεύει στην διερεύνηση μιας γενικής προσέγγισης για τη διαχείριση απόρρητων βιομετρικών δεδομένων σε κρυπτογραφικές εφαρμογές. Η γενίκευση αυτή βασίζεται με δυο προσεγγίσεις: μέσω της προσπάθειας ελαχιστοποίησης των υποθέσεων που αφορούν τα δεδομένα και μέσω της παρουσίασης τεχνικών που είναι ευρέως εφαρμόσιμες όπου χρησιμοποιούνται βιομετρικά δεδομένα σε ψηφιακή μορφή.

Επειδή τα βιομετρικά στοιχεία προέρχονται από διάφορες πηγές που είναι ως επί το πλείστον εκτός του ελέγχου κανενός, είναι φρόνιμο να γίνουν όσο το δυνατόν λιγότερες υποθέσεις για το πώς κατανέμονται. Ειδικότερα, ένας αντίπαλος μπορεί να γνωρίζει περισσότερα για την κατανομή από τους σχεδιαστές και τους χρήστες ενός συστήματος. Φυσικά, κάποιος μπορεί να προσπαθήσει να μετρήσει μερικές ιδιότητες μιας βιομετρικής κατανομής, αλλά θα ήταν επικίνδυνο το να βασιστεί σε τέτοιου είδους μετρήσεις για την ανάλυση της ασφάλειας, επειδή ο αντίπαλος μπορεί να διαθέτει ακόμη πιο ακριβείς μετρήσεις. Για παράδειγμα, ακόμη και αν υποτεθεί ότι κάποια ιδιότητα ενός βιομετρικού συμπεριφέρεται σύμφωνα με μια κατανομή (π.χ. κάποια διακριτοποίηση της κανονικής κατανομής), θα μπορούσε κανείς να προσδιορίσει τη μέση τιμή της κατανομής μετά τη λήψη ενός αριθμού δειγμάτων. Ένας αντίπαλος, λοιπόν, μπορεί να πάρει περισσότερες μετρήσεις, και έτσι να προσδιορίσει τη μέση τιμή με μεγαλύτερη ακρίβεια.

Αντί να υποτεθεί ότι ορισμένα στατιστικά στοιχεία σχετικά με τα βιομετρικά δεδομένα εισόδου είναι διαθέσιμα, υποθέτουμε μόνο ότι η είσοδος είναι απρόβλεπτη: δηλαδή, ότι αν σε ένα αντίπαλο επιτραπεί να κάνει μόνο μια υπόθεση σχετικά με την τιμή της εισόδου, η πιθανότητα να είναι σωστή είναι 2^m για κάποιο m. Πρόκειται για την

ελάχιστη υπόθεση στις εφαρμογές που θεωρούμε. Πράγματι, αν είναι εύκολο να μαντέψει κάποιος την είσοδο, τότε δεν μπορεί κανείς να τη χρησιμοποιήσει για να αντλήσει, ας πούμε, ένα μυστικό κλειδί για κρυπτογράφηση ή έναν απομακρυσμένο έλεγχο ταυτότητας. Φυσικά, ο καθορισμός της ακριβούς τιμής του m μπορεί από μόνο του να είναι μια πρόκληση. Ωστόσο, ένα κάτω φράγμα για το m είναι αναγκαίο για κάθε είδος ισχυρισμών ασφαλείας.

Ομοίως, ενώ είναι εφικτή κάποια κατανόηση των σφαλμάτων στις μετρήσεις βιομετρικών, προτιμούμε να ελαχιστοποιηθούν οι παραδοχές που κάνουμε σχετικά με αυτά τα σφάλματα. Υποθέτουμε μόνο ότι μεταγενέστερες μετρήσεις γίνονται σε μια δεδομένη, επιτρεπτή απόσταση από τις μετρήσεις που ελήφθησαν κατά την εγγραφή.

Η ευρεία εφαρμογή των προσεγγίσεων που παρουσιάζονται εδώ πηγάζει από την αρχική παρατήρηση ότι πολλές προηγούμενες λύσεις για συγκεκριμένα προβλήματα ασφαλείας που βασίζονται σε θορυβώδη δεδομένα (συμπεριλαμβανομένων των βιομετρικών δεδομένων) είχαν κοινές βασικές τεχνικές και αναλύσεις. Αντί για σχεδιασμό λύσεων για κάθε συγκεκριμένη ρύθμιση που προκύπτει, φαίνεται χρήσιμο να εξεταστούν οι κοινές ιδιότητες που έχουν οι εν λόγω λύσεις, και να ενσωματωθούν σε αρχέτυπα που να μπορούν να χρησιμοποιηθούν σε διάφορα πλαίσια.

Υπάρχει ένα αρκετά μεγάλο κομμάτι βιβλιογραφίας που μπορεί να παρέχει ασφάλεια αν υπάρχει ένα μυστικό, ομοιόμορφα τυχαίο και αξιόπιστα αναπαραγόμενη σειρά από bits (το οποίο μπορεί να χρησιμοποιηθεί για παράδειγμα σαν μυστικό κλειδί, ή σαν είσοδος για την παραγωγή ενός δημοσίου/προσωπικού κλειδιού). Συνεπώς, αν τα βιομετρικά δεδομένα μπορούν να μετατραπούν σε τέτοιες σειρές από bits, τότε μια ευρεία γκάμα κρυπτογραφικών τεχνικών μπορεί να χρησιμοποιηθεί ώστε να παρέχει ασφάλεια από βιομετρικά. Για να γίνει αυτό, παρουσιάζουμε έναν εξαγωγέα ασαφών πρότυπων όρων (primitive term fuzzy extractor). Και επιπλέον, ως ένα βήμα για την κατασκευή της εξαγωγών ασάφειας, και ως ένα ενδιαφέρον αντικείμενο από μόνο του, παρουσιάζουμε ένα άλλο θεμελιακό στοιχείο, που ονομάζεται ασφαλές σκίτσο (secure sketch).

Επειδή οι βιομετρικές πληροφορίες έχουν και διαφορετικά μοτίβα λάθους δεν υποθέτουμε καμία συγκεκριμένη έννοια ομοιότητας-απόστασης μεταξύ διαφορετικών μετρήσεων του ίδιου βιομετρικού στοιχείου. Αντιθέτως, στον καθορισμό των θεμελιακών στοιχείων μας, απλά υποθέτουμε ότι το αρχικό βιομετρικό προέρχεται από κάποιο μετρικό χώρο, και ότι μία προσέγγισή του θα απέχει το πολύ t από το αρχικό σε

αυτό το χώρο. Θεωρούμε συγκεκριμένες μετρικές μόνο κατά την κατασκευή συγκεκριμένων κατασκευών, τις οποίες παρέχουμε για την Hamming απόσταση, την απόσταση συνόλων (set distance) και την απόσταση σύνταξης (edit distance). Κατασκευές για άλλες έννοιες απόστασης είναι επίσης δυνατές, και ορισμένες τέτοιες υπάρχουν στη βιβλιογραφία. Φυσικά, οι βιομετρικά μετρήσεις συχνά πρέπει να υποστούν επεξεργασία πριν ενσωματωθούν σε κάποιο βολικό μετρικό χώρο. Για παράδειγμα, τεχνικές, όπως η Iris Code μετατρέπουν τις εικόνες της ίριδας σε σειρές δεδομένων στο χώρο Hamming.

1.2 Οργάνωση του τόμου

Στο 2ο το κεφάλαιο αναφέρονται κάποιοι βασικοί ορισμοί στο πεδίο της διπλωματικής εργασίας.

Στο 3ο κεφάλαιο παρουσιάζονται τα χαρακτηριστικά των βιομετρικών δεδομένων και των βιομετρικών συστημάτων, καθώς και η χρήση τους στην κρυπτογραφία.

Στο 4ο κεφάλαιο αυτό αναφέρονται τα στάδια της επεξεργασίας των βιομετρικών δεδομένων για αναγνώριση και αυθεντικοποίηση του χρήστη.

Στο 5ο περιγράφονται βιομετρικοί αλγόριθμοι που χρησιμοποιούνται για την επεξεργασία των βιομετρικών δεδομένων με σκοπό τη χρήση τους για αναγνώριση και αυθεντικοποίηση, πως τα δεδομένα αυτά μετασχηματίζονται και ποια είναι τα προβλήματα που προκύπτουν.

Στο 6ο κεφάλαιο παρουσιάζονται αναλυτικά οι επιθέσεις στις οποίες μπορεί να είναι ευάλωτο ένα βιομετρικό σύστημα και οι τρόποι αναγνώρισής τους μέσω μοντέλων απειλών.

Στο 7ο κεφάλαιο περιγράφονται οι τεχνολογίες προστασίας των βιομετρικών δεδομένων που χρησιμοποιεί η κρυπτογραφία και στο 8ο κεφάλαιο γίνεται η εφαρμογή των τεχνολογιών αυτών για απομακρυσμένο έλεγχο πρόσβασης.

Τέλος, στο 9ο κεφάλαιο έχουμε μία σύνοψη της εργασίας, αναφέρονται τα συμπεράσματά μας και πιθανές εφαρμογές των κρυπτογραφικών σχημάτων που αναλύθηκαν.

Κεφάλαιο 2. Βασικοί ορισμοί

Σε αυτό το κεφάλαιο αναφέρονται κάποιοι βασικοί ορισμοί για την κατανόηση της παρούσας εργασίας.

2.1 Ταυτοποίηση και Αυθεντικοποίηση

Με τον όρο ταυτοποίηση εννοούμε τη συσχέτιση ενός ατόμου με μια ταυτότητα και την επιβεβαίωση ή μη, ότι αυτή η ταυτότητα είναι αυθεντική . Ενώ με τον όρο αυθεντικοποίηση εννοούμε τη διαδικασία επιβεβαίωσης της ταυτότητας του ατόμου .
Για να γίνει η ταυτοποίηση και αυθεντικοποίηση χρησιμοποιούνται οι ακόλουθες παραδοσιακές τεχνικές (1) (2) :

- Κάτι που κατέχουμε: Αναφέρεται σε κάποιο φυσικό αντικείμενο, το οποίο μπορεί να είναι ένα διαβατήριο, στο οποίο η ταυτοποίηση δεν γίνεται αυτόματα και απαιτείται η ανθρώπινη παρέμβαση, ή μια μαγνητική κάρτα, με την οποία γίνεται αυτόματη ταυτοποίηση μέσω ενός συστήματος/ υπολογιστή. Η προσέγγιση αυτή είναι γνωστή ως παράγων κατοχής (possession factor).
- Κάτι που γνωρίζουμε: Αναφέρεται σε κάποιο “μυστικό”, το οποίο για κάθε άτομο να είναι συγκεκριμένο, όπως ένας κωδικός (PIN). Η προσέγγιση αυτή είναι γνωστή ως παράγων γνώσης (knowledge factor).
- Κάτι που είμαστε: Αναφέρεται στην μέτρηση ενός ή περισσοτέρων βιολογικών χαρακτηριστικών, όπως στα δακτυλικά αποτυπώματα και την υπογραφή. Η προσέγγιση αυτή είναι γνωστή και ως παράγων ύπαρξης (being factor).

Παρατηρούμε ότι στις δύο πρώτες περιπτώσεις υπάρχουν τρωτά σημεία καθώς τα αντικείμενα ή οι κωδικοί που χρησιμοποιούνται μπορούν να κλαπούν, πλαστογραφηθούν ή να ξεχαστούν. Για τα βιολογικά χαρακτηριστικά όμως δεν ισχύει αυτό. Περισσότερο πρόβλημα αποτελεί για παράδειγμα η αλλοίωσή τους από το χρόνο.

2.2 Βιομετρία

Η λέξη βιομετρία προέρχεται από τις δύο ελληνικές λέξεις την "βίος" που σημαίνει ζωή και την "μετρικός" που σημαίνει μια μέτρηση (3) (4). Αναφέρεται στην αναγνώριση ενός ατόμου μέσω των βιομετρικών του χαρακτηριστικών. Αυτά μπορεί να είναι χαρακτηριστικά που αφορούν είτε την ανατομία είτε τη συμπεριφορά του ατόμου. Αυτή

η τεχνική αναγνώρισης είναι προφανώς πιο αξιόπιστη σε σχέση με παραδοσιακά συστήματα ασφάλειας μιας και τα χαρακτηριστικά ενός ατόμου είναι μοναδικά.

2.3 Βιομετρικά χαρακτηριστικά

Βιομετρικά χαρακτηριστικά είναι τα ανθρώπινα γνωρίσματα που συνθέτουν την ταυτότητα ενός ατόμου, όπως τα χαρακτηριστικά του προσώπου, τα μάτια, ακόμη και ο σφυγμός. Στα βιομετρικά χαρακτηριστικά συμπεριλαμβάνονται επίσης η συμπεριφορά ή οι επαναλαμβανόμενες κινήσεις που χαρακτηρίζουν ένα άτομο και μέσα από αυτά μπορούμε να το αναγνωρίσουμε. Τα συγκεκριμένα γνωρίσματα μπορούν να χρησιμοποιηθούν για να καθορίσουν την ταυτότητά μας.

2.4 Βιομετρικό Σύστημα

Ένα βιομετρικό σύστημα είναι ουσιαστικά ένα σύστημα αναγνώρισης προτύπων που λειτουργεί αποκτώντας βιομετρικά δεδομένα από ένα άτομο, στη συνέχεια εξάγει ένα σύνολο χαρακτηριστικών από τα ληφθέντα δεδομένα και τέλος συγκρίνει αυτό το σύνολο με το εγγεγραμμένο πρότυπο που βρίσκεται στη βάση δεδομένων του συστήματος. Ανάλογα με το πλαίσιο εφαρμογής, ένα βιομετρικό σύστημα μπορεί να λειτουργεί είτε σε λειτουργία επαλήθευσης είτε σε λειτουργία αναγνώρισης. Έχει σχεδιαστεί χρησιμοποιώντας τις ακόλουθες τέσσερις κύριες ενότητες: (i) μονάδα αισθητήρα, (ii) μονάδα εξαγωγής χαρακτηριστικών, (iii) μονάδα αντιστοίχισης και (iv) μονάδα βάσης δεδομένων συστήματος (5).

Κεφάλαιο 3. Βιομετρικά Δεδομένα

Στο κεφάλαιο παρουσιάζονται τα χαρακτηριστικά των βιομετρικών δεδομένων και των βιομετρικών συστημάτων καθώς και η χρήση τους στην κρυπτογραφία.

3.1 Χαρακτηριστικά βιομετρικών δεδομένων

Για την ευκολία της χρήσης τους αλλά και για καλύτερα αποτελέσματα των μεθόδων αναγνώρισής τους, τα βιομετρικά δεδομένα θα πρέπει να πληρούν κάποια βασικά χαρακτηριστικά. Αυτά είναι τα εξής (6):

- Οικουμενικότητα (Universality):το βιομετρικό χαρακτηριστικό θα πρέπει να είναι υπαρκτό σε όλα τα άτομα.
- Μοναδικότητα (Distinctiveness/Uniqueness): κανένα άτομο δεν έχει ίδιο βιομετρικό χαρακτηριστικό με κανένα άλλο.
- Σταθερότητα (Permanence/Stability): το βιομετρικό χαρακτηριστικό θα πρέπει να παραμένει αναλύωτο, όσον αφορά το κριτήριο αντιστοίχισης τουλάχιστον για μία χρονική περίοδο.
- Συλλεκτικότητα (Collectability): το χαρακτηριστικό θα πρέπει να μπορεί να μετρηθεί ποσοτικά

Σε ένα βιομετρικό σύστημα αναγνώρισης θα πρέπει να συμπεριληφθούν επίσης και τα παρακάτω ζητήματα (6), (7):

- Επίδοση (Performance): αναφέρεται στην επιτεύξιμη ακρίβεια και ταχύτητα αναγνώρισης, στους πόρους που απαιτούνται για την επίτευξη της επιθυμητής απόδοσης, καθώς και στους λειτουργικούς και περιβαλλοντικούς παράγοντες που την επηρεάζουν.
- Αποδοχή (Acceptability): αναφέρεται στο κατά πόσο οι άνθρωποι είναι πρόθυμοι να αποδεκτούν τη χρήση ενός χαρακτηριστικού τους στην καθημερινή τους ζωή.
- Αντοχή στην πλαστογράφηση (Forgeresistance/Circumvention): απεικονίζει πόσο εύκολα το σύστημα μπορεί να ξεγελαστεί από τη χρησιμοποίηση δόλιων μεθόδων.

3.2 Βιομετρικά δεδομένα ως μέσο αυθεντικοποίησης

Αυθεντικοποίηση είναι η διαδικασία που διαπιστώνει την πραγματική ταυτότητα ενός χρήστη. Ωστόσο, η αναγνώριση ενός χρήστη και ο έλεγχος πρόσβασης απαιτούν ύψιστη ασφάλεια μιας και μπορεί να αφορούν σχέσεις πολιτείας-πολίτη, απομακρυσμένες εμπορικές συναλλαγές, εξοπλισμούς ασφαλείας και εγκληματολογικές έρευνες.

Τα βιομετρικά δεδομένα άρχισαν λοιπόν να υιοθετούνται ως ένας τρόπος για να καταστεί δυνατή η ισχυρή, κρυπτογραφικά ασφαλής πιστοποίηση των ανθρώπινων χρηστών χωρίς να απαιτείται από αυτούς να θυμούνται ή να αποθηκεύουν παραδοσιακά κρυπτογραφικά κλειδιά. Το σώμα μας παρέχει μοναδικά γνωρίσματα που θα μπορούσαν να χρησιμοποιηθούν για να αποδείξουμε την ταυτότητά μας, όπως για παράδειγμα, τα δακτυλικά μας αποτυπώματα, η γεωμετρία των χεριών, η ανάγνωση της ίριδας κ.α.. Αυτός ο τρόπος πιστοποίησης είναι πιο εύχρηστος καθώς δεν απαιτεί την αποστήθιση κάποιου κωδικού και φυσικά πιο ασφαλής καθώς το χαρακτηριστικό είναι μοναδικό και ο χρήστης το φέρει πάντα πάνω του.

Προτού μπορέσουν να χρησιμοποιηθούν τέτοια δεδομένα σε υπάρχοντα κρυπτογραφικά πρωτόκολλα, πρέπει να αντιμετωπιστούν δύο ζητήματα: πρώτον, τα βιομετρικά δεδομένα δεν κατανέμονται ομοιόμορφα και ως εκ τούτου δεν προσφέρουν αποδεδειγμένες εγγυήσεις ασφαλείας εάν χρησιμοποιούνται για παράδειγμα ως κλειδί για μια ψευδοτυχαία συνάρτηση. Ενώ το πρόβλημα της ανομοιομορφίας μπορεί να αντιμετωπιστεί χρησιμοποιώντας μια συνάρτηση κατακερματισμού, που μπορεί να θεωρηθεί ένας ισχυρός εξαγωγέας, ένα δεύτερο και πιο δύσκολο πρόβλημα είναι ότι τα βιομετρικά δεδομένα δεν μπορούν να αναπαραχθούν ακριβώς, καθώς δύο βιομετρικές σαρώσεις του ίδιου χαρακτηριστικού είναι σπάνια πανομοιότυπες. Έτσι, τα παραδοσιακά πρωτόκολλα δεν εγγυώνται την ορθότητα όταν οι χρήστες χρησιμοποιούν κοινόχρηστο μυστικό που προέρχεται από βιομετρικά δεδομένα.

3.1 Χρήση βιομετρίας στην κρυπτογραφία

Η κρυπτογραφία βασίζεται παραδοσιακά σε ομοιόμορφα κατανεμημένες και επακριβώς αναπαραγωγίσιμες τυχαίες συμβολοσειρές για τα μυστικά της. Η πραγματικότητα, ωστόσο, καθιστά δύσκολη τη δημιουργία, την αποθήκευση και την

αξιοπιστία ανάκτησης τέτοιων συμβολοσειρών. Για παράδειγμα, τα βιομετρικά δεδομένα, όπως ένα δακτυλικό αποτύπωμα ή η σάρωση ίριδας, ενώ θα δούμε παρακάτω ότι χρησιμοποιούνται για την παραγωγή τέτοιων συμβολοσειρών, δε συνάδουν πολλές φορές με την ομοιόμορφη κατανομή, ούτε αναπαράγονται ακριβώς κάθε φορά που μετριούνται.

Για να απεικονίσουμε τη χρήση τυχαίων συμβολοσειρών σε ένα απλό παράδειγμα, ας εξετάσουμε τον έλεγχο ταυτότητας με κωδικό πρόσβασης. Ένας χρήστης, η Alice, έχει κωδικό πρόσβασης και θέλει να αποκτήσει πρόσβαση στον λογαριασμό της. Ο server αποθηκεύει ορισμένες πληροφορίες $y = f(w)$ σχετικά με τον κωδικό πρόσβασης w. Όταν η Alice δηλαδή εισάγει τον κωδικό της w, της επιτρέπεται η πρόσβαση μόνο εάν $f(w) = y$. Σε αυτό το απλό παράδειγμα, υποθέτουμε ότι είναι ασφαλές για την Alice να εισαγάγει έναν κωδικό πρόσβασης για ταυτοποίηση. Ωστόσο, η μακροπρόθεσμη αποθήκευση του δεν θεωρείται ασφαλής. Ο στόχος, λοιπόν, είναι να σχεδιάσουμε μία συνάρτηση f που είναι δύσκολο να αντιστραφεί (δηλαδή, δεδομένου του y να είναι είναι δύσκολο να βρεθεί το w έτσι ώστε $f(w) = y$), έτσι ώστε κανείς να μην μπορεί να αποκαλύψει τον κωδικό πρόσβασης της Alice από το y. Τέτοιες συναρτήσεις ονομάζονται μονόδρομες.

Δυστυχώς, η παραπάνω λύση έχει πολλά προβλήματα όταν χρησιμοποιείται σε κωδικούς πρόσβασης που είναι διαθέσιμοι στην πραγματική ζωή. Πρώτον, ο ορισμός της μονόδρομης συνάρτησης προϋποθέτει ότι το w είναι πραγματικά ομοιόμορφο και δεν εγγυάται τίποτα εάν αυτό δεν συμβαίνει. Ωστόσο, οι κωδικοί πρόσβασης που έχουν κατασκευαστεί από ανθρώπους ή οι βιομετρικοί, απέχουν πολύ από τους ομοιόμορφους, παρόλο που υπάρχει κάποια τυχαιότητα σε αυτούς. Δεύτερον, η Alice πρέπει να αναπαράγει τον κωδικό πρόσβασής της ακριβώς κάθε φορά που επικυρώνει τον εαυτό της. Αυτός ο περιορισμός περιορίζει σοβαρά τα είδη των κωδικών πρόσβασης που μπορούν να χρησιμοποιηθούν. Πράγματι, ένας άνθρωπος μπορεί να απομνημονεύσει με ακρίβεια και να πληκτρολογήσει αξιόπιστα μόνο σχετικά σύντομους κωδικούς πρόσβασης, οι οποίοι δεν παρέχουν επαρκές επίπεδο ασφάλειας. Μεγαλύτερα επίπεδα ασφάλειας επιτυγχάνονται με μεγαλύτερους κωδικούς πρόσβασης και φυσικά βιομετρικούς, όπως φράσεις, απαντήσεις σε ερωτηματολόγια, χειρόγραφες υπογραφές, δακτυλικά αποτυπώματα, σαρώσεις αμφιβληστροειδούς,

φωνητικές εντολές και άλλες τιμές που επιλέγονται από τον άνθρωπο ή παρέχονται από τη φύση, πιθανώς και σε συνδυασμό.

Ακόμα, φαίνεται ότι τα βιομετρικά δεδομένα περιέχουν πολύ περισσότερη αντοχή από τους κωδικούς πρόσβασης που μπορούν να απομνημονευθούν από τον άνθρωπο. Μετρούμε την αντοχή του κωδικού με βάση την εντροπία της πληροφορίας, δηλαδή με βάση τον αριθμό των bits. Αντί να μετράμε τις απόπειρες πρόβλεψης που απαιτούνται μετράμε τον λογάριθμο με βάση 2 ενός δεδομένου αριθμού που αντιπροσωπεύει τον αριθμό των "bits εντροπίας" σε έναν κωδικό πρόσβασης.

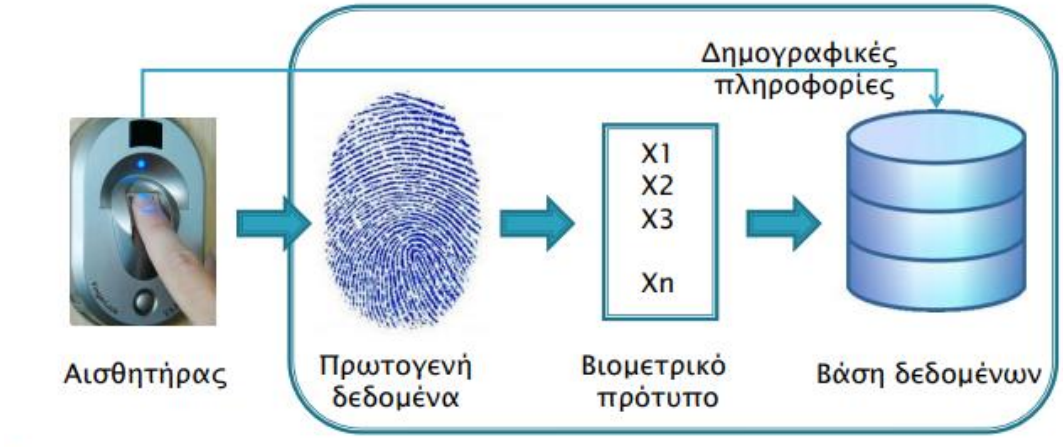
Ωστόσο, δύο βιομετρικές ενδείξεις είναι σπάνια πανομοιότυπες, παρόλο που είναι πιθανό να είναι κοντά: παρομοίως, οι άνθρωποι είναι απίθανο να θυμούνται με ακρίβεια τις απαντήσεις τους σε πολλές ερωτήσεις κατά καιρούς, αν και τέτοιες απαντήσεις πιθανότατα θα είναι παρόμοιες. Με άλλα λόγια, η ικανότητα ανοχής ενός περιορισμένου αριθμού σφαλμάτων στον κωδικό πρόσβασης διατηρώντας την ασφάλεια είναι ζωτικής σημασίας εάν θέλουμε να αποκτήσουμε μεγαλύτερη ασφάλεια από ό, τι παρέχεται από τυπικούς σύντομους κωδικούς πρόσβασης που επιλέγονται από τον χρήστη. Ο έλεγχος ταυτότητας με κωδικό πρόσβασης που περιγράφεται παραπάνω είναι ένα μόνο παράδειγμα μιας κρυπτογραφικής εφαρμογής όπου εμφανίζονται τα θέματα της ανομοιομορφίας και της ανοχής σφαλμάτων.

Κεφάλαιο 4. Στάδια Βιομετρικής Αναγνώρισης και Αυθεντικοποίησης

Στο κεφάλαιο αυτό αναφέρονται τα 3 κύρια στάδια της επεξεργασίας των βιομετρικών δεδομένων για αναγνώριση και αυθεντικοποίηση.

4.1 Εγγραφή

Σε αυτό το στάδιο γίνεται η καταγραφή των βιομετρικών χαρακτηριστικών. Μπορεί να γίνει με τη χρήση αισθητήρα , κάμερας, μικροφώνου, scanner κ.α. όπου θα παραχθούν τα πρωτογενή δεδομένα. Ωστόσο, αποτελεί πρόβλημα, ότι οι καταγραφές του ίδιου βιομετρικού στοιχείου μπορεί να διαφέρουν λίγο μεταξύ τους (ενδο-ατομική μεταβλητότητα) και αυτό μπορεί να οφείλεται σε εξωγενείς αιτίες, όπως μια μικρή αλλαγή στον τρόπο τοποθέτησης, π.χ. να μην υπάρχει καλή επαφή του δαχτύλου με τον αισθητήρα, ή και κάποιο πρόβλημα στον αισθητήρα. Επίσης, υπάρχουν και οι εγγενείς αιτίες καθώς με την πάροδο του χρόνου κάποια χαρακτηριστικά αλλοιώνονται, ή υπάρχουν τραύματα που δεν υπήρχαν, διάφορες παθήσεις κ.α. οπότε η βάση δεδομένων ενδεχομένως να χρειάζεται ανά διαστήματα ενημέρωση.

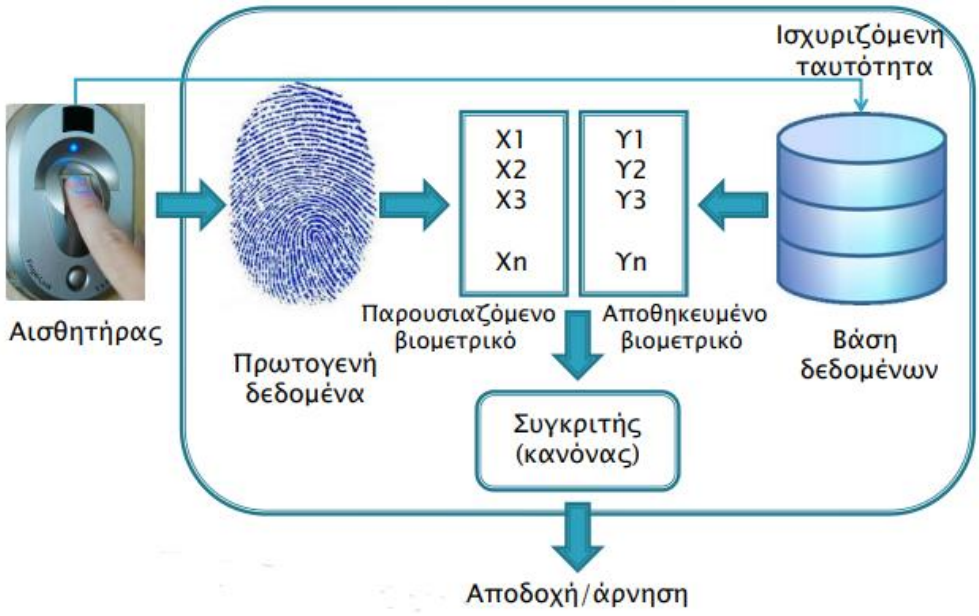


Εικόνα 1: Εγγραφή χρήστη *(8)*

4.2 Ψηφιακή Αναπαράσταση

Μετά την καταγραφή των δεδομένων, αυτά επεξεργάζονται και αποθηκεύονται στη βάση δεδομένων για μελλοντική χρήση. Σκοπός αυτού του σταδίου είναι η αποθήκευση του βιομετρικού χαρακτηριστικού και όχι η διαφορετικότητα που παρουσιάζει και το διαφοροποιεί από κάποιον άλλον χρήστη. Εδώ πλέον δεν αποθηκεύονται με την αρχική τους μορφή αλλά με τη μορφή διανυσμάτων, που αποτελούν τα βιομετρικά πρότυπα.

.

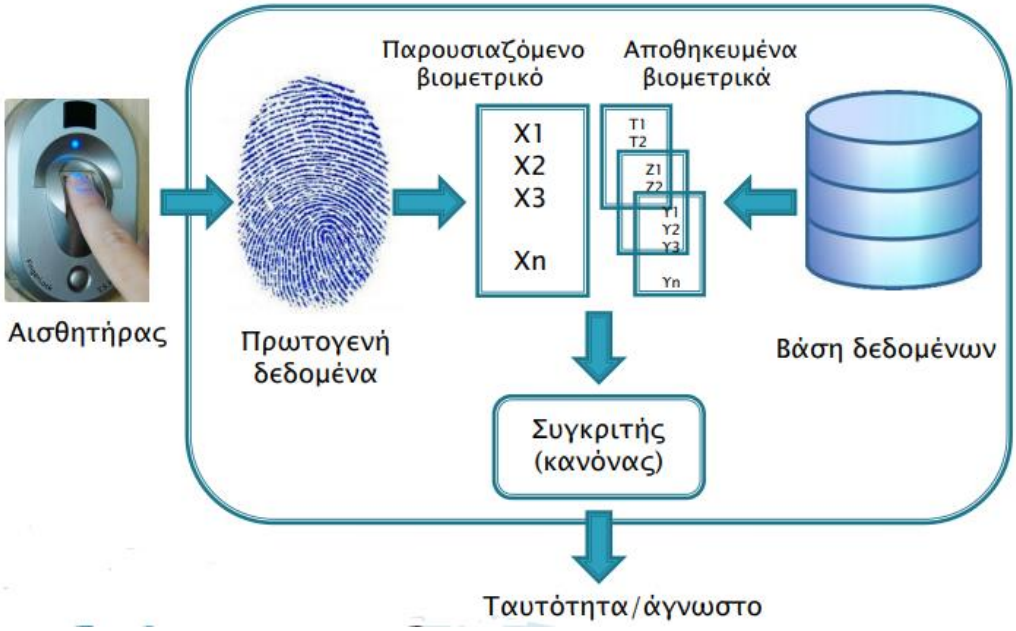


Εικόνα 2: Αυθεντικοποίησ χρήστη *(8)*

4.3 Σύγκριση

Σε αυτό το σημείο αναγνωρίζεται η δυνατότητα πρόσβασης. Το δείγμα μας συγκρίνεται με όλα τα αποθηκευμένα δεδομένα για να βρεθεί το αντίστοιχο και να γίνει η αυθεντικοποίηση. Για να συγκριθούν, εγκαθιδρύεται αρχικά ένα είδος ομοιότητας ή απόστασης μεταξύ τους.

Το πιο καθοριστικό, είναι η εξαγωγή των χαρακτηριστικών. Θα πρέπει να εξαχθούν με τέτοιο τρόπο ώστε να υπάρχει διαχωρισμός από κάποιο άλλο άτομο. Με την εξαγωγή έχουμε τη δημιουργία νέου προτύπου (template), το οποίο περιλαμβάνει κωδικοποιημένα όλα τα χαρακτηριστικά που προέκυψαν από το προηγούμενο στάδιο. Στην ουσία το νέο πρότυπο είναι αυτό που συγκρίνεται για να προκύψει ταυτοποίηση.



Εικόνα 3: Πιστοποίηση χρήστη *(8)*

Κεφάλαιο 5. Βιομετρικοί Αλγόριθμοι

Στην ενότητα αυτή παρουσιάζουμε βιομετρικούς αλγόριθμους που χρησιμοποιούνται για την επεξεργασία των βιομετρικών δεδομένων με σκοπό τη χρήση τους για αναγνώριση και αυθεντικοποίηση.

5.1 Βιομετρικοί Αλγόριθμοι Αντιστοίχισης

Οι βιομετρικοί αλγόριθμοι είναι αυτοματοποιημένες μέθοδοι που επιτρέπουν σε ένα βιομετρικό σύστημα να αναγνωρίζει ένα άτομο από τα ανατομικά ή συμπεριφορικά του χαρακτηριστικά. Αποτελούνται από μια ακολουθία αυτοματοποιημένων λειτουργιών που εκτελούνται από το σύστημα για την αυθεντικοποίηση. Αυτές οι λειτουργίες περιλαμβάνουν αξιολόγηση ποιότητας, βελτιστοποίηση, εξαγωγή χαρακτηριστικών, ταξινόμηση, αντιστοίχιση και μίξη, καθώς και αλγόριθμους συμπίεσης, που χρησιμοποιούνται συχνά για τη μείωση του χώρου αποθήκευσης και του εύρους ζώνης. Η ποιότητα αναφέρεται στη χρησιμότητα ενός βιομετρικού δείγματος ως προς την ποσότητα των πληροφοριών που προσφέρονται για τη διάκρισή του από ένα άλλο . Η βελτιστοποίηση συνήθως χρησιμοποιεί προηγούμενες γνώσεις σχετικά με το ληφθέν δεδομένο για τη διευκόλυνση των αυτόματων αλγορίθμων εξαγωγής χαρακτηριστικών ή για την καλύτερη οπτικοποίησή τους.

Πολλές εφαρμογές απαιτούν αποθήκευση ή μετάδοση των βιομετρικών δεδομένων (π.χ. εικόνες). Αυτά τα δεδομένα μπορεί να είναι μεγάλα και συχνά είναι επιθυμητό να συμπιεστούν για εξοικονόμηση χώρου αποθήκευσης ή εύρους ζώνης μετάδοσης. Αυτή η συμπίεση μπορεί να είναι είτε με απώλειες είτε όχι. Οι αλγόριθμοι συμπίεσης χωρίς απώλειες εγγυώνται ότι κάθε bit του αρχικού σήματος παραμένει αμετάβλητο μετά τη συμπίεση των δεδομένων. Υψηλότερη αναλογία συμπίεσης μπορεί να επιτευχθεί με απώλειες, αυτό όμως μπορεί να επηρεάσει την επακόλουθη εξαγωγή χαρακτηριστικών και να υποβαθμίσει τα αντίστοιχα αποτελέσματα. Τα βιομετρικά συστήματα χρησιμοποιούν συχνά συμπίεση με απώλεια, που επιλέγεται με τέτοιο τρόπο ώστε να χάνεται μια ελάχιστη ποσότητα κρίσιμων πληροφοριών, για να επιτευχθεί η καλύτερη ισορροπία μεταξύ ποιότητας δεδομένων και μεγέθους αναπαράστασης (9), (10).

Το βιομετρικό δείγμα αποκτάται από μια βιομετρική συσκευή και παράγει μια ηλεκτρονική αναπαράσταση σημάτων πολλών διαστάσεων (π.χ. δακτυλικό αποτύπωμα ή εικόνες προσώπου) (11). Για να αποφευχθεί η «κατάρα των πολλών διαστάσεων», αυτά τα σήματα πολλών διαστάσεων δεν συγκρίνονται άμεσα. Αντίθετα, μια πιο συμπαγής αναπαράσταση του σήματος - που ονομάζεται "πρότυπο" - εξάγεται από το μη επεξεργασμένο σήμα και χρησιμοποιείται για τη σύγκριση. Οι διάφορες διαδικασίες που χρησιμοποιούνται για τη σύγκριση τους ονομάζονται βιομετρικοί αλγόριθμοι.

Οι βιομετρικές τεχνικές είναι αποτελεσματικές για την αναγνώριση των ανθρώπων, επειδή τα χαρακτηριστικά των βιομετρικών χαρακτηριστικών διακρίνονται σε κάθε άτομο. Στην πράξη, ωστόσο, η φύση των βιομετρικών δεδομένων καθώς και οι περιορισμοί των τεχνικών βιομετρικής ανίχνευσης μπορούν να προκαλέσουν σημαντική μείωση της ακρίβειας του συστήματος. Είναι απαραίτητο επομένως να αναπτυχθούν βιομετρικοί αλγόριθμοι που είναι ισχυροί σε αυτές τις παραλλαγές.

Τα βιομετρικά δεδομένα υποβάλλονται σε επεξεργασία για την εξαγωγή ενός συνόλου σημαντικών και διακριτικών χαρακτηριστικών που αντιπροσωπεύουν το υποκείμενο βιομετρικό χαρακτηριστικό. Αυτά τα χαρακτηριστικά μπορεί να είναι για παράδειγμα οι μικρολεπτομέριες για δακτυλικά αποτυπώματα (7). Η εξαγωγή χαρακτηριστικών μπορεί να σχετίζεται με τη μείωση των διαστάσεων, όπου το μη επεξεργασμένο σήμα εισόδου είναι πολλών διαστάσεων, και περιέχει περιττές πληροφορίες (11) . Τα βιομετρικά δεδομένα υποβάλλονται σε επεξεργασία για την εξαγωγή ενός συνόλου σημαντικών και διακριτικών χαρακτηριστικών που αντιπροσωπεύουν το υποκείμενο βιομετρικό χαρακτηριστικό. Ανεξάρτητα από το χαρακτηριστικό, ο αλγόριθμος εξαγωγής τους ελέγχει σε μεγάλο βαθμό την απόδοση της αντιστοίχισης (7). Το εξαγόμενο σύνολο αναφέρεται συνήθως ως πρότυπο και χρησιμοποιείται ως είσοδος για την αντιστοίχιση.

Ένας αλγόριθμος αντιστοίχισης συγκρίνει τα νέα δεδομένα που εισάγει ο χρήστης με τα αποθηκευμένα πρότυπα στη βάση δεδομένων για να παράγει βαθμολογίες που αντιπροσωπεύουν την ομοιότητα μεταξύ της εισόδου και του προτύπου. Επίσης ο αλγόριθμος αυτός θα πρέπει να μπορεί να αντιμετωπίσει και παραλλαγές που μπορεί να υπάρχουν στα βιομετρικά δεδομένα (12). Αυτές οι παραλλαγές μπορεί να είναι το αποτέλεσμα ουλών, γήρανσης, ασθένειας ή να προέρχονται από κάποιον θόρυβο (φωτισμός, θόλωση κίνησης) του βιομετρικού χαρακτηριστικού.

5.1.1 Μετρήσεις απόδοσης αλγόριθμου βιομετρικής αντιστοίχισης

Πιο αναλυτικά, ένας αλγόριθμος βιομετρικής αντιστοίχισης έχει σαν είσοδο ένα βιομετρικό χαρακτηριστικό και την αντίστοιχη προσέγγισή του και ως έξοδο μια τιμή που κυμαίνεται στο διάστημα $[\mathbf{0}, \mathbf{1}]$ που δείχνει κατά πόσο είναι όμοια τα μηνύματα αυτά μεταξύ τους. Φυσικά, υπάρχει ένα προκαθορισμένο όριο ανοχής για το οποίο αν η τιμή ομοιότητας το ξεπερνά, δεχόμαστε την ομοιότητα, ενώ την απορρίπτουμε αντίστοιχα.

Το όριο ανοχής που επιδεικνύει το σύστημα, κατά την διαδικασία της σύγκρισης των προτύπων, αποτελεί έναν εξαιρετικά κρίσιμο παράγοντα για την σωστή λειτουργία ενός βιομετρικού συστήματος. Όπως έχουμε ήδη αναφέρει, είναι σχεδόν αδύνατη η απόλυτη ταύτιση του βιομετρικού προτύπου που δημιουργήθηκε στην πρώτη σάρωση κατά την εγγραφή του χρήστη με μία μετέπειτα σάρωση του ίδιου βιομετρικού. Γι'αυτό το λόγο επηρεάζεται και η διαδικασία της αναγνώρισης. Ωστόσο, παρά την επιρροή που έχει στην αναγνώριση, δε θα θέλαμε να πετύχουμε την πλήρη ταύτιση καθώς ο αλγόριθμος θα απέρριπτε ακόμα και τους εξουσιοδοτημένους χρήστες. Βέβαια, δε θα θέλαμε να έχουμε και υψηλά επίπεδα ανοχής γιατί αυτό θα έκανε το σύστημά μας ευάλωτο στην εξαπάτηση από μη εξουσιοδοτημένους χρήστες. Για να είναι λοιπόν, το σύστημά μας λειτουργικό αλλά και ασφαλές είναι κρίσιμη η επιλογή του ορίου ανοχής.

Η αποτελεσματικότητα, λοιπόν, του αλγορίθμου αποδεικνύεται από το ποσοστό των λάθος αντιστοιχίσεων που έγιναν δεκτοί FMR (falsematchingrate) καθώς και από το ποσοστό των σωστών αντιστοιχίσεων που δεν έγιναν δεκτοί FNMR(falsenon-matchingrate).Προφανώς για καλύτερα αποτελέσματα αυτά τα ποσοστά θα πρέπει να είναι χαμηλά.Οι δυο αυτοί δείκτες συμπληρώνουν ο ένας τον άλλον, καθώς όταν αυξάνεται ο ένας μειώνεται ο άλλος. Αυτό σημαίνει πως αν ένα σύστημα κατασκευαστεί με τρόπο ώστε να είναι χαμηλό το ποσοστό του FMR, τότε θα είναι δύσκολη και η πρόσβαση των μη εξουσιοδοτημένων χρηστών. Αντιθέτως, αν κατασκευαστεί με χαμηλό ή και με μηδενικό ποσοστό του FNMR, τότε η πρόσβαση των μη εξουσιοδοτημένων χρηστών θα είναι και πιο εύκολη.

Τέτοιου είδους αλγόριθμοι μπορούν να χρησιμοποιηθούν και για την αντιστοίχιση πλειάδων μηνυμάτων. Για παράδειγμα για να ελέγξουμε την αντιστοίχιση μεταξύ 2 πλειάδων μηνυμάτων, ο αλγόριθμος θα ελέγξει πόσα ζεύγη μηνυμάτων μεταξύ αυτών γίνονται δεκτά ως προς την ομοιότητα, και αν ο αριθμός του είναι ικανοποιητικός

σύμφωνα με τα αντίστοιχα κριτήρια, τότε δεχόμαστε και την αντιστοιχία μεταξύ των πλειάδων (13).

5.1.2 Ορισμός των μικρολεπτομεριών (Minutiaepoints)

Παραδοσιακά, δύο δακτυλικά αποτυπώματα συγκρίνονται με τη χρήση διακριτών χαρακτηριστικών που ονομάζονται μικρολεπτομέρειες. Αυτά τα χαρακτηριστικά περιλαμβάνουν σημεία στο δέρμα ενός δακτύλου, όπως οι κορυφογραμμές, πιο συγκεκριμένα το τελείωμά τους και τις διακλαδώσεις τους. Για την αναζήτηση και αντιστοίχιση δακτυλικών αποτυπωμάτων, καταγράφεται η θέση συντεταγμένων και ο προσανατολισμός της κορυφογραμμής σε κάθε σημείο λεπτομερειών. Η θέση κάθε λεπτομέρειας αντιπροσωπεύεται από μια θέση συντεταγμένων στην εικόνα του δακτυλικού αποτυπώματος. Ο προσανατολισμός των λεπτομερειών απεικονίζεται σε μοίρες, με μηδενικές μοίρες που δείχνουν οριζόντια και προς τα δεξιά, ενώ όταν αυξάνονται προχωρούν αριστερόστροφα. Ο προσανατολισμός ενός άκρου κορυφογραμμής καθορίζεται μετρώντας τη γωνία μεταξύ του οριζόντιου άξονα και της γραμμής που ξεκινά από το σημείο λεπτομερειών και διατρέχει το μέσο της κορυφογραμμής. Ο προσανατολισμός μιας διακλάδωσης καθορίζεται με μέτρηση της γωνίας μεταξύ του οριζόντιου άξονα και της γραμμής που ξεκινά από το σημείο λεπτομερειών και διατρέχει το μέσο της ‘’κοιλάδας’’ μεταξύ των διακλαδισμένων κορυφογραμμών (14).

5.1.3 Ο αλγόριθμος MINDTCT για την εξαγωγή των μικρολεπτομεριών

Ο Mindtct εισάγει μια εικόνα δακτυλικού αποτυπώματος και ανιχνεύει αυτόματα λεπτομερή στοιχεία στο δακτυλικό αποτύπωμα (14).

1. Input Fingerprint File: Έχει μια επιλογή που θα επιτρέπει να βελτιώσει εικόνες πολύ χαμηλής αντίθεσης. Δηλαδή, θα αξιολογήσει το ιστόγραμμα της εικόνας εισαγωγής και εάν η εικόνα έχει πολύ χαμηλή αντίθεση, τη βελτιώνει, διαφορετικά δεν τροποποιείται.

2. Generate Image Maps: Επειδή η ποιότητα της εικόνας ενός δακτυλικού αποτυπώματος μπορεί να διαφέρει, είναι σημαντικό να μπορούμε να αναλύσουμε την εικόνα και να προσδιορίσουμε περιοχές που έχουν ‘’υποβαθμιστεί’’ και είναι

πιθανότατα να έχουν προκαλέσει προβλήματα. Μπορούν να μετρηθούν διάφορα χαρακτηριστικά για να μεταφέρουν πληροφορίες σχετικά με την ποιότητα εντοπισμένων περιοχών στην εικόνα. Αυτά περιλαμβάνουν τον προσδιορισμό της κατεύθυνσης των κορυφογραμμών , τον εντοπισμό περιοχών χαμηλής αντίθεσης, υψηλής καμπυλότητας κ.α.. Οπότε δημιουργούνται οι παρακάτω χάρτες:

- Direction Map (Χάρτης κατεύθυνσης):Ο σκοπός αυτού του χάρτη είναι να αντιπροσωπεύει περιοχές της εικόνας με επαρκή δομή κορυφογραμμής. Οι καλά διαμορφωμένες και σαφώς ορατές κορυφογραμμές είναι απαραίτητες για αξιόπιστη ανίχνευση σημείων λήξης, κορυφής και διακλάδωσης. Επιπλέον, ο χάρτης κατεύθυνσης καταγράφει το γενικό προσανατολισμό των κορυφογραμμών.
- Low Contrast Map (Χάρτης χαμηλής αντίθεσης):Αυτός ο χάρτης διαχωρίζει το φόντο της εικόνας από το δακτυλικό αποτύπωμα και χαρτογραφεί ‘’λεκέδες’’ και περιοχές που δεν έχουν αποτυπωθεί έντονα. Οι λεπτομέρειες δεν εντοπίζονται σε μπλοκ χαμηλής αντίθεσης στην εικόνα.
- Low Flow Map (Χάρτης χαμηλής ροής):Είναι πιθανό, κατά τη λήψη του χάρτη αρχικής κατεύθυνσης, ορισμένα μπλοκ να μην έχουν κυρίαρχη ροή κορυφογραμμής. Αυτά τα μπλοκ αντιστοιχούν συνήθως σε περιοχές χαμηλής ποιότητας στην εικόνα. Αρχικά, αυτά τα μπλοκ δεν έχουν προσανατολισμό στον χάρτη κατεύθυνσης, αλλά στη συνέχεια σε μερικά από αυτά μπορεί να εκχωρηθεί προσανατολισμός παρεμβάλλοντας τη ροή κορυφογραμμής γειτονικών μπλοκ. Ο χάρτης χαμηλής ροής σηματοδοτεί τα μπλοκ που δεν μπορούσαν αρχικά να εκχωρηθούν με κυρίαρχη ροή κορυφογραμμής.
- High Curve Map (Χάρτης υψηλής καμπύλης):Ο χάρτης υψηλής καμπύλης σηματοδοτεί μπλοκ που βρίσκονται σε περιοχές με υψηλή καμπυλότητα του δακτυλικού αποτυπώματος. Χρησιμοποιούνται δύο διαφορετικά μέτρα. Το πρώτο, που ονομάζεται στροβιλισμός, μετρά την αθροιστική αλλαγή στην κατεύθυνση ροής της κορυφογραμμής γύρω από όλους τους γείτονες ενός μπλοκ. Η δεύτερη, ονομαζόμενη καμπυλότητα, μετρά τη μεγαλύτερη αλλαγή κατεύθυνσης μεταξύ της ροής κορυφογραμμής ενός μπλοκ και της ροής κορυφογραμμής καθενός από τους γείτονές της.
- Quality Map (Χάρτης ποιότητας):Ο τελικός χάρτης εικόνας που παράγεται είναι ένας χάρτης ποιότητας. Όπως συζητήθηκε, ο χαμηλής αντίθεσης χάρτης,

ο χάρτης χαμηλής ροής και ο χάρτης υψηλής καμπύλης δείχνουν διαφορετικές περιοχές χαμηλής ποιότητας του εικόνα. Οι πληροφορίες σε αυτούς τους χάρτες ενσωματώνονται σε έναν γενικό χάρτη, τον χάρτη ποιότητας.

3. Binarize Image: Ο αλγόριθμος ανίχνευσης λεπτομερειών έχει σχεδιαστεί για να λειτουργεί σε μια εικόνα δύο επιπέδων (ή δυαδική) όπου τα μαύρα εικονοστοιχεία αντιπροσωπεύουν κορυφογραμμές και τα λευκά εικονοστοιχεία αντιπροσωπεύουν ‘’κοιλάδες’’ στο δέρμα του δακτύλου.Για να δημιουργήσουμε αυτήν τη δυαδική εικόνα, κάθε εικονοστοιχείο στην εικόνα εισόδου κλίμακας του γκρι πρέπει να αναλυθεί για να προσδιοριστεί εάν θα πρέπει να σημειωθεί ως ένα μαύρο ή άσπρο pixel.Αυτή η διαδικασία αναφέρεται ως δυαδικοποίηση εικόνας.

Πρέπει να σημειωθεί ότι το βήμα δυαδικοποίησης είναι κρίσιμο για την επιτυχή ανίχνευση των λεπτομερειών.Πρέπει να είναι ισχυρό όσον αφορά την αποτελεσματική αντιμετώπιση διαφορετικών βαθμών ποιότητας εικόνας και αξιόπιστο όσον αφορά την ακριβή απόδοση των κορυφογραμμών και των ‘’κοιλάδων’’.Είναι επιθυμητό να διατηρηθούν όσο το δυνατόν περισσότερες πληροφορίες για την εικόνα και η δομή της κορυφογραμμής / κοιλάδας, ώστε να μην χαθούν λεπτομέρειες, αλλά ανεπιθύμητο να αναδειχθούν οι υποβαθμισμένες περιοχές της εικόνας έως το σημείο εισαγωγής ψευδών λεπτομερειών.

4. Detect Minutiae:Σε αυτό το βήμα σαρώνεται η δυαδική εικόνα του δακτυλικού αποτυπώματος, και εντοπίζονται τοπικά μοτίβα εικονοστοιχείων που υποδηλώνουν το τέλος ή τον διαχωρισμό/διακλάδωση μιας κορυφογραμμής.

5. Remove False Minutiae: Αυτά το βήμα περιλαμβάνει την απομάκρυνση ‘’νησιών’’, ‘’λιμνών’’, ‘’τρυπών’’, λεπτομερειών σε περιοχές με κακή ποιότητα εικόνας, δευτερεύοντων λεπτομερειών, επικαλύψεων, λεπτομερειών που είναι πολύ πλατιές ή είναι πολύ στενές (πόροι).

6. Count Neighbor Ridges:Οι αντιστοιχιστές λεπτομερειών δακτυλικών αποτυπωμάτων χρησιμοποιούν συχνά βοηθητικές πληροφορίες. Συνήθως περιλαμβάνουν την κατεύθυνση των λεπτομερειών, τον τύπο τους και μπορεί να περιλαμβάνουν πληροφορίες που αφορούν τους πλησιέστερους γείτονές τους. Χρησιμοποιώντας αυτήν την τοπολογία, οι μετρήσεις κορυφογραμμών υπολογίζονται και καταγράφονται μεταξύ ενός σημείου λεπτομερειών και κάθε ενός από τους πλησιέστερους γείτονές του.

7. Assess Minutiae Quality:Ακόμη και με τη μακρά λίστα βημάτων κατάργησης ψευδών λεπτομεριών παραπάνω, κάποιες ωστόσο παραμένουν δυνητικά στη λίστα. Ένα ανθεκτικό ποιοτικό μέτρο μπορεί να βοηθήσει, καθώς τα ψευδή λεπτομερή στοιχεία θα έχουν χαμηλότερη ποιότητα από τα πραγματικά λεπτομερή.Δύο παράγοντες συνδυάζονται για να παράγουν ένα ποιοτικό μέτρο για κάθε σημείο λεπτομερειών που εντοπίστηκε. Ο πρώτος παράγοντας, λαμβάνεται απευθείας από τη θέση του σημείου λεπτομερειών στον χάρτη ποιότητας. Ο δεύτερος παράγοντας βασίζεται σε απλά στατιστικά στοιχεία των εικονοστοιχείων (μέση τιμή και τυπική απόκλιση) εντός της πλησιέστερης γειτονιάς του σημείου λεπτομερειών.

8. Output Minutiae File:Τα λεπτομερή στοιχεία που προκύπτουν εξάγονται σε ένα αρχείο. Παράγονται επίσης και άλλα αρχεία εξόδου. Αυτά περιλαμβάνουν ένα αρχείο για καθένα χάρτη εικόνων (Direction Map, Low Contrast Map, Low Flow Map, High Curve Map, Quality Map) και ένα αρχείο καταγραφής που περιλαμβάνει όλα τα λεπτομερή στοιχεία που εντοπίστηκαν και τα σχετικά χαρακτηριστικά τους.

5.1.4 Ο αλγόριθμος βιομετρικής αντιστοίχισης BOZORTH3

Έχουν προταθεί και εφαρμοστεί διάφοροι αλγόριθμοι για την αντιστοίχιση δύο δακτυλικών αποτυπωμάτων με αναπαράσταση λεπτομερειών. Ένας τύπος μεθόδου για την αντιστοίχιση δύο προτύπων δακτυλικών αποτυπωμάτων που βασίζονται σε λεπτομερή στοιχεία περιέχει ένα στάδιο ευθυγράμμισης, το οποίο μεγιστοποιεί τον αριθμό των αντίστοιχων λεπτομερειών αντιστοίχισης και ένα στάδιο υπολογισμού Ευκλείδειας απόστασης, στο οποίο αξιολογείται η ομοιότητα δύο δακτυλικών αποτυπωμάτων (15), (16). Δεδομένου ότι επιπρόσθετα χαρακτηριστικά ενός δακτυλικού αποτυπώματος, όπως τα σημεία πυρήνα ή δέλτα, είναι απαραίτητα για την υποβοήθηση της σύγκρισης, δεν είναι εγγυημένη η βέλτιστη αντιστοίχιση μιας εικόνας με χαμηλότερη ανάλυση ή πληροφορίας όπου λείπουν σημεία αναφοράς. Προκειμένου να διατηρηθεί η γενικότητα, το Εθνικό Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ανέπτυξε έναν αλγόριθμο αντιστοίχισης δακτυλικών αποτυπωμάτων, που ονομάζεται Bozorth matcher (17).

Ο αλγόριθμος αντιστοίχισης BOZORTH3 υπολογίζει μια βαθμολογία (σκορ) αντιστοίχισης μεταξύ των λεπτομερειών από δύο οποιαδήποτε δακτυλικά

αποτυπώματα ώστε προσδιοριστεί εάν προέρχεται από το ίδιο δάχτυλο. Είναι μια τροποποιημένη έκδοση που γράφτηκε από τον Allan S. Bozorth ενώ βρισκόταν στο FBI. Έχει τρία βασικά βήματα (18):

1. Κατασκευή ενδοδακτυλικών πινάκων σύγκρισης μικρολεπτομερειών (intra-fingerprint minutiae comparison tables) για το δακτυλικό αποτύπωμα του δείγματος και έναν πίνακα για κάθε δακτυλικό αποτύπωμα που είναι αποθηκευμένο στη βάση (gallery), για να συγκριθούν μεταξύ τους.
2. Κατασκευή διαδακτυλικού πίνακα συμβατότητας (inter-fingerprint pair-pair compatibility table), όπου το σύστημα συγκρίνει τον πίνακα σύγκρισης μικρολεπτομερειών του δείγματος με τον πίνακα σύγκρισης μικρολεπτομερειών της gallery και κατασκευάζει έναν νέο πίνακα συμβατότητας.
3. Σάρωση του διαδακτυλικού πίνακα συμβατότητας για τη δημιουργία συμπλέγματος και υπολογισμού σκορ αντιστοίχισης/ομοιότητας.

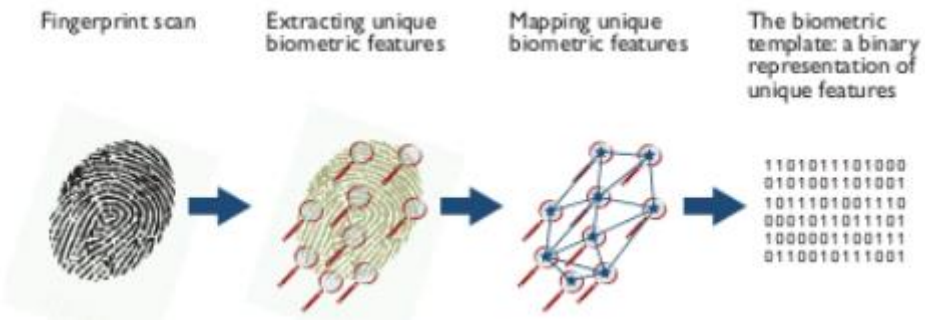
Χρησιμοποιεί μόνο τις συντεταγμένες (x, y, θ) των σημείων λεπτομερειών για την αντιστοίχιση των δακτυλικών αποτυπωμάτων, δηλαδή τη θέση συντεταγμένων και τον προσανατολισμός της κορυφογραμμής σε κάθε σημείο λεπτομερειών όπως αναφέρονται αναλυτικά στο εδάφιο 5.1.2. Δημιουργεί ξεχωριστούς πίνακες για να ταιριάζουν τα δακτυλικά αποτυπώματα που καθορίζουν την απόσταση και τον προσανατολισμό μεταξύ των λεπτομερειών σε κάθε δακτυλικό αποτύπωμα. Αυτοί οι δύο πίνακες συγκρίνονται για συμβατότητα και κατασκευάζεται ένας νέος πίνακας που αποθηκεύει πληροφορίες που δείχνουν την ομοιότητα μεταξύ των δακτυλικών αποτυπωμάτων. Ο πίνακας συμβατότητας μεταξύ των δακτύλων χρησιμοποιείται για τη δημιουργία ενός σκορ αντιστοίχισης, εξετάζοντας το μέγεθος και τον αριθμό των συμβατών ομάδων των λεπτομερειών (14).

5.2 Μετασχηματισμός βιομετρικών δεδομένων για την προστασία προτύπων

Για τον μετασχηματισμό των χαρακτηριστικών χρησιμοποιείται μια συνάρτηση βασισμένη σε κάποιες παραμέτρους, οι οποίες μπορούν να χρησιμοποιηθούν ως κλειδί, για τη δημιουργία ενός μετασχηματισμένου βιομετρικού ή μετασχηματισμένων διανυσμάτων χαρακτηριστικών. Τα μετασχηματισμένα χαρακτηριστικά ή διανύσματα είναι και αυτά που χρησιμοποιούνται για τη σύγκριση. Η συνάρτηση αυτή όπως αναφέραμε και παραπάνω θα ήταν πιο ιδανική όταν είναι μη αντιστρέψιμη, ώστε να είναι υπολογιστικά δύσκολο να υπολογιστεί παρά τη γνώση των παραμέτρων μετασχηματισμού. Αυτό σημαίνει ότι ακόμα και το κλειδί να γίνει γνωστό

από μία κακόβουλη οντότητα, συνεχίζει να μη παρέχει καμία πληροφορία για το πρότυπο βιομετρικό δεδομένο.

Ανεξάρτητα από τις τεχνικές μετασχηματισμού , αυτό που σημειώνουμε είναι ότι μόνο τα μετασχηματισμένα δεδομένα αποθηκεύονται στη βάση δεδομένων. Επομένως, ακόμα και αν παραβιαστεί η βάση, και αν τα κλειδιά φυσικά δεν είναι προσβάσιμα και ο μετασχηματισμός δε μπορεί να αντιστραφεί, τα πρότυπα βιομετρικά στοιχεία δε θα μπορέσουν να εξαχθούν.

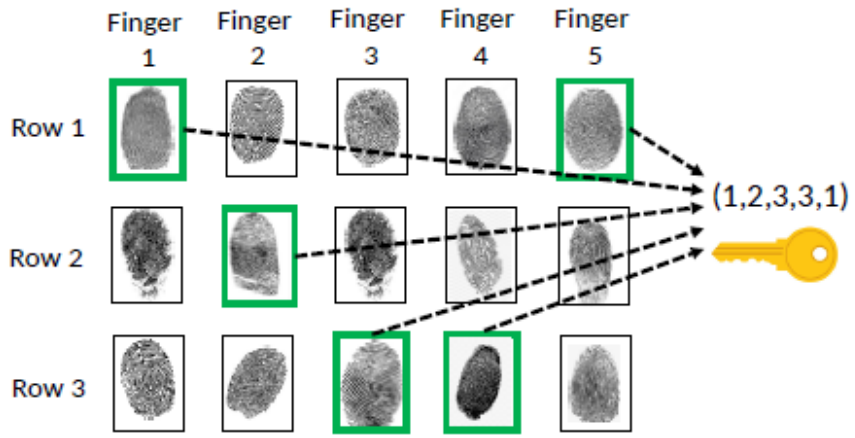


Εικόνα 4: Δημιουργία βιομετρικού προτύπου δακτυλικού αποτυπώματος *(19)*

Πιο αναλυτικά, σε μία βάση δεδομένων , ένας χρήστης καταχωρείται ως ένα διάνυσμα n διαφορετικών βιομετρικών χαρακτηριστικών $w = w_1 \dots w_n$. Στόχος είναι ένας πιστοποιημένος χρήστης να μπορεί να ανακτήσει το βιομετρικό πρότυπό του, δηλαδή να έχει πρόσβαση στο σύστημα, σε μία μετέπειτα σάρωση των βιομετρικών δεδομένων με πρότυπο $\hat{w} = \hat{w}_1 \dots \hat{w}_n$. Αποτελεί στόχο καθώς τα πρότυπα μεταξύ τους έχουν μικρές διαφορές αφού σπάνια οι σαρώσεις του ίδιου βιομετρικού χαρακτηριστικού είναι πανομοιότυπες.

Για να αποτρέψουμε όμως έναν κακόβουλο χρήστη να παραβιάσει τη βάση δεδομένων και να έχει πρόσβαση στο πρότυπο w, η κατασκευή μας κρύβει την αντιστοιχία των χρηστών με τα διανύσματα των βιομετρικών τους χαρακτηριστικών, τοποθετώντας τα με τυχαία σειρά. Έτσι ένας αντίπαλος δε μπορεί να επιλέξει διανύσματα συσχετισμένων προτύπων, αλλά πρέπει να προσπαθήσει να ανακατασκευάσει το w μέσω αναζήτησης brute-force, να δοκιμάσει δηλαδή όλα τα πιθανά w'. Δεδομένων αρκετών χρηστών, τέτοια αναζήτηση είναι υπολογιστικά ανέφικτη στην πράξη.

Για να κατασκευαστεί το w , ο χρήστης παρουσιάζει το κατά προσέγγιση $\hat{w} = \hat{w}_1 \dots \hat{w}_n$. Τα μετασχηματισμένα πρότυπα παραμένουν στο ίδιο πεδίο τιμών-χαρακτηριστικών όπως και τα αρχικά, επιτρέποντας έτσι τη χρήση ενός τυπικού αλγόριθμου βιομετρικής αντιστοίχισης για να βρεθούν οι αντιστοιχίες των $\hat{w}_i$ με τα περισσότερο όμοια w_i'στη βάση D, αποδίδοντας ένα νέο σύνολο προτύπων w' (13).



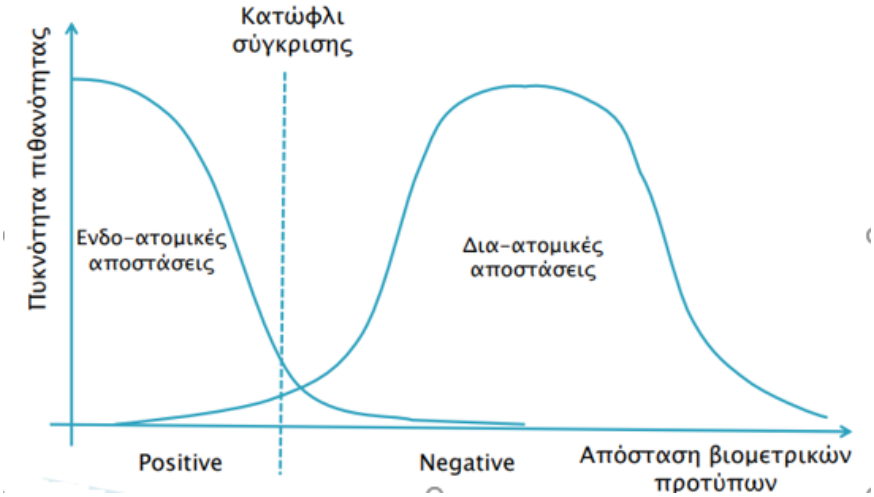
Εικόνα 5: Τα πρότυπα που αντιστοιχούν σε κάθε θέση δακτύλου αποθηκεύονται σε τυχαία σειρά. Κατά τον έλεγχο ταυτότητας, οι εμφανιζόμενες εικόνες δακτύλων αντιστοιχίζονται σε πρότυπα. οι αντίστοιχοι δείκτες γραμμής - π.χ. εδώ (1, 2, 3, 3, 1) - χρησιμοποιούνται για τη σύνθεση του κλειδιού του χρήστη. *(19)*

5.2.1 Το πρόβλημα των συσχετίσεων

Σε αντίθεση με τα συστήματα που βασίζονται στον κωδικό πρόσβασης, όπου είναι απαραίτητη η τέλεια αντιστοίχιση μεταξύ δύο αλφαριθμητικών συμβολοσειρών για την επικύρωση της ταυτότητας ενός χρήστη, ένα βιομετρικό σύστημα συναντά σπάνια δύο δείγματα του βιομετρικού χαρακτηριστικού ενός χρήστη που έχουν ως αποτέλεσμα ακριβώς το ίδιο σύνολο χαρακτηριστικών.

Η μεταβλητότητα που παρατηρείται στο σύνολο βιομετρικών χαρακτηριστικών ενός ατόμου αναφέρεται ως ενδοατομική μεταβλητότητα και μεταξύ συνόλων χαρακτηριστικών που προέρχονται από δύο διαφορετικά άτομα είναι γνωστή διατομική μεταβλητότητα. Ένα χρήσιμο σύνολο χαρακτηριστικών πρέπει να εμφανίζει χαμηλή ενδοατομική μεταβλητότητα και υψηλή διατομική μεταβλητότητα.

Δυστυχώς, είναι δύσκολο να σχεδιαστούν συναρτήσεις μετασχηματισμού που να διατηρούν ταυτόχρονα την διακριτότητα των προτύπων και τις μη αντιστρέψιμες ιδιότητες μαζί. Η συνάρτηση μετασχηματισμού θα πρέπει να είναι σχεδιασμένη με τέτοιο τρόπο, ώστε οι ενδοατομικές και οι διατομικές αποστάσεις στον μετασχηματισμένο χώρο να είναι παρόμοιες με τις αντίστοιχες στον αρχικό χώρο.



Εικόνα 6:Ταξινόμηση βιομετρικών προτύπων *(8)*

Ωστόσο, μια μεγάλη πρόκληση στην πράξη είναι ότι τα βιομετρικά πρότυπα από τον ίδιο χρήστη ενδέχεται να συσχετιστούν. Το βιομετρικό χαρακτηριστικό μπορεί να μην είναι μοναδικό ή η ψηφιακή αναπαράσταση του να μην αποτυπώνει όλες τις πληροφορίες σχετικά με αυτό, καθιστώντας το στην πράξη μη μοναδικό. Η γενετική ομοιότητα μεταξύ συγγενών (πχ δίδυμα, πατέρας και γιος) συνεισφέρει σε αυτήν την έλλειψη μοναδικότητας κάποιων βιομετρικών στοιχείων. Χαρακτηριστικό παράδειγμα είναι το σχεδόν ίδιο πρόσωπο των διδύμων. Αλλά και το φύλο είναι μία παράμετρος που μπορεί συνεισφέρει καθώς συσχετίζεται σημαντικά με τα δακτυλικά αποτυπώματα για παράδειγμα.

Επιπροσθέτως, ακόμα και η παραδοχή ότι τα βιομετρικά χαρακτηριστικά είναι μόνιμα δεν είναι απόλυτα σωστή. Αυτό γιατί υπάρχουν οι φυσιολογικές αλλαγές με την πάροδο του χρόνου, ασθένειες που μπορεί να προκαλέσουν αλλοίωση ή κάποιος τραυματισμός που μπορεί να προκαλέσει αλλαγή. Ακόμα όμως και αν παραμερίσουμε όλες αυτές τις παραμέτρους, ένα άλλο πρόβλημα είναι ότι τα βιομετρικά συστήματα βασίζονται πάνω στα μετασχηματισμένα χαρακτηριστικά και όχι απευθείας στα πρότυπα χαρακτηριστικά. Όπως αναφέραμε και στην αρχή λοιπόν, τα σύνολα χαρακτηριστικών που προκύπτουν από διαφορετικές μετρήσεις του ίδιου χαρακτηριστικού είναι σπάνια πανομοιότυπες.

Η αντιστοίχιση βιομετρικών στην πράξη, επομένως, δεν είναι ιδανική και υπόκειται σε μια σειρά από σφάλματα που οφείλονται στη θορυβώδη φύση των βιομετρικών στοιχείων. Ένα δάχτυλο μπορεί να ταιριάζει με το λάθος πρότυπο (που ανήκει σε διαφορετικό χρήστη) για την αντίστοιχη θέση του. Επομένως, απαιτείται κάποια μορφή

διόρθωσης σφαλμάτων για την ανάκτηση του κλειδιού. Είναι δύσκολο να επιτευχθεί ένα βασικό ανώτερο όριο σε αυτούς τους συσχετισμούς (13), (20). Για αυτό γίνεται και η χρήση των δεικτών FMR (falsematchingrate) και FNMR(falsenon-matchingrate) που αναφέρονται στην ενότητα 5.1.1.

5.2.2 Χώροι μηνυμάτων

Όταν αναφερόμαστε στην ανάγνωση ενός βιομετρικού δεδομένου θα χρησιμοποιούμε τον όρο μήνυμα. Ένα μήνυμα ουσιαστικά είναι το μετασχηματισμένο διάνυσμα βιομετρικών χαρακτηριστικών. Επειδή οι χρήστες μπορεί να χρησιμοποιούν πολλαπλά βιομετρικά δεδομένα ή διαφορετικές μορφές ενός χαρακτηριστικού είναι σημαντικό να λαμβάνουμε υπόψη κάθε δεδομένο σαν ξεχωριστό. Για παράδειγμα το αποτύπωμα του αντίχειρα είναι διαφορετικό από του δείκτη, προέρχονται δηλαδή από διαφορετικές κατανομές.

Θα το συμβολίζουμε το χώρο στον οποίο ανήκει το μήνυμα με κεφαλαίο γράμμα και τα περιεχόμενα στοιχεία του με μικρά. Πιο συγκεκριμένα, έστω W ο χώρος μηνυμάτων και w το στοιχείο του, δηλαδή το μήνυμα. Το μήνυμα είναι το διάνυσμα των n βιομετρικών δεδομένων του χρήστη όπου στην i-θέση αντιστοιχεί η i-οστή σάρωση του βιομετρικού στοιχείου. Οπότε συμβολίζουμε το διάνυσμα ως $w = w_1 \dots . w_n$, όπου $1 \leq i \leq n \leq |w|$.

Οι χρήστες μπορούν να πραγματοποιήσουν έλεγχο ταυτότητας χρησιμοποιώντας πολλαπλές βιομετρικές αναγνώσεις. Αυτές οι αναγνώσεις μπορεί να είναι πολυτροπικές, δηλαδή να περιλαμβάνουν διαφορετικούς τύπους φυσιολογικών χαρακτηριστικών (π.χ. δακτυλικό αποτύπωμα, σάρωση ίριδας, γεωμετρία χεριών κ.λπ.) ή μπορεί να περιλαμβάνουν πολλαπλές εμφανίσεις του ίδιου τύπου χαρακτηριστικού (π.χ. πολλαπλά δακτυλικά αποτυπώματα, δύο iris codes κ.λπ.) .

Είναι χρήσιμο να βλέπουμε τέτοιες περιπτώσεις ως ξεχωριστά βιομετρικά χαρακτηριστικά. Έτσι ένα μήνυμα μπορεί να προέρχεται από ένα χώρο μηνυμάτων W_i με πιθανότητα p_i.Έχουμε λοιπόν $W \subseteq W_1 x W_2 x \dots W_n$ με $w = w_1 \dots . w_n$. Τότε $p(w)$ είναι η πιθανότητα $w \in W$. Ωστόσο, επειδή τα βιομετρικά χαρακτηριστικά που δίνονται από έναν χρήστη δεν είναι ανεξάρτητα μεταξύ τους δε μπορούμε να ισχυριστούμε ότι ισχύει η πολλαπλασιαστική ιδιότητα $\prod_i p_i\ (w_i)$.

Επειδή, όπως αναφέραμε, τα βιομετρικά δεδομένα είναι θορυβώδη και το ίδιο χαρακτηριστικό ενός ίδιου χρήστη μπορεί να διαφέρει ελαφρώς, θα θεωρήσουμε μία συνάρτηση θορύβου για τη μοντελοποίηση των λαθών (13).

5.2.3 Μετρικοί χώροι

Κατά τη φάση αντιστοίχισης, το ληφθέν πρότυπο συγκρίνεται με άλλα υπάρχοντα πρότυπα, υπολογίζοντας την ομοιότητα μεταξύ τους. Για να ελέγξουμε κατά πόσο δύο πρότυπα είναι όμοια μεταξύ τους θα πρέπει να υπολογιστεί η απόσταση μεταξύ τους. Αυτό επιτυγχάνεται με τη χρήση των μετρικών χώρων.

Μετρικός χώρος είναι ένα σύνολο στο οποίο έχει οριστεί η έννοια της "απόστασης". Έστω ένα μη κενό σύνολο M και d: $MxM \rightarrow \mathbb{R}$ μια συνάρτηση. Η συνάρτηση αυτή θα λέγεται μετρική, και το ζεύγος (M, d) θα λέγεται μετρικός χώρος αν για κάθε$x, y, z \in M$ικανοποιεί τα ακόλουθα:

- $x = y \Leftrightarrow d(x, y) = 0 = d(y, x)$ (αξίωμα ταύτισης)
- $d(x, y) = d(y, x)$ (αξίωμα συμμετρίας)
- $d(x, y) \leq d(x, z) + d(z, y)$ (τριγωνική ανισότητα)

Κάποιοι από τους βασικούς μετρικούς χώρους που χρησιμοποιούνται για την ενσωμάτωση των βιομετρικών δεδομένων είναι:

- Απόσταση Hamming (Hamming distance): ο αριθμός των συμβολικών θέσεων που διαφέρουν μεταξύ των w και ŵ. Εδώ M = Fn για ένα αλφάβητο F, και dis(w,ŵ) ο αριθμός των στοιχείων που οι δύο συμβολοσειρές διαφοροποιούνται.
- Απόσταση συνόλων (Set Distance): το μέγεθος της συμμετρικής διαφοράς δύο συνόλων εισόδου w και ŵ), είναι κατάλληλο όταν η θορυβώδης είσοδος αντιπροσωπεύεται ως υποσύνολο χαρακτηριστικών από ένα σύνολο δυνατών χαρακτηριστικών. Εδώ το M αποτελείται από όλα τα υποσύνολα ενός συνόλου U. Για δύο εισόδους w,ŵ, η συμμετρική τους διαφορά είναι $w \Delta \hat{w} = |w \cup \hat{w} - w \cap \hat{w}|$.

Απόσταση σύνταξης (Edit Metric):ο αριθμός των εισαγωγών και διαγραφών που απαιτούνται για τη μετατροπή μιας συμβολοσειράς σε άλλη) εμφανίζεται, για

παράδειγμα, όταν ο κωδικός πρόσβασης έχει εισαχθεί ως συμβολοσειρά, λόγω σφαλμάτων πληκτρολόγησης ή λαθών που έγιναν κατά την αναγνώριση. Η απόσταση μεταξύ w και ŵ ορίζεται ως ο μικρότερος αριθμός εισαγωγών και διαγραφών χαρακτήρων που απαιτούνται για τη μετατροπή του w σε ŵ (21).

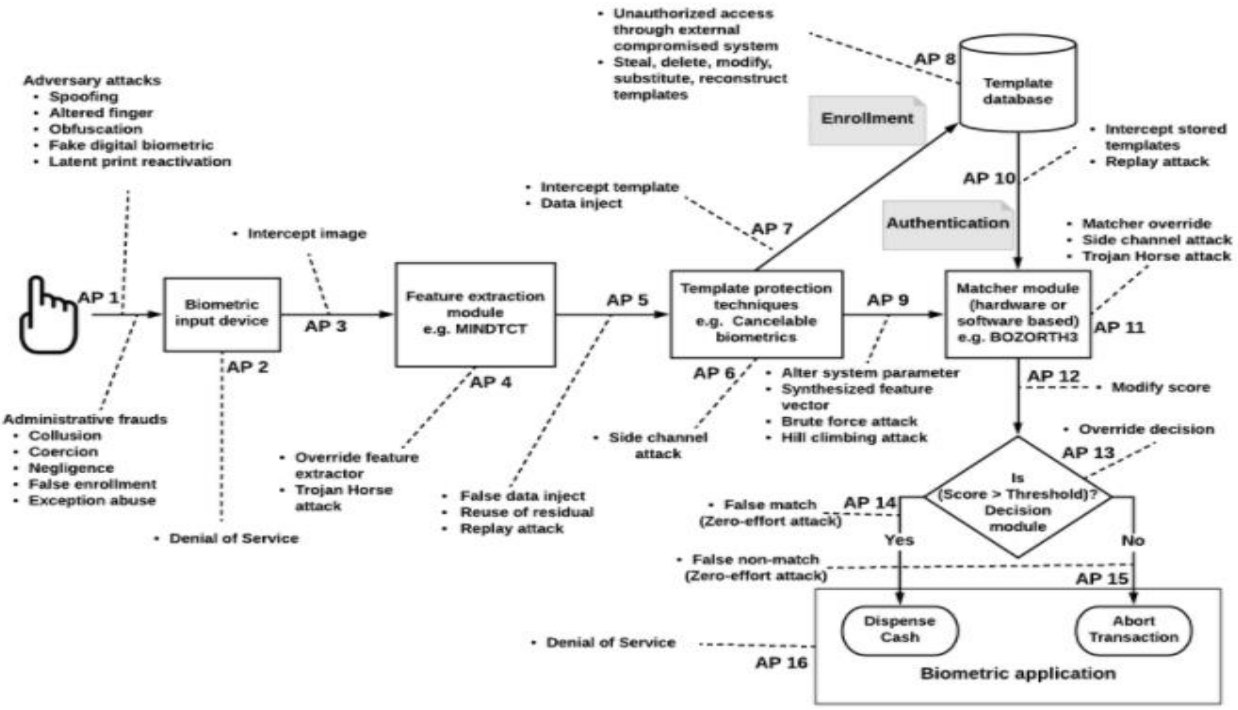
Κεφάλαιο 6. Ασφάλεια βιομετρικών συστημάτων- Επιθέσεις

Σε αυτό το κεφάλαιο παρουσιάζονται αναλυτικά οι τρόποι με τους οποίους μπορεί να επιτεθεί ένας αντίπαλος σε κάθε στάδιο των διαδικασιών που ακολουθούνται για να αυθεντικοποιηθεί ένας χρήστης μέσω των βιομετρικών του χαρακτηριστικών.

6.1 Προοπτική της ασφάλειας στα βιομετρικά συστήματα δακτυλικών αποτυπωμάτων

Ένα βιομετρικό σύστημα μπορεί να είναι ευάλωτο λόγω κάποιων τρωτών σημείων. Το βιομετρικό σύστημα δακτυλικών αποτυπωμάτων μπορεί να είναι ο στόχος του ίδιου του διαχειριστή του συστήματος, ενός εξουσιοδοτημένου χρήστη, ενός απλού ατόμου που επιτίθεται σε μια επίθεση DoS στο βιομετρικό δεδομένο εισόδου ή στη βιομετρική εφαρμογή ή ενός αντιπάλου που έχει γνώση του βιομετρικού συστήματος. Τα σενάρια που αφορούν το διαχειριστή του συστήματος ονομάζονται εσωτερικές επιθέσεις ή διοικητικές απάτες (insider attacks /administrative frauds).

Στο παρακάτω σχήμα παρουσιάζονται επιθέσεις που μπορούν να πραγματοποιηθούν σε διάφορα επίπεδα ενός βιομετρικού συστήματος και παρουσιάζονται στις παρακάτω παραγράφους.



Εικόνα 7: Ευπάθειες και επιθέσεις σε διαφορετικά επίπεδα ενός βιομετρικού συστήματος δακτυλικών αποτυπωμάτων. Ένας αριθμός που αντιστοιχεί σε ένα βέλος ή μια διακεκομμένη γραμμή αντιπροσωπεύει ένα σημείο επίθεσης. *(23)*

6.1.1 Άμεση και έμμεση επίθεση (Direct and Indirect Attack)

Ο αντίπαλος εκτελεί άμεσες επιθέσεις παρουσιάζοντας τα βιομετρικά χαρακτηριστικά ενός εγγεγραμμένου χρήστη στη συσκευή ανίχνευσης ώστε να αποκτήσει πρόσβαση στο σύστημα ως εξουσιοδοτημένος χρήστης. Ο εισβολέας στοχεύει τη συσκευή εισόδου ή την εφαρμογή που ελέγχεται από το βιομετρικό σύστημα για άμεση επίθεση καταστρέφοντάς τα, καθιστώντας το σύστημα απρόσιτο σε αυτούς τους χρήστες. Στην *Εικόνα 7*, αυτές οι επιθέσεις απεικονίζονται ως σημεία επίθεσης AP 1, AP 2 και AP 16. Καθώς η συσκευή ανίχνευσης είναι ένα εξωτερικό στοιχείο του συστήματος και είναι προσβάσιμη σε όλους, ένας εισβολέας χωρίς γνώση του εσωτερικού του βιομετρικού συστήματος μπορεί να εκτελέσει αυτήν την επίθεση (22) .

Αντιθέτως, οι έμμεσες επιθέσεις αναμένουν από τον εισβολέα να έχει εμπειρία σε βιομετρικά συστήματα για να προκαλέσει μια επίθεση. Το άτομο που εμπλέκεται άμεσα σε αυτούς τους τύπους επίθεσης μπορεί να είναι εξουσιοδοτημένος χρήστης ή μη. Η παρακολούθηση των πληροφοριών που μεταδίδονται μέσω του καναλιού επικοινωνίας, τα οποία στοχεύουν τα εσωτερικά στοιχεία του βιομετρικού συστήματος για να παρακάμψουν την έξοδο ή να χειριστεί το αποθηκευμένο πρότυπο είναι

παραδείγματα έμμεσων επιθέσεων. Τα σημεία επίθεσης AP 1, AP 2 και AP 16 στην *Εικόνα 7* εμπίπτουν σε αυτήν την κατηγορία.

6.1.2 Απόρριψη (Repudiation)

Ένα άτομο μπορεί να επωφεληθεί από τον εγγενή περιορισμό του βιομετρικού συστήματος. Ο εισβολέας μπορεί να αρνηθεί να έχει πρόσβαση στο σύστημα υποστηρίζοντας το ψευδές φαινόμενο αποδοχής που σχετίζεται με το σύστημα.

6.1.3 Επιθέσεις ως προς τα βιομετρικά δεδομένα

I. Μόλυνση ή κρυφή απόκτηση (Contamination/covert acquisition)

Ο εξουσιοδοτημένος χρήστης μπορεί να αφήνει , εν αγνοία του, τα ίχνη των δακτυλικών αποτυπωμάτων του στην καθημερινή του ρουτίνα. Ο αντίπαλος αντιγράφει τα βιομετρικά δεδομένα του χρήστη και τα χρησιμοποιεί για να παραβιάσει το σύστημα.

II. Εξαναγκασμός (Coercion)

Ο εξουσιοδοτημένος χρήστης απειλείται από τον αντίπαλο και τον αναγκάζει να του δώσει το δικαίωμα πρόσβασης.

III. Αμέλεια (Negligence)

Ένας νόμιμος χρήστης μπορεί να ξεχάσει να αποσυνδεθεί από τη βιομετρική εφαρμογή ενώ ο εισβολέας τον παρατηρεί. Ο αντίπαλος εκμεταλλεύεται ένα τέτοιο περιστατικό αμέλειας. Συνεχίζει τη διαδικασία προσποιούμενος τον εξουσιοδοτημένο χρήστη και μπορεί να πραγματοποιήσει μερικές ακόμη συναλλαγές ή ακόμη και να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες σχετικά με τον χρήστη.

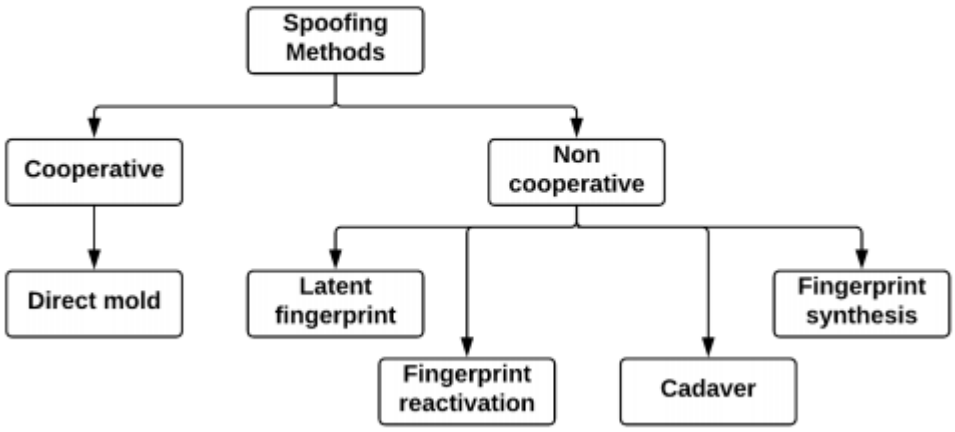
6.1.4 Εσωτερικές επιθέσεις (Insider attacks)

Ο διαχειριστής του συστήματος ή το εξουσιοδοτημένο άτομο μπορεί να βοηθήσει στην εκτέλεση μιας εσωτερικής επίθεσης στο βιομετρικό σύστημα. Ο διαχειριστής αποκαλύπτει τα ελαττώματα του συστήματος στον εισβολέα ή ο νόμιμος χρήστης συνεργάζεται στην εκτέλεση τέτοιων επιθέσεων.

- Συμπαιγνία (Collusion): σε αυτή την περίπτωση ένας νόμιμος χρήστης, όπως ο διαχειριστής συστήματος, με πλήρη δικαιώματα πρόσβασης, είναι ο εισβολέας. Έχει πρόσβαση και παράνομα και τροποποιεί τις παραμέτρους του συστήματος.

Ο εισβολέας μπορεί ακόμα να αλλάξει τα δικαιώματα πρόσβασης ενός εξουσιοδοτημένου χρήστη.

- Απάτη εγγραφής ή ψευδή εγγραφή (Enrollment fraud or false enrollment): ο διαχειριστής είναι η αρχή που συμμετέχει στη φάση εγγραφής. Μπορεί να βοηθήσει τον εισβολέα εγγράφοντας ως νόμιμο χρήστη. Ο διαχειριστής μπορεί να έχει προσωπικό όφελος με την παράνομη εγγραφή για είσοδο σε κυβερνητικούς χώρους με υψηλή ασφάλεια.
- Κατάχρηση εξαίρεσης (Exception abuse): Η διαδικασία χειρισμού εξαιρέσεων που έχει σχεδιαστεί για να διευκολύνει εξουσιοδοτημένους χρήστες σε περίπτωση έκτακτης ανάγκης μπορεί να καταστεί ευάλωτη στο σύστημα. Ο διαχειριστής συστήματος χρησιμοποιεί αυτήν τη δυνατότητα για να βοηθήσει τον εισβολέα να αποκτήσει πρόσβαση στο σύστημα ως εγγεγραμμένος χρήστης. Ο διαχειριστής συστήματος επαναφέρει το προκαθορισμένο κατώφλι σε χαμηλότερη τιμή έτσι ώστε ο αντίπαλος να μπορεί να επωφεληθεί από το σφάλμα ψευδούς αντιστοίχισης και να εξουσιοδοτηθεί.



Εικόνα 8: Μέθοδοι που χρησιμοποιούνται για τη δημιουργία τεχνητών δακτυλικών αποτυπωμάτων *(23)*

- Λειτουργία ερπυσμού (Function creep): ο διαχειριστής μπορεί να συλλέξει βιομετρικά δείγματα ενός ατόμου των οποίων ο αριθμός μπορεί να υπερβαίνει αυτό που θα έπρεπε να αποθηκευτεί για αντιστοίχιση στη φάση ελέγχου ταυτότητας. Τα άλλα χαρακτηριστικά μαζί με τα προσωπικά στοιχεία και τα αναγνωριστικά του χρήστη, όπως ο αριθμός κοινωνικής ασφάλισης, μπορούν

να πωληθούν σε ιδιωτικούς οργανισμούς για οικονομικούς ή άλλους κακόβουλους λόγους.

Το σύστημα, λοιπόν, θα πρέπει να έχει πολλούς διαχειριστές με διαφορετικά επίπεδα προνομίων, έτσι ώστε μια μεμονωμένη αρχή να μην μπορεί να επιτεθεί σε μια εσωτερική επίθεση, όπως συμπαιγνία και κατάχρηση εξαιρέσεων. Η ευθύνη εγγραφής μπορεί επίσης να διανέμεται σε διάφορα τμήματα για να αποφευχθεί η πιθανότητα απάτης εγγραφής. Τέλος μπορεί να εκδοθεί μια έξυπνη κάρτα ταυτότητας σε κάθε υπάλληλο της οποίας η ταυτοποίηση θα εκτελείται από άλλο τμήμα.

6.1.5 Επιθέσεις αισθητήρα (Sensor attacks)

Οι επιθέσεις σε επίπεδο αισθητήρα καθορίζουν πώς ένας εισβολέας μπορεί να αποκτήσει πρόσβαση στο σύστημα με χειραγωγημένη βιομετρική υποβολή σε αυτόν. Οι επιθέσεις στην είσοδο συστήματος καθορίζονται ως Type 1 στην *Εικόνα 7*. Δεδομένου ότι αυτές οι επιθέσεις πραγματοποιούνται στο σημείο εισόδου του βιομετρικού συστήματος, οι μηχανισμοί ασφαλείας που εφαρμόζονται για την ψηφιακή προστασία, όπως τα κρυπτοσυστήματα, είναι αναποτελεσματικοί σε τέτοια σενάρια.

- Επίθεση αντίγραφου/πλαστογράφησης ή επίθεση μίμησης (Spoofing/ mimicry attack): η υποβολή κλεμμένων ή ψεύτικων δακτυλικών αποτυπωμάτων σε ένα βιομετρικό σύστημα ονομάζεται επίθεση πλαστογράφησης. Μια επίθεση πλαστογράφησης αντιπροσωπεύει την παρουσίαση ψευδών δεδομένων, ή ψευδούς βιομετρικού ισχυρισμού ότι είναι νόμιμη, σε μια προσπάθεια παράκαμψης των ελέγχων του βιομετρικού συστήματος (24).Η πλαστογράφηση είναι πιθανώς ο ευκολότερος τρόπος για να εξουσιοδοτηθεί ένας εισβολέας. Για να πετύχει, ο εισβολέας δεν χρειάζεται να γνωρίζει για τα εσωτερικά στοιχεία του συστήματος.
- Μεταμφίεση (Masquerade): η επίθεση μεταμφιέσεων είναι ένας γενικός όρος που δίνεται σε οποιαδήποτε απόπειρα του αντίπαλου να προσποιείται ότι είναι νόμιμος χρήστης για πρόσβαση είτε στο σύστημα είτε στις πληροφορίες και τις υπηρεσίες ενός εγγεγραμμένου χρήστη. Ο εισβολέας σε τέτοιες περιπτώσεις δημιουργεί ψεύτικα δακτυλικά αποτυπώματα ή μεταβάλλει το αποτύπωμα του εξουσιοδοτημένου χρήστη για να πραγματοποιήσει μια επίθεση πλαστογράφησης.

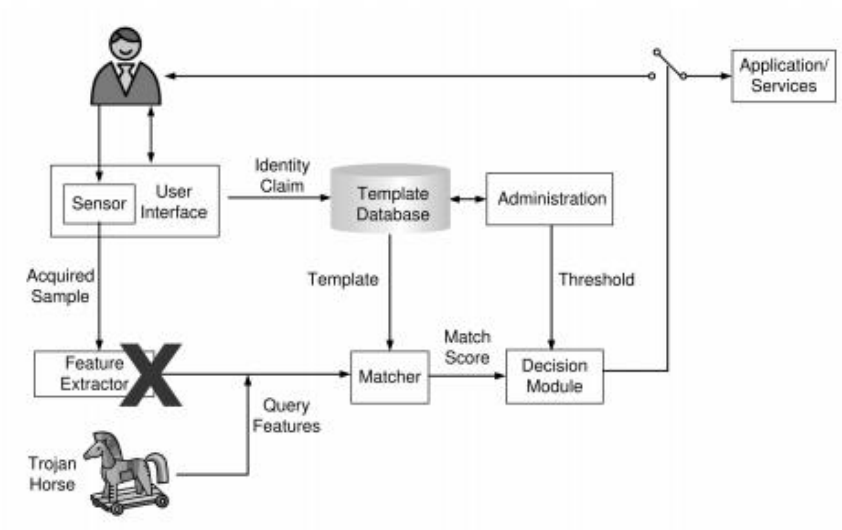
- Τροποποίηση υποβολής δακτυλικών αποτυπωμάτων (Altered fingerprint submission): τα αλλοιωμένα δακτυλικά αποτυπώματα είναι πραγματικά αποτυπώματα που χρησιμοποιούνται για να αποκρύψουν την ταυτότητά τους για να αποφύγουν την ταυτοποίηση από ένα βιομετρικό σύστημα.
- Απόκρυψη (Obfuscation): η απόκρυψη μπορεί να οριστεί ως μια εσκεμμένη προσπάθεια ενός ατόμου να καλύψει την ταυτότητά του από ένα βιομετρικό σύστημα αλλάζοντας το βιομετρικό γνώρισμα πριν από την απόκτησή του από το σύστημα π.χ. ακρωτηριασμός των ακμών των δακτυλικών αποτυπωμάτων αυτών χρησιμοποιώντας λειαντικό υλικό (25). Η τροποποιημένη υποβολή δακτυλικών αποτυπωμάτων εμπίπτει στην κατηγορία της απόκρυψης. Δεν είναι εγγυημένο ότι ένα αλλοιωμένο δακτυλικό αποτύπωμα θα πετύχει πάντα στην αποφυγή του βιομετρικού συστήματος, καθώς ο αριθμός των σημείων λεπτομερειών που εξάγονται από την αμετάβλητη περιοχή πριν και μετά τον ακρωτηριασμό δεν επαρκεί για μια επιτυχημένη αντιστοίχιση σε κάθε περίπτωση.
- Ψεύτικο ψηφιακό βιομετρικό (Fake digital biometric): τα λανθάνοντα ψηφιακά δακτυλικά αποτυπώματα μπορούν να χρησιμοποιηθούν από τον αντίπαλο για να επίθεση μεταμφίεσης. Η επανάληψη ενός σετ χαρακτηριστικών στη μονάδα αντιστοίχισης είναι ένα παράδειγμα επίθεσης με ψεύτικη ψηφιακή βιομετρική υποβολή. Ο αντίπαλος μπορεί να ανακατασκευάσει τα υποκείμενα δεδομένα προτύπου για να εξουσιοδοτηθεί ως γνήσιος χρήστης και έτσι να κρύψει τη δική του ταυτότητα.
- Ψεύτικο φυσικό βιομετρικό (Fake physical biometric): η πλαστογράφηση είναι η διαδικασία δημιουργίας ψεύτικου φυσικού δακτυλικού αποτυπώματος ενός νόμιμου χρήστη για είσοδο στο σύστημα.
- Λανθάνουσα εκτύπωση (Latent print reactivation): μια λανθάνουσα εκτύπωση του δακτυλικού αποτυπώματος θα δημιουργηθεί στην επιφάνεια του βιομετρικού αισθητήρα λόγω της έκκρισης ιδρώτα από αδένες στην παλάμη ή την επαφή με το λιπαρό ή κολλώδες υλικό. Οι εμφανίσεις του δακτυλικού αποτυπώματος στην επιφάνεια του αισθητήρα μπορούν να χρησιμοποιηθούν από τον αντίπαλο για τη δημιουργία ευανάγνωστων εκτυπώσεων.

6.1.6 Επίθεση προς τον εξαγωγέα των χαρακτηριστικών (Feature extractor attacks)

Το επίπεδο εξαγωγής χαρακτηριστικών είναι υπεύθυνο για τον εντοπισμό των μικρολεπτομεριών από την εικόνα δακτυλικών αποτυπωμάτων που δημιουργείται από τη συσκευή εισόδου. Ο αντίπαλος μπορεί να στοχεύσει τη μονάδα εξαγωγής χαρακτηριστικών έτσι ώστε να είναι ανίκανη να δημιουργήσει το πραγματικό χαρακτηριστικό που αντιστοιχεί στο αποτυπωμένο δακτυλικό αποτύπωμα.

- Παράκαμψη εξαγωγής χαρακτηριστικών (Override feature extractor): η επίθεση στη μονάδα εξαγωγής χαρακτηριστικών από τον αντίπαλο περιλαμβάνει την αντικατάσταση του σετ χαρακτηριστικών που εξήχθη από τη μονάδα με το σετ χαρακτηριστικών που επέλεξε ο εισβολέας. Αυτό συνήθως πραγματοποιείται μέσω επίθεσης στο software ή το hardware του βιομετρικού συστήματος (24).

- Επίθεση Δούρειος ίππος (Trojan horse attack): η Εικόνα *9* δείχνει μια επίθεση Trojan Horse εναντίον της μονάδας εξαγωγής χαρακτηριστικών. Αυτού του είδους η επίθεση διακόπτει τη διαδικασία του βιομετρικού συστήματος για να παρακάμψει την εξαγωγή χαρακτηριστικών. Είναι ένα κακόβουλο πρόγραμμα που μπορεί να ελεγχθεί από απόσταση από τον αντίπαλο μέσω εντολών. Μόλις ενεργοποιηθεί, μπορεί να διαγράψει, να αντιγράψει ή να τροποποιήσει τα δεδομένα από το σύστημα.



Εικόνα 9: Μια επίθεση Trojan Horse εναντίον της μονάδας εξαγωγής χαρακτηριστικών *(26)*

6.1.7 Επιθέσεις στο τεχνικό επίπεδο προστασίας προτύπων (Attacks on template protection techniques module)

Τα χαρακτηριστικά που εξάγονται από τη μονάδα εξαγωγής χαρακτηριστικών χρησιμοποιούνται για τη δημιουργία ενός ασφαλούς ψηφιακού προτύπου χρησιμοποιώντας κρυπτογραφικές τεχνικές. Η μονάδα προστασίας προτύπων που είναι υπεύθυνη για την εκτέλεση της μετάφρασης ενός διανύσματος χαρακτηριστικών σε ένα βιομετρικό πρότυπο με κρυπτογραφημένη ασφάλεια είναι πιθανός στόχος του εισβολέα. Ο εισβολέας στοχεύει να εξαγάγει πληροφορίες σχετικά με το κλειδί που χρησιμοποιείται στον αλγόριθμο κρυπτογράφησης. Οι επιθέσεις στη μονάδα τεχνικής προστασίας προτύπων καθορίζονται ως AP 6 στην Εικόνα *7*.

Οι επιθέσεις μέσω της παρακολούθησης καναλιών (Side channel attacks-SCA) στοχεύουν μια συγκεκριμένη τεχνολογία που ανακτά το ενσωματωμένο μυστικό κλειδί του κρυπτοσυστήματος (27) .Σε αυτές τις επιθέσεις, ο αντίπαλος χρησιμοποιεί τη διαρροή πληροφοριών, όπως στατιστικά κατανάλωσης ενέργειας, πληροφορίες χρονισμού ή την ηλεκτρομαγνητική ακτινοβολία για να ανακτήσει το κλειδί του αλγορίθμου κρυπτογράφησης. Ένα ηλεκτρομαγνητικό πεδίο δημιουργείται λόγω της κίνησης των ηλεκτρικών φορτίων. Οι ηλεκτρομαγνητικές επιθέσεις εκμεταλλεύονται συσχετισμούς μεταξύ ενδιάμεσων δεδομένων (λειτουργία του μυστικού κλειδιού) και παραλλαγές στις ηλεκτρομαγνητικές εκπομπές από συσκευές ανθεκτικές σε παραβιάσεις, όπως έξυπνες κάρτες (28). Κατά τον συγχρονισμό επιθέσεων καναλιού, ο χρόνος εκτέλεσης ενός κρυπτογραφικού αλγορίθμου αποκαλύπτει τις πολύτιμες πληροφορίες που σχετίζονται με τον μυστικό κώδικα που εμπλέκεται στον υπολογισμό, όπως ένα κλειδί κρυπτογράφησης.

6.1.8 Επιθέσεις ως προς την αντιστοίχιση (Matcher module attacks)

Η μονάδα αντιστοίχισης στο βιομετρικό σύστημα είναι ένα στοιχείο υλικού ή λογισμικού που είναι υπεύθυνο για την εκτέλεση της αντιστοίχισης μεταξύ του προτύπου που δημιουργείται από ζωντανό δακτυλικό αποτύπωμα και του αποθηκευμένου προτύπου κατά τη φάση ελέγχου ταυτότητας. Η έξοδος του αλγόριθμου αντιστοίχισης είναι η βαθμολογία ομοιότητας μεταξύ των δύο προτύπων. Ο αντίπαλος που στοχεύει τη μονάδα αντιστοίχισης στοχεύει στην επίτευξη βαθμολογίας αντιστοίχισης πάνω από το προκαθορισμένο όριο για μη εγγεγραμμένο

δακτυλικό αποτύπωμα. Οι επιθέσεις αυτού του είδους καθορίζονται ως AP 11 στην Εικόνα *7*.

I. Επίθεση αναρρίχησης (Hill climbing attack):κλιμακούμενη επαναλαμβανόμενη επίθεση στους δείκτες ομοιότητας. Πιο συγκεκριμένα, σε ένα δείγμα επιφέρεται μία μικρή τροποποίηση και αν η βαθμολογία ομοιότητας βελτιωθεί, τότε η τροποποίηση διατηρείται, αλλιώς απορρίπτεται. Αυτή η διαδικασία επαναλαμβάνεται μέχρι η βαθμολογία ομοιότητας κάποια στιγμή να ξεπεράσει το ορισμένο όριο αποδοχής.

II. Παράκαμψη αντιστοίχισης ή λάθος αντιστοίχιση (Matcher override / false match): ο αντίπαλος που στοχεύει τη μονάδα αντιστοίχισης παρακάμπτει τη βαθμολογία που δημιουργήθηκε για τη σύγκριση προτύπων με μια βαθμολογία αντιστοίχισης πάνω από το προκαθορισμένο όριο.

III. Trojan horse attack: καταστέλλεται η πραγματική έξοδος βαθμολογίας αντιστοίχισης του συγκριτή με την προκαθορισμένη βαθμολογία έτσι ώστε ο αντίπαλος να μπορεί να παρακάμψει όλα τα προηγούμενα στάδια στο βιομετρικό σύστημα και να εξακολουθεί να έχει άδεια πρόσβασης στο εφαρμογή.

IV. Επιθέσεις παρακολούθησης καναλιού (Side channel attacks): ανάλυση του χρόνου και της ενέργειας που απαιτούνται από τον αλγόριθμο για διάφορες λειτουργίες. Για παράδειγμα, υπάρχει συσχέτιση του χρόνου με τον δείκτη ομοιότητας, όσο πιο υψηλός είναι ο δείκτης απαιτείται και περισσότερος χρόνος (29).

- Απλή ανάλυση ισχύος (Simple power analysis-SPA): το ρεύμα που ρέει από τη μονάδα τροφοδοσίας στη μονάδα αντιστοίχισης ενός βιομετρικού συστήματος μπορεί να αναλυθεί για να ανιχνεύσει μοτίβα κατανάλωσης ισχύος που διαρρέουν τις πληροφορίες που σχετίζονται με τις κρυπτογραφικές λειτουργίες. Ο αντίπαλος θεωρείται ότι από την ανάλυση της ενέργειας μπορεί να αποκτήσει γνώσεις για τον πίνακα που περιέχει αποθηκευμένα τα βιομετρικά δεδομένα. Οι πιο συνηθισμένες άμυνες εναντίον του SCA περιλαμβάνουν την προσθήκη θορύβου, εικονικές οδηγίες και εξισορρόπηση κατανάλωσης ενέργειας.
- Ανάλυση ισχύος συσχέτισης (Correlation power analysis-CPA): είναι ένα στατιστικό εργαλείο που χρησιμοποιεί την απόσταση Hamming για την αξιολόγηση διαρροής της κρυπτογραφικής μονάδας ή / και την ανάκτηση των

μυστικών δεδομένων όπως το κλειδί κρυπτογράφησης ή πληροφορίες των μικρολεπτομεριών σε περίπτωση βιομετρικού συστήματος δακτυλικών αποτυπωμάτων.

- Ανάλυση διαφορικής ισχύος (Differential power analysis-DPA): η εφαρμογή τεχνικών ανάλυσης διαφορικής ισχύος στην αντιστοίχιση δακτυλικών αποτυπωμάτων είναι δύσκολη λόγω του σχετικά μεγάλου αριθμού των προτύπων και της γραμμικότητας των αλγορίθμων αντιστοίχισης (30).

Αντιμετώπιση (Side channel attacks- SCA): η τεχνική της απόκρυψης (masking) προτείνεται συνήθως ως τρόπος αντιμετώπισης των επιθέσεων DPA (31). Επίσης, για να αποφευχθεί ο απομακρυσμένος έλεγχος της ενέργειας με τη βοήθεια του φάσματος είναι ο αλγόριθμος να είναι ισόποσα κατανεμημένος ώστε να μη φαίνεται σε ποιο σημείο γίνονται οι κρυπτογραφικές πράξεις (32).

6.1.9 Επιθέσεις των προτύπων στη βάση δεδομένων

Η βάση δεδομένων των προτύπων αποθηκεύει κρυπτογραφημένα βιομετρικά στοιχεία και λεπτομέρειες για κάθε εγγεγραμμένο χρήστη. Το βιομετρικό σύστημα χρησιμοποιεί ένα αποθηκευμένο πρότυπο και πληροφορίες που αντιστοιχούν σε αυτό για να εκτελέσει την ταυτοποίηση και την επαλήθευση ενός χρήστη στη φάση ελέγχου ταυτότητας. Η κύρια πρόθεση του εισβολέα είναι να επαναχρησιμοποιήσει ή να παραβιάσει τα αποθηκευμένα πρότυπα. Τα κλεμμένα βιομετρικά στοιχεία μπορούν να χρησιμοποιηθούν για να επιχειρήσουν μια επίθεση man-in-the-middle, όπως μια επίθεση επανάληψης (replay attack). Ο εισβολέας μπορεί να διαγράψει τα αποθηκευμένα πρότυπα για να εκτελέσει μια επίθεση DoS (Denial Of Service). Η Εικόνα *7* αντιπροσωπεύει μια επίθεση στη βάση δεδομένων ως AP 8.

- Αναδημιουργία προτύπου (Template reconstruction): ο εισβολέας εισβάλλει στην ηλεκτρονική βάση δεδομένων όπου τα κρυπτογραφημένα βιομετρικά δεδομένα αποθηκεύονται, σπάζοντας έναν λογαριασμό βάσης δεδομένων με δικαιώματα διαχειριστή ή εκμεταλλευόμενος την ευπάθεια στο λογισμικό της βάσης δεδομένων. Τροποποιεί τα υπάρχοντα κρυπτογραφημένα βιομετρικά στοιχεία ή ανακατασκευάζει ένα νέο πρότυπο από αυτά. Τα τροποποιημένα και ανακατασκευασμένα πρότυπα αποτελούν τη βάση για μια επίθεση επανάληψης. Εάν ο εισβολέας μπορεί να παραποιήσει και να τροποποιήσει τις πληροφορίες του προτύπου και να δημιουργήσει ένα ψευδές αναγνωριστικό σε ένα παράνομο

άτομο, αυτό ονομάζεται επίθεση τροποποίησης προτύπου. Ο αντίπαλος μπορεί να χρησιμοποιήσει τα τροποποιημένα βιομετρικά για να εκτελέσει hill-climbing attack στο AP 9 στην Εικόνα 7. Ένας πιθανός τρόπος για τον μετριασμό της ανακατασκευής δακτυλικών αποτυπωμάτων από το αποθηκευμένο πρότυπο είναι να δημιουργήσουμε πρότυπα από κρυπτογραφημένα λεπτομερή στοιχεία αντί να αποθηκεύουμε τα λεπτομερή αυτά στοιχεία στο πρότυπο.

- Μη εξουσιοδοτημένη τροποποίηση προτύπου (Unauthorized template modification): ο εισβολέας μπορεί να στοχεύσει την ηλεκτρονική βάση δεδομένων από ένα εξωτερικό σύστημα που έχει παραβιαστεί. Μια τέτοια προσπάθεια είναι δύσκολο να εντοπιστεί, καθώς το παραβιασμένο σύστημα είναι ως επί το πλείστον ένας ηλεκτρονικός υπολογιστής που έχει παραβιαστεί υπό τον έλεγχο του εισβολέα. Ο αντίπαλος μπορεί να κλέψει τα πρότυπα για να εκτελέσει επίθεση επανάληψης. Μπορεί ακόμη και να διαγράψει και να αντικαταστήσει τα πρότυπα για να εκτελέσει μια επίθεση DoS για τους γνήσιους χρήστες.
- Παράκαμψη (Circumvention): η απειλή παράκαμψης μπορεί να χαρακτηριστεί ως επίθεση απορρήτου, όπου ο εισβολέας λαμβάνει τα μη εξουσιοδοτημένα δεδομένα (για παράδειγμα, πρόσβαση στα ιατρικά αρχεία ενός άλλου χρήστη) ή, ως επίθεση όπου ο εισβολέας χειρίζεται το σύστημα (για παράδειγμα, αλλάζοντας αυτά τα αρχεία , υποβολή πλαστών ασφαλιστικών απαιτήσεων, κ.λπ.) (33).Ο αντίπαλος εξουσιοδοτείται προσπαθώντας οποιαδήποτε επίθεση, όπως πλαστογράφηση, επανάληψη, διοικητικές απάτες κ.λπ., να αποκτήσει πρόσβαση στην εφαρμογή και, στη συνέχεια, να παρακάμψει τα δεδομένα της εφαρμογής.

6.1.10 Man in The Middle (MiTM) attack

Σε ένα τυπικό σενάριο μιας MiTM επίθεσης στο βιομετρικό σύστημα, ο εισβολέας παρεμποδίζει το κανάλι επικοινωνίας να συλλέξει τα βιομετρικά δεδομένα ενός νόμιμου χρήστη. Ο εισβολέας, σε αυτήν την περίπτωση, μπορεί να στοχεύσει στα σημεία AP 3, AP 5, AP 7, AP 9, AP 10 και AP 12 από την Εικόνα 7 στο βιομετρικό σύστημα. Αυτές οι επιθέσεις είναι παρόμοιες με τις επιθέσεις επανάληψης, όπου ο εισβολέας παρακολουθεί το κανάλι επικοινωνίας κατά τη λήψη των βιομετρικών

δεδομένων και στη συνέχεια τροποποιεί αυτά τα δεδομένα για πρόσβαση στο σύστημα ως νόμιμος χρήστης.

- Επίθεση επανάληψης (Replay attack): στην επίθεση επανάληψης (επίσης γνωστή ως επίθεση ψευδούς εισαγωγής δεδομένων), ένας εισβολέας παρακάμπτει το σαρωτή και χρησιμοποιεί την ψηφιακή εικόνα που είχε δημιουργηθεί προηγουμένως από έναν νόμιμο χρήστη για πρόσβαση στο σύστημα. Αναπαρίσταται ως AP 5 στην *Εικόνα 7*, και απαιτεί από τον εισβολέα να έχει καλή γνώση του συστήματος και της βάσης δεδομένων. διακυβεύονται.

Μια μέθοδος για τον μετριασμό μιας επίθεσης επανάληψης υποθέτει ότι ο αισθητήρας είναι αρκετά έξυπνος για να ανταποκριθεί σε ένα ερώτημα από έναν ασφαλή διακομιστή συναλλαγών. Κάθε φορά που ο αισθητήρας αγγίζεται με ένα δάχτυλο χρήστη, ο διακομιστής συναλλαγών στέλνει ένα ερώτημα, π.χ. μια τυχαία τιμή pixel, στον αισθητήρα. Εάν η εικόνα που λαμβάνεται από τον εξαγωγέα χαρακτηριστικών έχει την ίδια τιμή εικονοστοιχείου με την ανταπόκριση του αισθητήρα, τότε η συναλλαγή συνεχίζεται, διαφορετικά μια προσπάθεια παράκαμψης του αισθητήρα εντοπίζεται και η συναλλαγή ματαιώνεται.

- Επαναχρησιμοποίηση υπολειμμάτων (Reuse of residuals) : το βιομετρικό σύστημα μπορεί να κρατήσει το ανακτημένο ψηφιακό πρότυπο στην κύρια μνήμη του για κάποιο χρονικό διάστημα μετά την εκτέλεση της αντίστοιχης λειτουργίας. Ο αντίπαλος μπορεί να χρησιμοποιήσει τα διαθέσιμα βιομετρικά στοιχεία στην κύρια μνήμη για πρόσβαση στο σύστημα ως νόμιμος χρήστης. Αναπαρίσταται στο AP 5 στην *Εικόνα 7* .
- Παράκαμψη παραμέτρου συστήματος ή τροποποίηση (System parameter override or modification): ο εισβολέας χειρίζεται τις παραμέτρους του συστήματος για να διευρύνει το εύρος της ψευδούς αποδοχής και στη συνέχεια να μειώσει το περιθώριο ψευδούς απόρριψης. Ως αποτέλεσμα μιας τέτοιας αλλαγής παραμέτρων συστήματος (FMR, FNMR παράγρ.5.1.1), ο αντίπαλος δημιουργεί μια διαδρομή για πρόσβαση στην εφαρμογή στην *Εικόνα 7* με εικόνες δακτυλικών αποτυπωμάτων κακής ποιότητας ή λανθασμένα δεδομένα.
- Διάνυσμα συνθετικών χαρακτηριστικών (Synthesized feature vector): ο αντίπαλος με γνώση του βιομετρικού συστήματος μπορεί να δημιουργήσει

ένα βιομετρικό πρότυπο έξω από το σύστημα και να το εισάγει απευθείας στη ροή δεδομένων του καναλιού επικοινωνίας. Η επίθεση αναρρίχησης (Hill climbing attack) μπορεί να χρησιμοποιήσει αυτό το συνθετικό πρότυπο στο AP 9 στην *Εικόνα 7*.

- Βίαιη επίθεση (Brute force attack): μεγάλος αριθμός δοκιμών ενός συνόλου βιομετρικών χαρακτηριστικών για να βρεθεί ένα που να μπορέσει να παραβιάσει το σύστημα. Αναπαρίστανται στην *Εικόνα 7* στο AP 4.
- Υποκλοπή καναλιού αποθήκευσης και εισαγωγή δεδομένων (Storage channel intercept and data inject): ο εισβολέας μπορεί να εισάγει ψευδή δεδομένα απευθείας στη ροή δεδομένων που είναι συνδεδεμένη στη βάση δεδομένων. Μια τέτοια απειλή παρουσιάζεται ως AP 7 και AP 10 στην *Εικόνα 7*. Τα δεδομένα που μεταδίδονται μέσω του καναλιού επικοινωνίας μπορούν να κρυπτογραφηθούν για να αποφευχθεί η υποκλοπή.
- Τροποποίηση βαθμολογίας: ο αντίπαλος μπορεί να διευκολύνει τη διαδικασία ελέγχου ταυτότητας τροποποιώντας τη βαθμολογία αντιστοίχισης μεταξύ του καναλιού που συνδέει τη μονάδα αντιστοίχισης και τη μονάδα απόφασης. Παρακάμπτει τον πραγματικό δείκτη με υψηλότερο πάνω από το όριο. Η *Εικόνα 7* αντιπροσωπεύει μια απειλή όπως το AP 12.

6.1.11 Τροποποίηση δικαιωμάτων πρόσβασης

Ο διαχειριστής εγγράφει χρήστες με διαφορετικά δικαιώματα πρόσβασης στη βιομετρική εφαρμογή. Εάν ο αντίπαλος μειώσει τα δικαιώματα ενός υψηλά προνομιούχου χρήστη, τότε οδηγεί σε επίθεση DoS. Το σύστημα απειλείται όταν ένας χρήστης εγγεγραμμένος με δικαιώματα χαμηλής πρόσβασης αποκτά ξαφνικά δικαιώματα διαχειριστή. Σε κάθε περίπτωση, ο αντίπαλος πρέπει αρχικά να αποκτήσει διαπιστευτήρια διαχειριστή συστήματος.

6.1.12 Παράκαμψη απόφασης

Η ενότητα αποφάσεων αποδέχεται ή απορρίπτει έναν χρήστη ως εγγεγραμμένο και εξουσιοδοτημένο με βάση τη σύγκριση μεταξύ του δείκτη ομοίτητας που προκύπτει και τον προκαθορισμένο. Ο εισβολέας μπορεί να χρησιμοποιήσει Trojan horse για να παρακάμψει την ενότητα αποφάσεων και να δώσει το αποτέλεσμα υπέρ του. Για

παράδειγμα, μια τέτοια επίθεση μπορεί να χρησιμοποιηθεί από τον αντίπαλο για να παραχωρήσει πρόσβαση στην εφαρμογή στην *Εικόνα 7* ή να απαγορεύσει σε όλους τους άλλους χρήστες τη χρήση της εφαρμογής.

6.1.12.1 Επίθεση άρνησης υπηρεσίας (Denial of service -DoS)

Η επίθεση DoS καθιστά το σύστημα απρόσιτο στους εξουσιοδοτημένους χρήστες. Για ένα σύστημα βιομετρικού ελέγχου ταυτότητας, ένας διαδικτυακός διακομιστής ελέγχου ταυτότητας που επεξεργάζεται αιτήματα πρόσβασης μπορεί να βομβαρδιστεί με πολλά ψεύτικα αιτήματα πρόσβασης σε ένα σημείο, όπου οι υπολογιστικοί πόροι του διακομιστή δεν μπορούν να χειριστούν έγκυρα ζητά πια (33).

6.1.13 Εισχώρηση/Εισβολή (Intrusion)

Στην επίθεση εισβολής, η κακόβουλη οντότητα εισβάλλει στην ενότητα αποθήκευσης προτύπων μέσω ενός εξωτερικού συστήματος. Το σενάριο όπου το σύστημα αναγνωρίζει έναν απατεώνα ως εξουσιοδοτημένο χρήστη είναι επίσης περίπτωση εισβολής. Η ενίσχυση της ασφάλειας του διακομιστή έναντι όλων των πιθανών τρωτών σημείων, τα στοιχεία ελέγχου πρόσβασης στη βάση δεδομένων, η υπογραφή αποθηκευμένων προτύπων, η αποθήκευση κρυπτογραφημένων προτύπων μπορούν να είναι τα πιθανά αντίμετρα κατά της εισβολής.

6.1.14 Επιθέσεις μηδενικής προσπάθειας (Zero-effort attacks)

Η επίθεση μηδενικής προσπάθειας είναι ένα όφελος που λαμβάνει ένας αντίπαλος και το πρόβλημα που αντιμετωπίζει ένας εγγεγραμμένος χρήστης λόγω των περιορισμών του συστήματος. Πρόκειται για εσφαλμένο έλεγχο ταυτότητας (ένας μη εγγεγραμμένος χρήστης πιστοποιείται λόγω σφάλματος) και σενάριο απόρριψης (ένας εγγεγραμμένος χρήστης απορρίπτεται λόγω σφάλματος). Αυτή η επίθεση είναι το αποτέλεσμα της μετατόπισης του προκαθορισμένου κατωφλίου σε χαμηλότερη ή υψηλότερη τιμή. Η Εικόνα *7* δείχνει αυτό το σενάριο ως AP 14 και AP 15.

6.2 Μοντέλα Απειλών(Threat Models)

Σε αυτήν την ενότητα, παρουσιάζονται μοντέλα απειλών που υπάρχουν για ένα βιομετρικό σύστημα δακτυλικών αποτυπωμάτων. Ένα μοντέλο απειλής είναι ένας τρόπος αναγνώρισης διαφόρων επιθέσεων (ή πιθανών απειλών) σε ένα σύστημα.

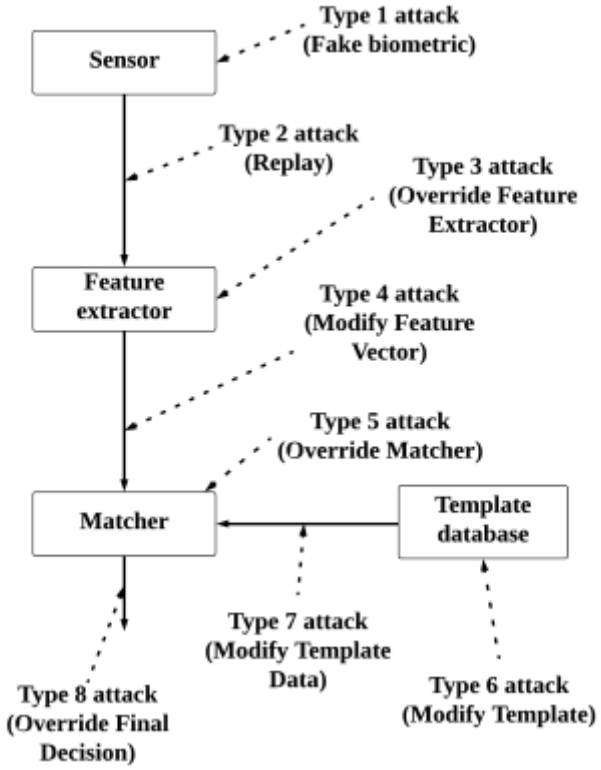
Παρουσιάζονται τέσσερα μοντέλα που επισημαίνουν διαφορετικές επιθέσεις και ευπάθειες στο βιομετρικό σύστημα.

6.2.1 Μοντέλο Ratha et al.

Το μοντέλο Ratha et al. που φαίνεται στην Εικόνα 10 είναι το πρώτο μοντέλο απειλής που προτείνεται για ένα βιομετρικό σύστημα δακτυλικών αποτυπωμάτων. Προσδιορίζει οκτώ ευπάθειες με βάση το σημείο πρόσβασης των πληροφοριών σε ένα βιομετρικό σύστημα (34).Αυτές οι ευπάθειες οδηγούν σε έναν συγκεκριμένο τύπο επίθεσης, που αντιπροσωπεύεται ως Τύπος 1 έως Τύπος 8, στα στοιχεία του συστήματος.

Επίθεση τύπου 1: Σύμφωνα με το μοντέλο, οι αισθητήρες είναι επιρρεπείς σε πλαστογράφηση.

Επίθεση τύπου 2: Η παρακολούθηση του καναλιού επικοινωνίας μεταξύ αισθητήρα και εξαγωγέα χαρακτηριστικών από τον αντίπαλο αποτελεί τη βάση για την επίθεση τύπου 2. Το Masquerading είναι μια επίθεση τύπου 2.



Εικόνα 10: Οι Ratha et al. μοντέλο *(34)* : Τα διακεκομμένα βέλη υποδεικνύουν το σημείο πρόσβασης τωνπληροφοριών για την τοποθέτηση ενός συγκεκριμένου τύπου επίθεσης

Επίθεση τύπου 3: Ο εισβολέας μπορεί να παρακάμψει τη μονάδα εξαγωγής χαρακτηριστικών με τη βοήθεια ενός Trojan horse .

Επίθεση τύπου 4: Το κανάλι επικοινωνίας μεταξύ του προγράμματος εξαγωγής χαρακτηριστικών και της αντιστοίχισης μπορεί να στοχευτεί από τον εισβολέα. Ο αντίπαλος αναχαιτίζει τα χαρακτηριστικά που μεταδίδονται μέσω του καναλιού επικοινωνίας και το επαναλαμβάνει μετά από ένα χρονικό κενό. Τα προηγουμένως παρεμποδισμένα και αλλοιωμένα / τροποποιημένα σύνολα χαρακτηριστικών μπορούν να μεταδοθούν απευθείας στη φάση αντιστοίχισης παρακάμπτοντας τη μονάδα εξαγωγής χαρακτηριστικών.

Επίθεση τύπου 5: Απειλή για τη μονάδα αντιστοίχισης που παρακάμπτει το δείκτη ομοιότητας χρησιμοποιώντας ένα Trojan horse . Σε αυτήν την επίθεση, ο αντίπαλος στέλνει εντολές εξ αποστάσεως για να δημιουργήσει μια υψηλή βαθμολογία αντιστοίχισης και να στείλει θετική απόκριση στη βιομετρική ελεγχόμενη εφαρμογή και να παρακάμψει εντελώς τη διαδικασία ελέγχου ταυτότητας. Μπορεί ακόμη και να προκαλέσει επίθεση DoS, δίνοντας εντολή να δημιουργήσει επ 'αόριστον χαμηλό δείκτη ομοιότητας.

Επίθεση τύπου 6: Ο εισβολέας μπορεί να διερευνήσει τρόπους διαρροής της βάσης δεδομένων. Ο αντίπαλος όχι μόνο συλλέγει τα αποθηκευμένα πρότυπα που έχουν διαρρεύσει, αλλά και τα επαναπληρώνει και τα τροποποιεί για να εξουσιοδοτηθεί για λογαριασμό διαφορετικών εγγεγραμμένων χρηστών.

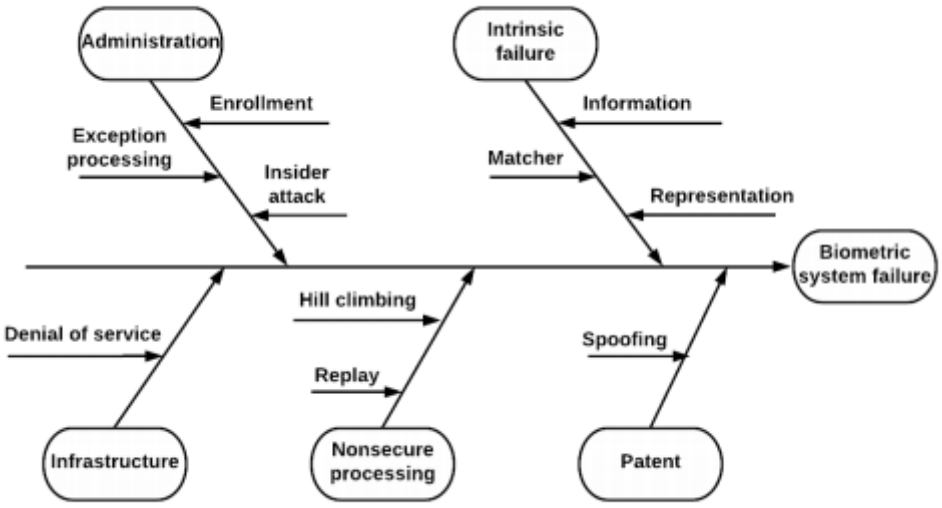
Επίθεση τύπου 7: Στο σενάριο επίθεσης τύπου 7, ο αντίπαλος παρακολουθεί το κανάλι επικοινωνίας μεταξύ της βάσης δεδομένων προτύπων και της μονάδας αντιστοίχισης για τη συλλογή προτύπων από τη ροή δεδομένων. Αυτά τα αναχαιτισμένα πρότυπα μπορούν να αναπαραχθούν άμεσα ή να τροποποιηθούν και στη συνέχεια να αναπαραχθούν στη μονάδα αντιστοίχισης για πρόσβαση στο σύστημα με την ταυτότητα διαφορετικών χρηστών.

Επίθεση τύπου 8: Ο αντίπαλος μπορεί να παρακάμψει όλα τα στοιχεία του συστήματος και να χειριστεί άμεσα την απόφαση του συστήματος υπέρ του. Μια επίθεση για παράκαμψη της τελικής απόφασης του βιομετρικού

συστήματος υπέρ του αντιπάλου ακυρώνει τα εξαιρετικά χαρακτηριστικά απόδοσης της βιομετρικής εφαρμογής.

6.2.2 Το μοντέλο fishbone

Η Εικόνα *11* δείχνει το μοντέλο fishbone (αιτία και αποτέλεσμα) (35) .Το μοντέλο απεικονίζει τις αιτίες που καθορίζουν την ευπάθεια ενός βιομετρικού συστήματος. Εντοπίζονται πέντε αιτίες που οδηγούν σε ευπάθειες στο βιομετρικό σύστημα. Τα βέλη καθορίζουν τα αποτελέσματα, δηλαδή τις πιθανές επιθέσεις λόγω αυτών των αιτιών.



Εικόνα 11: Μοντέλο Fishbone *(35)* .Τα μπλοκ υποδηλώνουν τις φάσεις επεξεργασίας ενός βιομετρικού συστήματος που είναι ευάλωτοι στόχοι σε αυτό το μοντέλο. Οι πιθανές επιθέσεις αναφέρονται στα βέλη.

I. Η **εγγενής αποτυχία (Intrinsic failure)** περιλαμβάνει τους περιορισμούς του συστήματος και τα λάθη που ευθύνονται για την εσφαλμένη αποδοχή ενός μη εγγεγραμμένου ατόμου ή την εσφαλμένη απόρριψη ενός εγγεγραμμένου χρήστη. Οι παραλλαγές μεταξύ χρηστών προκαλούν μεγάλες παραλλαγές στα ζωντανά και αποθηκευμένα πρότυπα του εγγεγραμμένου χρήστη που οδηγούν σε ψευδή απόρριψη. Αυτό το σφάλμα μπορεί να οφείλεται σε ακατάλληλη τοποθέτηση του δακτύλου στον αισθητήρα. Η έλλειψη ατομικότητας ή μοναδικότητας (κυρίως μεταξύ των διδύμων στο σύστημα αναγνώρισης προσώπου) μπορεί να οδηγήσει σε μεγάλη ομοιότητα μεταξύ των συνόλων χαρακτηριστικών δύο διαφορετικών ατόμων που οδηγούν σε ψευδή απόρριψη.
II. Η **αιτία διαχείρισης (Administration cause)** περιγράφει τους τρόπους με τους οποίους ένα ανέντιμο προσωπικό, όπως ένας διαχειριστής συστήματος μπορεί

να παίξει το ρόλο ενός αντιπάλου. Ένας ανέντιμος διαχειριστής μπορεί να βοηθήσει έναν αντίπαλο είτε να επιτύχει μια επιτυχημένη επίθεση, είτε να προκαλέσει απάτη εγγραφής ή κατάχρηση εξαίρεσης.

III. Οι **αιτίες της υποδομής (Infrastructure causes)** περιλαμβάνουν ελαττώματα σχεδιασμού συστήματος που καθιστούν το σύστημα ευαίσθητο σε επιθέσεις. Τα εξαρτήματα υλικού όπως ο αισθητήρας, το λογισμικό που υλοποιείται στη μονάδα εξαγωγής χαρακτηριστικών και στη μονάδα αντιστοίχισης μαζί με το κανάλι επικοινωνίας μεταξύ διαφόρων στοιχείων του συστήματος αποτελούν την υποδομή του βιομετρικού συστήματος. Ένα πρόγραμμα Δούρειου ίππου μπορεί να χρησιμοποιηθεί από τον αντίπαλο για να παρακάμψει το πρόγραμμα αντιστοίχισης ή απόφασης.

IV. Οι **αιτίες μη ασφαλούς επεξεργασίας (Non-secure processing causes)** επισημαίνουν τις ευπάθειες που οφείλονται σε ανασφαλή διαδικασία εγγραφής και ελέγχου ταυτότητας. Ο αντίπαλος μπορεί με hill-climbing ή replay attack να υποκλέψει τις πληροφορίες και να εξουσιοδοτηθεί παρακάμπτοντας τον αισθητήρα. Η μη ασφαλής βάση δεδομένων μπορεί να διαρρεύσει τα αποθηκευμένα πρότυπα. Ο αντίπαλος χρησιμοποιεί τα πρότυπα που συλλέγονται έτσι για να επιτεθεί μια επίθεση επανάληψης. Η λειτουργία ερπυσμού είναι ένα φαινόμενο διασταύρωσης των βιομετρικών χαρακτηριστικών ενός εγγεγραμμένου χρήστη. Ο αντίπαλος συλλέγει τα βιομετρικά στοιχεία ενός χρήστη είτε μέσω διαρροής βάσης δεδομένων είτε μέσω καναλιού επικοινωνίας από το σύστημα του εργοδότη του και το χρησιμοποιεί σε άλλες εφαρμογές όπως τραπεζικές υπηρεσίες, υπηρεσίες διαβατηρίων κ.λπ.

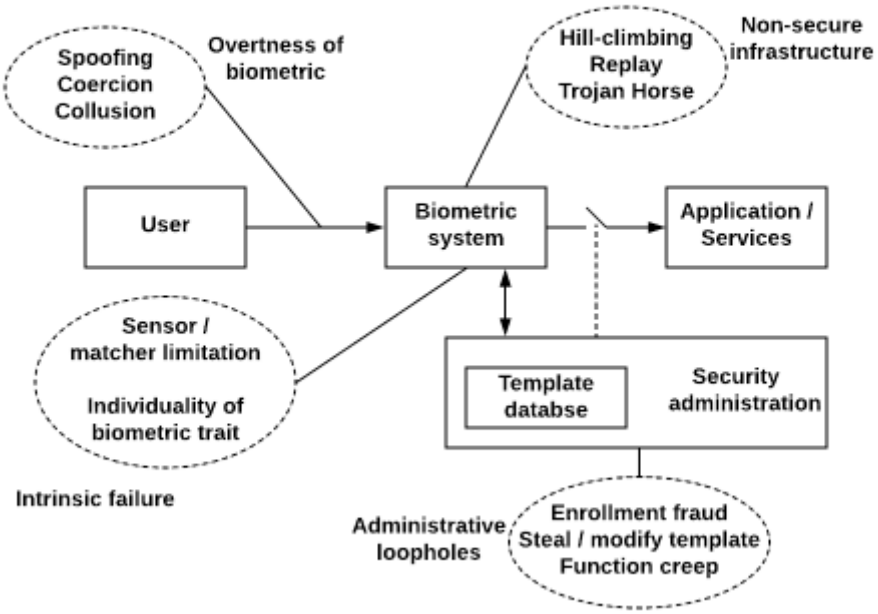
V. Η **αμέλεια** σχετίζεται με το απόρρητο των βιομετρικών προτύπων. Ο εισβολέας συλλέγει κρυφά τα βιομετρικά στοιχεία ενός γνήσιου χρήστη από τον αισθητήρα ή τους δημόσιους χώρους που επισκέπτεται ο χρήστης. Αυτά τα βιομετρικά στοιχεία μπορούν να χρησιμοποιηθούν για τη δημιουργία ψεύτικου φυσικού ή κολλώδους δακτύλου για την επίθεση μιας πλαστογραφικής επίθεσης

Αυτό το μοντέλο επισημαίνει τα γενικά σφάλματα που πρέπει να αποφεύγονται και τις τεχνικές ασφαλείας που πρέπει να εφαρμόζονται κατά το σχεδιασμό ενός βιομετρικού συστήματος. Ο πιο απλός τρόπος για τη διασφάλιση του βιομετρικού συστήματος είναι

να αποθηκεύσουμε το πρότυπο και τις μονάδες συστήματος (στοιχεία) σε έξυπνες κάρτες. Τέτοια συστήματα καλούνται ως system-on-card or match-on-card.

6.2.3 Μοντέλο Nagar et al.

Η Εικόνα *12* δείχνει το Nagar et al. μοντέλο. Αυτό το μοντέλο βασίζεται στο μοντέλο Fishbone όσον αφορά τον προσδιορισμό των αιτίων για ευπάθειες και τις επιπτώσεις τους σε ένα βιομετρικό σύστημα.



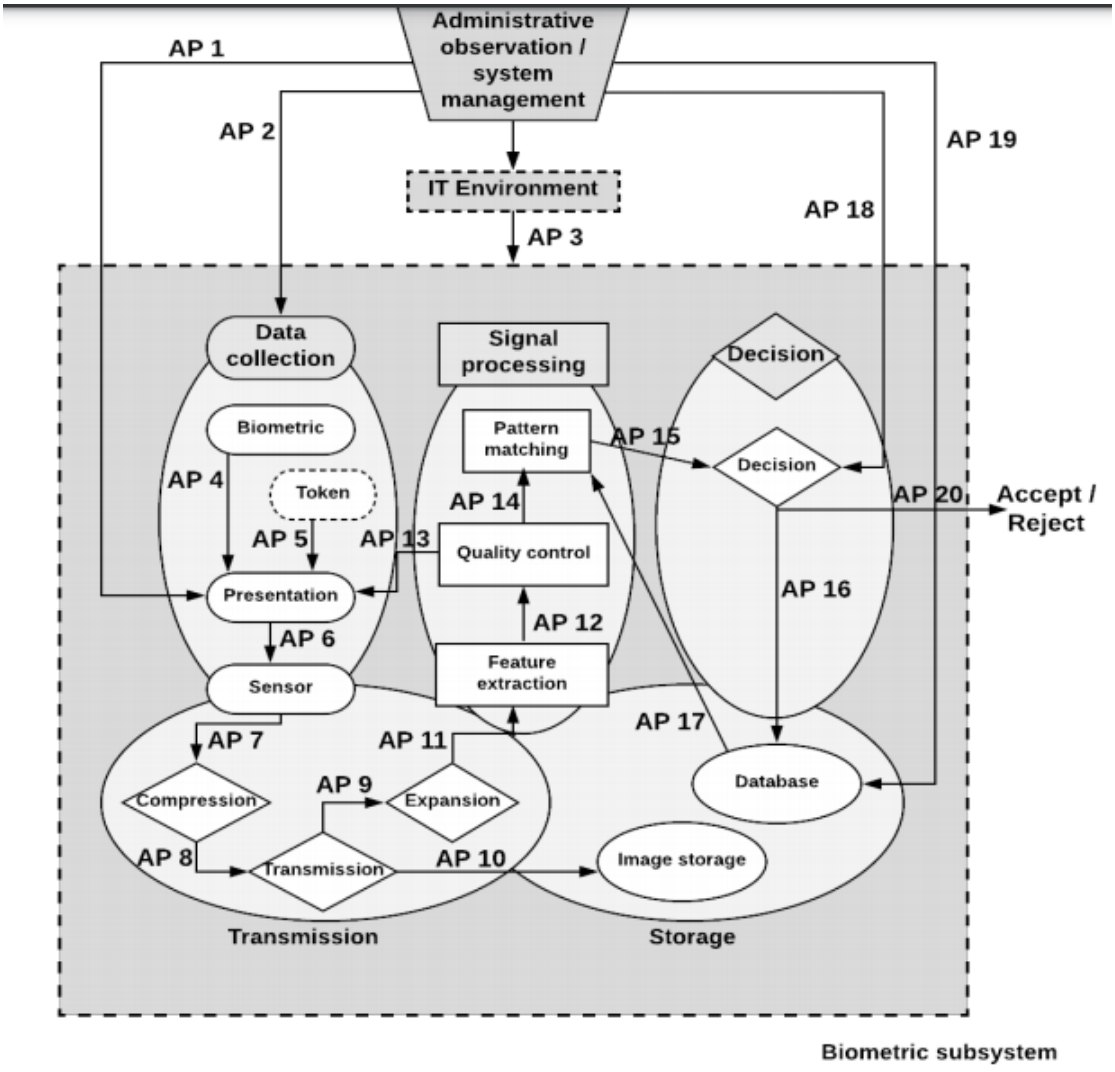
Εικόνα 12:Μοντέλο Nagar et al. *(35)*

- Η **μη ασφαλής υποδομή (non-secure infrastructure)** μπορεί να διαρρεύσει ευαίσθητες πληροφορίες στον αντίπαλο μέσω του καναλιού επικοινωνίας. Τα στοιχεία του συστήματος, όπως η μονάδα εξαγωγής χαρακτηριστικών ή η μονάδα αντιστοίχισης είναι επίσης ευάλωτα σε επιθέσεις Trojan, η οποία παρακάμπτει την πραγματική έξοδο αυτών των στοιχείων.
- Η **έκθεση των βιομετρικών χαρακτηριστικών (Overtness of biometric)** περιλαμβάνει τις επιθέσεις που χρησιμοποιούν τις εμφανείς πληροφορίες σχετικά με τα βιομετρικά στοιχεία, όπως το πρόσωπό μας, το δακτυλικό αποτύπωμα που αφήνεται σε δημόσιους χώρους, η φωνή μας για μια συνομιλία κ.λπ. επιθέσεις στοχευμένες από τον αντίπαλο σε μια βιομετρική συσκευή εισόδου.

- Η **εγγενής αποτυχία (Intrinsic failure)** περιλαμβάνει τους περιορισμούς του συστήματος που είναι υπεύθυνοι για την εσφαλμένη αποδοχή ενός μη εγγεγραμμένου χρήστη. Το προκαθορισμένο κατώφλι αποφασίζει την αυθεντικότητα ενός χρήστη που αξιώνει.

Ένας διαχειριστής συστήματος μπορεί να εκμεταλλευτεί κενά διαχείρισης για να καταχραστεί τα διοικητικά του δικαιώματα. Ο διαχειριστής μπορεί να υποστηρίξει τον αντίπαλο σε συμπαιγνία, απάτη εγγραφής ή πλαστογράφηση. Το καλύτερο αντίμετρο κατά των επιθέσεων που αφορούν εσωτερικό προσωπικό με προνόμια διαχείρισης είναι να ορίσουμε πολλούς διαχειριστές συστήματος για κάθε εργασία υπεύθυνου.

6.2.4 Bartlow and Cukic framework



Εικόνα 13: Πλαίσιο Bartlow και Cukic: Το AP αντιπροσωπεύει ένα Attack Point. Το βιομετρικό σύστημα χωρίζεται σε τρεις ενότητες, δηλαδή, ενότητα διοικητικής παρατήρησης / διαχείρισης συστήματος, ενότητα περιβάλλοντος πληροφορικής και ενότητα βιομετρικών υποσυστημάτων. Η ενότητα βιομετρικών υποσυστημάτων χωρίζεται σε πέντε υποσύστημα, δηλαδή, συλλογή δεδομένων, επεξεργασία σήματος, απόφαση, υποσύστημα μετάδοσης και αποθήκευσης. *(23)*

Ο Wayman πρότεινε να ταξινομήσει ένα βιομετρικό σύστημα ως μια σύνθεση πέντε βασικών υποσυστημάτων ανάλογα με την εφαρμογή του, δηλαδή τη συλλογή δεδομένων, τη μετάδοση, την επεξεργασία σήματος (που περιλαμβάνει εξαγωγή χαρακτηριστικών, ποιοτικό έλεγχο, αντιστοίχιση προτύπων), αποθήκευση και απόφαση (36). Η *Εικόνα 13* δείχνει το πλαίσιο Bartlow και Cukic (24), (37)**,** ως επέκταση του μοντέλου Ratha et al. και την αρχιτεκτονική υποσυστήματος του Wayman, τα οποία επικεντρώνονται κυρίως στην τεχνική δοκιμή βιομετρικών συσκευών.

Μελετούμε το μοντέλο χωρίζοντάς το σε 3 επίπεδα και βρίσκουμε περισσότερα από είκοσι ευάλωτα σημεία επίθεσης. Τα 3 επίπεδα (που φαίνονται σε σκούρο γκρι χρώμα στην *Εικόνα 13*) είναι συγκεκριμένα η ενότητα διοικητικής παρατήρησης / διαχείρισης συστήματος, η μονάδα περιβάλλοντος IT και η μονάδα βιομετρικού υποσυστήματος. Το βιομετρικό υποσύστημα κατηγοριοποιείται περαιτέρω σε πέντε υποσυστήματα (τα οβάλ σχήματα στην *Εικόνα 13*) σύμφωνα με την πρόταση του Wayman. Τα βέλη αντιπροσωπεύουν το σημείο των επιθέσεων και των τρωτών σημείων στα υποσυστήματα και τις διάφορες ενότητες του συστήματος.

Στην *Εικόνα 13,* η λειτουργική μονάδα διαχείρισης συστήματος αντιπροσωπεύει τους ‘’άπιστους΄΄ διαχειριστές συστήματος και το βέλος που προέρχεται από αυτό δείχνει τα πιθανά σημεία επίθεσης από τέτοιο προσωπικό που στοχεύει διαφορετικά στοιχεία. Τα σημεία επίθεσης AP 1 και AP 2 στοχεύουν τη μονάδα συλλογής δεδομένων του βιομετρικού υποσυστήματος όπου ο αντίπαλος ζητά βοήθεια από τον διαχειριστή. Τα σημεία επίθεσης AP 18 και AP 20 καθορίζουν τον χειρισμό της τελικής απόφασης από τον διαχειριστή υπέρ του αντιπάλου. Ο ‘’άπιστος΄΄ διαχειριστής μπορεί να πραγματοποιήσει εσφαλμένη εγγραφή μέσω του AP 19.

Το υποσύστημα περιβάλλοντος IT περιλαμβάνει εφαρμογές, όπως λειτουργικό σύστημα και σύστημα διαχείρισης βάσεων δεδομένων που αλληλεπιδρούν άμεσα ή έμμεσα με το βιομετρικό σύστημα. Το σημείο επίθεσης AP 3 δείχνει την πιθανότητα επίθεσης μέσω αυτών των εφαρμογών.

Το βιομετρικό υποσύστημα καθορίζει τα εσωτερικά στοιχεία του βιομετρικού συστήματος, τη μετάδοση δεδομένων μεταξύ τους και τα στοχευόμενα ευάλωτα σημεία. Στην ενότητα συλλογής δεδομένων τα σημεία επίθεσης, AP 4, AP 5 και AP 6 είναι ευάλωτα σε επιθέσεις που πραγματοποιούνται μέσω των συσκευών εισόδου. Επιθέσεις όπως spoofing, replay και masquerade μπορούν να τοποθετηθούν σε αυτό το

επίπεδο. Η συμπίεση και μετάδοση βιομετρικών δεδομένων αντιπροσωπεύεται με μια μονάδα μετάδοσης που είναι ευαίσθητη σε επιθέσεις, όπως replay, και masquerade που φαίνονται από τα σημεία επίθεσης, AP 7, AP 8, AP 9, AP 10 και AP 11 στην *Εικόνα 13*. Σε αυτόν τον τρόπο επίθεσης, ο αντίπαλος που παρακολουθεί το κανάλι επικοινωνίας συλλέγει τις πληροφορίες που απαιτούνται για την εκτελέσει επιθέσεις replay, hill climbing ή brute force.

Η μονάδα επεξεργασίας σήματος περιλαμβάνει την εξαγωγή χαρακτηριστικών, την αντιστοίχιση προτύπων και τα στοιχεία ελέγχου ποιότητας εικόνας. Ο αντίπαλος χρησιμοποιεί ένα Trojan στα AP 12 και AP 14 για να στοχεύσει τον εξαγωγέα χαρακτηριστικών και τη μονάδα ελέγχου ποιότητας, αντίστοιχα. Ο εισβολέας μπορεί ακόμη και να χρησιμοποιήσει μια εικόνα κακής ποιότητας στο AP 13 για να επιτεθεί με hill climbing ή brute force επίθεση. Χρησιμοποιώντας την επίθεση αναρρίχησης (hill climbing), ο εισβολέας μπορεί να κατασκευάσει μια εικόνα δακτυλικών αποτυπωμάτων μέχρι να επιτευχθεί η πρόσβαση στο σύστημα. Ακόμα, ο αντίπαλος μπορεί να εφαρμόσει τεχνικές επεξεργασίας εικόνων για να δημιουργήσει πολλαπλά αντίγραφα μιας εικόνας κακής ποιότητας, βελτιώνοντάς τη και χρησιμοποιώντας όλες αυτές τις εικόνες για να εκτελέσει μια επίθεση ωμής βίας (brute force).

Η παρακολούθηση των πληροφοριών μεταξύ της μονάδας αντιστοίχισης προτύπων και της μονάδας αποφάσεων παρουσιάζεται στο AP 15. Η διαδικασία λήψης δεδομένων μέσω διαρροής της βάσης δεδομένων και εκ νέου μετάδοσής τους στη μονάδα αντιστοίχισης γίνεται σε σημεία επίθεσης, AP 16 και AP 17, αντίστοιχα. Η προσπάθεια παράκαμψης του τελικού συμπεράσματος της ενότητας αποφάσεων σε συνεργασία με έναν κακόβουλο διαχειριστή αντιπροσωπεύεται με το AP 20.

AP	Στοχευμένο σημείο επίθεσης	Πιθανή επίθεση	Τρόποι αποφυγής επίθεσης	Αναφορές
1	Βιομετρική συσκευή εισόδου	Κακόβουλες επιθέσεις και διεφθαρμένοι χρήστες	Φυσική ανίχνευση, Πρωτόκολλο πρότυπης απάντησης	(38), (39), (40), (23), (41)

2	Βιομετρική συσκευή εισόδου	Άρνηση συστήματος (DoS)	Ανθεκτικές συσκευές	(35), (24)
3	Κανάλι επικοινωνίας μεταξύ αισθητήρα και μονάδας εξαγωγής χαρακτηριστικών	Υποκλοπή εικόνας δακτυλικών αποτυπωμάτων	Διαβίβαση δεδομένων μέσω κρυπτογραφημένης διαδρομής / ασφαλούς καναλιού	(35)
4	Μονάδα εξαγωγής χαρακτηριστικών	Επίθεση Trojan Horse, παράκαμψη εξαγωγής χαρακτηριστικών	Υπογραφή κώδικα (Code signing)	(35)
5	Κανάλι επικοινωνίας μεταξύ της μονάδας εξαγωγής χαρακτηριστικών και της μονάδας τεχνικών προστασίας προτύπων	Επίθεση Επανάληψης (Replay attack)	Σύστημα με βάση την απόκριση, εξαγωγείς χαρακτηριστικών μίας χρήσης	(24), (42)
6	Μονάδα τεχνικής προστασίας προτύπων	Επιθέσεις παρακολούθησης καναλιού (Side channel attacks)	Κάλυψη καναλιού (masking), και προσθήκη προστατευτικού τοίχους στο κανάλι	(30), (43)
7	Κανάλι επικοινωνίας μεταξύ της μονάδας τεχνικών προστασίας προτύπων και της βάσης δεδομένων	Υποκλοπή προτύπου, εισαγωγή δεδομένων	Χρήση ισχυρών και δοκιμασμένων βιομετρικών αλγόριθμων	(44)
8	Βάση δεδομένων	Κλοπή, διαγραφή , τροποποίηση προτύπου	Ισχυρός server, έλεγχοι πρόσβασης DB, υπογραφή προτύπων, αποθήκευση κρυπτογραφημένων προτύπων, αποθήκευση	(35), (45), (46)

			προτύπων σε έξυπνη κάρτα	
9	Κανάλι επικοινωνίας μεταξύ της μονάδας τεχνικών προστασίας προτύπων και της μονάδας αντιστοίχισης	Επίθεση αναρρίχησης (Hill-climbing attack), επίθεση ωμής βίας (Brute force attack)	Πολιτικές χρονικού ορίου / κλειδώματος	(47), (48)
10	Κανάλι επικοινωνίας μεταξύ της βάσης δεδομένων και της μονάδας αντιστοίχισης	Επίθεση Επανάληψης (Replay attack)	Χρονική σφράγιση (Timestamps or Time to Live TTL)πρωτόκολλο)	(24)
11	Μονάδα αντιστοίχισης	Επίθεση Trojan horse, επιθέσεις παρακολούθησης καναλιού (Side channel attacks)	Κάλυψη (Masking), designing ICs with active shield, Code signing	(30), (32)
12	Κανάλι επικοινωνίας μεταξύ της μονάδας αντιστοίχισης και της μονάδας αποφάσεων	Τροποποίηση δείκτη ομοιότητας	Αμοιβαίος έλεγχος ταυτότητας μεταξύ της μονάδας αντιστοίχισης και απόφασης	
13	Μονάδα αποφάσεων	Παράκαμψη απόφασης	Code signing	(24)
14	Κανάλι επικοινωνίας μεταξύ της μονάδας αποφάσεων και της βιομετρικής εφαρμογής	Επίθεση μηδενικής προσπάθειας [Zero-effort attack (FMR)]	Σχεδιασμός ισχυρής αντιστοίχισης	(49), (48)
15	Κανάλι επικοινωνίας μεταξύ της μονάδας αποφάσεων και της βιομετρικής εφαρμογής	Επίθεση μηδενικής προσπάθειας [Zero-effort attack (FNMR)]	Σχεδιασμός ισχυρής αντιστοίχισης	(49)

16	Βιομετρική εφαρμογή	Άρνηση συστήματος (DoS)	Παρακολούθηση CCTV,ανάπτυξη ασφάλειας	(24), (35)

Πίνακας 1: Ο πίνακας αναφέρει τα ευάλωτα σημεία των βιομετρικών συστημάτων και των επιθέσεων που μπορεί να δεχθούν καθώς και τους τρόπους αποφυγής αυτών *(23)*.

Κεφάλαιο 7. Βιομετρικά Σχήματα & Κρυπτογραφία

Στο κεφάλαιο αυτό παρουσιάζονται τεχνικές που έχουν ως στόχο την κρυπτογράφηση των βιομετρικών δεδομένων. Αναφερόμαστε στα ασφαλή σκίτσα , στους ασαφείς εξαγωγείς και στον συνδυασμό των δύο αυτών τεχνικών. Επίσης αναφέρεται η έννοια της εντροπίας των δεδομένων ώστε να διασφαλιστεί η ασφάλεια του απορρήτου της πληροφορίας.

7.1 Κύριες διαδικασίες ενός βιομετρικού συστήματος

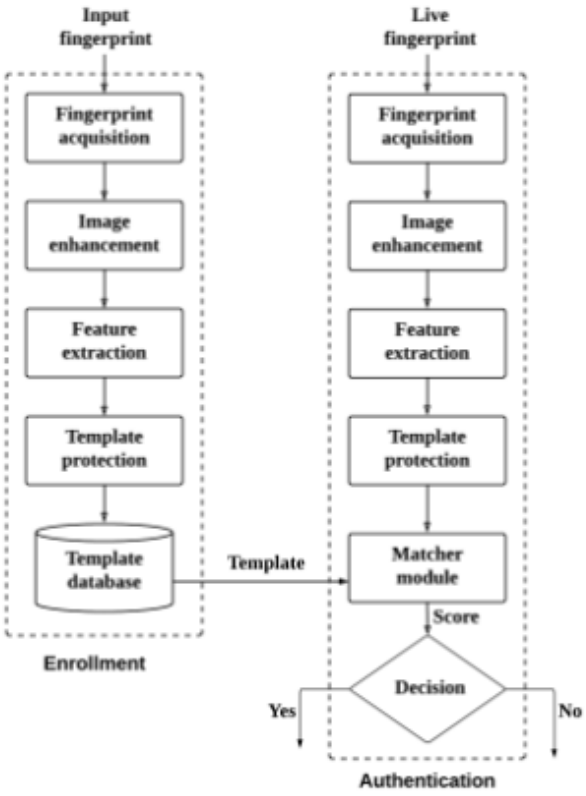
Τα βιομετρικά συστήματα μετατρέπουν τα βιομετρικά δεδομένα σε πρότυπα, τα οποία στη συνέχεια χρησιμοποιούνται για τη μετέπειτα σύγκριση. Για να επιτευχθεί αυτή η μετατροπή χρειάζεται μια διαδικασία πολλαπλών επιπέδων.

1. Αρχικά, υπάρχει η διαδικασία της εγγραφής (enrollment) κατά την οποία συλλέγονται τα βιομετρικά δεδομένα των χρηστών μέσω μιας συσκευής απόκτησης, όπως ένας αισθητήρας.
2. Στη συνέχεια, τα ανεπεξέργαστα αυτά βιομετρικά δεδομένα επεξεργάζονται για να δημιουργηθούν τα αντίστοιχα πρότυπα. Για τη δημιουργία τους χρησιμοποιείται ένας βιομετρικός αλγόριθμος ο οποίος εντοπίζει τα κύρια χαρακτηριστικά που καθιστούν το βιομετρικό δεδομένο μοναδικό. Ο αλγόριθμος που έχει παρουσιαστεί στο εδάφιο 5.1.3 είναι και ο MINDTCP ο οποίος εξάγει τις μικρολεπτομέριες (minutiae points) ενός δακτυλικού αποτυπώματος που το διαφοροποιούν από άλλα. Τα αρχικά βιομετρικά δεδομένα αποθηκεύονται τελικά ως διανύσματα μετασχηματισμένων βιομετρικών δεδομένων, και αναφέρονται ως πρότυπα.
3. Έπειτα, τα πρότυπα βιομετρικά δεδομένα χρησιμοποιούνται για τη σύγκριση με μεταγενέστερες προσπάθειες ταυτοποίησης κατά τις οποίες ο χρήστης καταχωρεί τα βιομετρικά στοιχεία του. Για τη σύγκριση χρησιμοποιείται ένας αλγόριθμος βιομετρικής αντιστοίχισης , ο οποίος υπολογίζει το βαθμό ομοιότητας μεταξύ του πρότυπου βιομετρικού και του πρότυπου σύγκρισης. Ο αλγόριθμος αυτός χειρίζεται τις πληροφορίες που περιέχονται στα βιομετρικά

πρότυπα ώστε να υπολογίσει διακυμάνσεις ή κάποιο θόρυβο για παράδειγμα με σκοπό να παρέχει έγκυρες αντιστοιχίσεις. Ένας τέτοιος αλγόριθμος είναι και ο Bozorth που παρουσιάστηκε αναλυτικά στο εδάφιο 5.1.4.

Έχοντας τον βαθμό ομοιότητας που εξάγει ο αλγόριθμος βιομετρικής αντιστοίχισης έχουμε μία εικόνα σύμφωνα με τη συσχέτιση των δύο προτύπων. Φυσικά υπάρχει ένα όριο που εδραιώνει το βαθμό ομοιότητας ώστε να κριθεί μία σύγκριση. Όταν ξεπερνά αυτό το όριο η αντιστοιχία μας είναι έγκυρη, ενώ όχι όταν συμβαίνει το αντίθετο. Ωστόσο το όριο αυτό πρέπει να επιλεγεί κατάλληλα ώστε να έχουμε υψηλό ποσοστό σωστών αντιστοιχίσεων και χαμηλό ποσοστό λάθος αντιστοιχίσεων.

Τέλος, κάθε φορά που ένας χρήστης αλληλεπιδρά με ένα βιομετρικό σύστημα για να αυθεντικοποιηθεί , δημιουργείται κάθε φορά ένα μοναδικό βιομετρικό πρότυπο. Όμως και δύο δακτυλικά αποτυπώματα του ίδιου δακτύλου μπορεί να δημιουργήσουν εντελώς διαφορετικά πρότυπα. Γι’ αυτό το λόγο, όταν επεξεργαστούν από τον αλγόριθμο βιομετρικής αντιστοίχισης θα πρέπει να αναγνωρίζεται ότι προέρχονται από τον ίδιο χρήστη.



Εικόνα 14: Βιομετρικό Σύστημα Δακτυλικών Αποτυπωμάτων (50)

7.2 Βιομετρική κρυπτογράφηση και ασφάλεια

Επικεντρωνόμαστε κυρίως στο να βεβαιωθούμε ότι τα βιομετρικά δεδομένα που είναι αποθηκευμένα ως πρότυπα είναι κρυπτογραφημένα (χρησιμοποιώντας κλειδί) και είναι πρακτικά ανέφικτο να αποκαλύψουμε το μυστικό κλειδί κρυπτογράφησης ή να αναδημιουργήσουμε τα αρχικά δακτυλικά αποτυπώματα ενός χρήστη. Αυτό επιτυγχάνεται με τη χρήση βιομετρικών κρυπτοσυστημάτων τα οποία παρέχουν τα οφέλη της κρυπτογραφίας και της χρήσης των βιομετρικών δεδομένων.

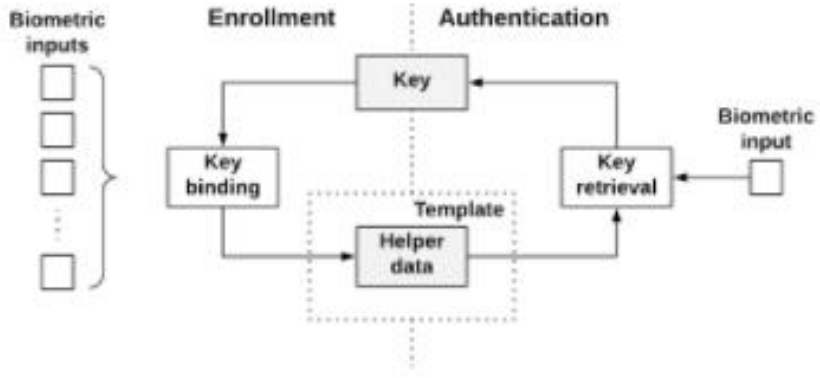
Τα βιομετρικά κρυπτοσυστήματα μπορούν να σχεδιαστούν με δύο τρόπους. Είτε να χρησιμοποιήσουν τα βιομετρικά στοιχεία ενός ατόμου για να δημιουργήσουν ένα ψηφιακό κλειδί, είτε να συνδέσουν με ασφάλεια ένα μυστικό κλειδί με τα βιομετρικά στοιχεία του χρήστη. Η "απελευθέρωση κλειδιού" αναφέρεται στη χρήση βιομετρικού ελέγχου ταυτότητας για την απελευθέρωση ενός κρυπτογραφικού κλειδιού που είχε

αποθηκευτεί προηγουμένως, ενώ η "δημιουργία κλειδιών" αναφέρεται στην εξαγωγή / δημιουργία ενός κρυπτογραφικού κλειδιού από ένα βιομετρικό πρότυπο.

Η πλειοψηφία των κρυπτοσυστημάτων απαιτεί την αποθήκευση βιομετρικών δημόσιων πληροφοριών, οι οποίες εφαρμόζονται για την ανάκτηση ή τη δημιουργία κλειδιών. Τέτοιες βιομετρικές εξαρτώμενες πληροφορίες αναφέρονται ως βοηθητικά δεδομένα (helper data) από τις οποίες προκύπτουν δύο αντιφατικές απαιτήσεις:

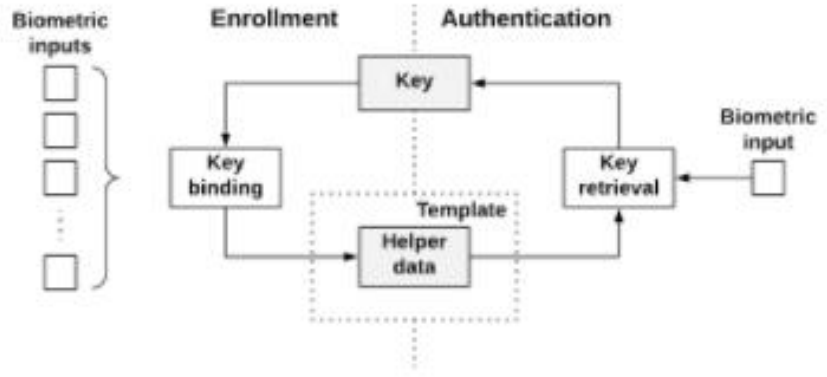
- θα πρέπει να περιέχουν επαρκείς πληροφορίες που να επιτρέπουν την αντιστοιχία μεταξύ ενός πρότυπου βιομετρικού στοιχείου που είναι ήδη αποθηκευμένο στο σύστημα με το αντίστοιχο στοιχείο που θα καταχωρήσει ο χρήστης την επόμενη φορά που θα το σκανάρει ώστε να αποκτήσει πρόσβαση στο σύστημα.
- δεν πρέπει να διαρρεύσουν κρίσιμες πληροφορίες σχετικά με το πρότυπο.

Το κρυπτογραφικό κλειδί είναι στενά συνδεδεμένο με το βιομετρικό πρότυπο έτσι ώστε να μην μπορεί να απελευθερωθεί χωρίς επιτυχημένο βιομετρικό έλεγχο ταυτότητας. Επομένως, είναι και συνδεδεμένο με το σύνολο των χαρακτηριστικών, ενώ το χαρακτηριστικό μιας ψεύτικης ταυτότητας είναι είτε διασκορπισμένο είτε πολύ μακριά από τα χαρακτηριστικά του νόμιμου χρήστη. Αυτή η παραλλαγή διακρίνει το μετασχηματισμένο χαρακτηριστικό του εγγεγραμμένου χρήστη από το χαρακτηριστικό της ψευδούς ταυτότητας.



Εικόνα 15: Δέσμευση κλειδιού από το βιομετρικό δείγμα (50)

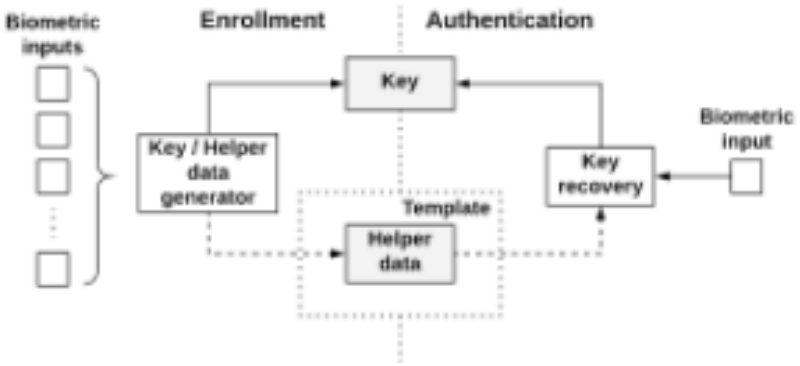
Στην



Εικόνα 15 παρουσιάζεται η βασική ιδέα για τη χρήση των βοηθητικών δεδομένων. Το κλειδί συνδυάζεται με ένα βιομετρικό δείγμα για τη δημιουργία βοηθητικών δεδομένων κατά την εγγραφή (enrollment). Ένα νέο βιομετρικό δείγμα, δηλαδή μία νέα σάρωση του ίδιου βιομετρικού δεδομένου, μαζί με τα αποθηκευμένα βοηθητικά δεδομένα χρησιμοποιούνται για την απελευθέρωση του ίδιου κλειδιού κατά τον έλεγχο ταυτότητας. Σε αυτό το σχήμα, είναι υπολογιστικά ανέφικτο να ανακτήσουμε το αρχικό βιομετρικό πρότυπο ή το μυστικό κλειδί, δεδομένου μόνο των βοηθητικών δεδομένων. Αυτό σημαίνει ότι η εντροπία τους διατηρείται υψηλή.

Η βιομετρική κρυπτογράφηση, λοιπόν, συνδέει με ασφάλεια ένα ψηφιακό κλειδί με ένα βιομετρικό δεδομένο ή δημιουργεί ένα ψηφιακό κλειδί από το βιομετρικό, ώστε να μην χρειάζεται να αποθηκευτεί βιομετρική εικόνα ή πρότυπο. Θα παρουσιάσουμε δύο από τις βασικές τεχνολογίες βιομετρικής κρυπτογράφησης, το ασφαλές σκίτσο (secure sketch) και τον ασαφή εξαγωγέα (fuzzy extractor).

Στο παρακάτω σχήμα παρουσιάζεται η βασική ιδέα πίσω από το σχήμα δημιουργίας κλειδιών. Οι τεχνικές δημιουργίας κλειδιών εξάγουν ένα κρυπτογραφικό κλειδί από ένα βιομετρικό δείγμα κατά τη διάρκεια της εγγραφής μαζί με τα βοηθητικά δεδομένα, εάν είναι απαραίτητο, και το ίδιο κλειδί πρέπει να εξαχθεί χρησιμοποιώντας ένα νέο βιομετρικό δείγμα (και τα βοηθητικά δεδομένα όταν είναι διαθέσιμα) κατά τον έλεγχο ταυτότητας.



Εικόνα 16: Δημιουργία κλειδιών *(50)*

7.3 Βιομετρικά κρυπτοσυστήματα για την προστασία προτύπων

Τα βιομετρικά κρυπτοσυστήματα είναι σχεδιασμένα για να ενσωματώνουν με ασφάλεια ένα ψηφιακό κλειδί μαζί με βιομετρικά δεδομένα ή να παράγουν ένα ψηφιακό κλειδί από βιομετρικά δεδομένα, προσφέροντας έτσι λύσεις για την απελευθέρωση κλειδιού έπειτα από βιομετρική ταύτιση και για την προστασία των βιομετρικών προτύπων. Τα κλειδιά μπορεί ακόμη να είναι κλειδιά κλασικής συμμετρικής κρυπτογραφίας, όπου η φύλαξη τους είναι προβληματική. Αντικαθιστώντας με αυτόν τον τρόπο τις λύσεις απελευθέρωσης κλειδιού βάσει κάποιου κωδικού, έχουμε σημαντικά οφέλη ως προς την ασφάλεια.

Τα συστήματα αυτά παρέχουν, επίσης, τα μέσα για να υιοθετηθούν κρυπτογραφικά πρωτόκολλα με βιομετρικά δεδομένα, τα οποία είναι από την φύση τους δεδομένα με θόρυβο (noisy data). Υπάρχουν δύο κατηγορίες: 1) παραγωγής κλειδιού (key-generating) όπου δυαδικά κλειδιά δημιουργούνται από τα βιομετρικά χαρακτηριστικά και 2) ενσωμάτωσης κλειδιού (key-binding), όπου ένα τυχαίο κλειδί ενσωματώνεται με ασφάλεια στα βιομετρικά δεδομένα. Η πλειοψηφία των βιομετρικών κρυπτοσυστημάτων απαιτεί την ύπαρξη κάποιων δημόσιων πληροφοριών ή αλλιώς βοηθητικών δεδομένων (helper data) τα οποία χρησιμοποιούνται για την απόκτηση ή την παραγωγή κλειδιών.

Εξαιτίας της μεταβλητότητας που παρουσιάζουν τα περισσότερα βιομετρικά χαρακτηριστικά, δεν είναι δυνατή η απευθείας εξαγωγή κλειδιών. Τα βοηθητικά δεδομένα, βοηθούν στην ανακατασκευή των κλειδιών. Από αυτά τα δεδομένα θα πρέπει να είναι αδύνατον ή υπολογιστικά πάρα πολύ δύσκολο να εξαχθούν πληροφορίες σχετικές με τα αρχικά βιομετρικά χαρακτηριστικά ή το κλειδί. Η βιομετρική σύγκριση γίνεται έμμεσα, με το να επαληθεύεται η εγκυρότητα των κλειδιών, οπότε το αποτέλεσμα της διαδικασίας αυθεντικοποίησης είναι είτε ένα κλειδί, είτε ένα μήνυμα λάθους. Καθώς η επαλήθευση των κλειδιών, γίνεται με βιομετρική σύγκριση στον κρυπτογραφημένο χώρο, τα βιομετρικά κρυπτοσυστήματα χρησιμοποιούνται σαν μέσο προστασίας βιομετρικών προτύπων και παράλληλα παρέχουν την δυνατότητα απελευθέρωσης κλειδιού.

Ένα σύστημα ενσωμάτωσης κλειδιού (key binding system) μπορεί να χρησιμοποιηθεί για να προστατεύσει ένα βιομετρικό πρότυπο με την βοήθεια ενός δυαδικού κλειδιού, ασφαλίζοντας έτσι ένα σύστημα βιομετρικής αναγνώρισης, ή για να απελευθερώσει ένα κρυπτογραφικό κλειδί μόνο όταν ο κάτοχος του κλειδιού παρουσιάσει ένα συγκεκριμένο βιομετρικό χαρακτηριστικό. Και στις δύο αυτές περιπτώσεις ένα μυστικό κλειδί, ανεξάρτητα από το ποια βιομετρία θα χρησιμοποιηθεί, ενσωματώνεται κατά την διάρκεια της εγγραφής με ένα πρότυπο αναφοράς για να παραχθούν τα βοηθητικά δεδομένα. Τα βοηθητικά δεδομένα στην συνέχεια χρησιμοποιούνται μαζί με τα βιομετρικά χαρακτηριστικά του δείγματος κατά την φάση της αναγνώρισης για να αποκτηθεί το μυστικό. Συνήθως, υπάρχει και η ικανότητα χειρισμού των ενδοατομικών διαφορών, χρησιμοποιώντας κώδικες διόρθωσης λαθών. Όμως, σε γενικές γραμμές δεν είναι εφικτό να χρησιμοποιηθούν εξελιγμένοι και αποκλειστικοί συγκριτές, με αποτέλεσμα να μειώνεται η ακρίβεια ταύτισης.

Σε ένα σύστημα παραγωγής κλειδιού, τα βοηθητικά δεδομένα προέρχονται μόνο από το βιομετρικό πρότυπο. Τα κλειδιά παράγονται απευθείας από τα βοηθητικά δεδομένα και ένα βιομετρικό δείγμα. Ενώ η αποθήκευση των βοηθητικών δεδομένων δεν είναι υποχρεωτική, η πλειοψηφία των προτεινόμενων σεναρίων παραγωγής κλειδιού τα αποθηκεύει. Αν τα σενάρια παραγωγής κλειδιού εξάγουν κλειδιά χωρίς την χρήση βοηθητικών δεδομένων, αυτά δεν μπορούν να ανανεωθούν στην περίπτωση παραβίασης.

Τα βοηθητικά δεδομένα που προέρχονται από κάποιο σενάριο παραγωγής κλειδιού, αποκαλούνται επίσης “fuzzy extractors” ή “secure sketches”. Ένας fuzzy extractor εξάγει με αξιοπιστία ένα τυχαίο αλφαριθμητικό (string) από ένα βιομετρικό δείγμα που

παίρνει σαν είσοδο, ενώ τα αποθηκευμένα βοηθητικά δεδομένα βοηθούν στην ανακατασκευή. Ενώ αντίθετα, σε ένα secure sketch, τα βοηθητικά δεδομένα εφαρμόζονται για να ανακτηθεί το αρχικό βιομετρικό πρότυπο (51), (52).

7.4 Η έννοια της εντροπίας

Παρόλο που άλλοι παράγοντες, όπως η κρυπτογράφηση του αλγορίθμου και η ασφαλής εφαρμογή, παίζουν μεγάλο ρόλο στην ασφάλεια της κρυπτογραφίας, εστιάζουμε την προσοχή μας στην τυχαιότητα των κλειδιών, ένα ζήτημα που συχνά παρεξηγείται ή παραμελείται. Ακόμη και οι καλύτεροι αλγόριθμοι δεν μπορούν να αντισταθμίσουν τα αδύναμα κλειδιά που δημιουργήθηκαν με ανεπαρκή εντροπία.

Η εντροπία είναι ένα μέτρο τυχαιότητας ή αβεβαιότητας. Η τυπική μονάδα μέτρησης είναι bit. Είναι δύσκολο να αποκτήσουμε καλή εντροπία από πραγματικά συστήματα υπολογιστών, επειδή οι πηγές απρόβλεπτης συμπεριφοράς ελαχιστοποιούνται από το σχεδιασμό. Επομένως, για να αποκτήσουμε καλή εντροπία πρέπει να βρούμε πηγές αληθινής τυχαιότητας, εκείνες που έρχονται σε αντίθεση με τη φύση του τυπικού συστήματος υπολογιστών και επομένως μπορεί να είναι δύσκολο να χρησιμοποιηθούν.

Στις περισσότερες περιπτώσεις, η έξοδος από μια συγκεκριμένη πηγή περιέχει προκατάληψη και συσχετισμούς - συμπτώματα μη τυχαιότητας - λόγω ατελειών στη μέτρηση ή στο σχεδιασμό. Ενώ η εξάλειψη του συσχετισμού είναι πολύ δύσκολη στην πράξη, η μεροληψία μπορεί να μετριαστεί. Συχνά, η έξοδος της πηγής εντροπίας περνά έπειτα μέσω ψευδοτυχαίας συνάρτησης για να κατανείμει ομοιόμορφα την εντροπία στα bit των δειγμάτων εξόδου. Μία τέτοια συνάρτηση είναι η hash.

Αν και είναι εύκολο να κατανοηθεί διαισθητικά, η έννοια της πραγματικής τυχαιότητας είναι δύσκολο να οριστεί και να ποσοτικοποιηθεί. Κάποιος μπορεί να το προσεγγίσει μελετώντας άπειρες ακολουθίες δυαδικών ψηφίων ή δειγμάτων και να μετρήσει τις ιδιότητές τους, ορισμένα στατιστικά στοιχεία όπως μεροληψία, άλλα μη στατιστικά όπως έλλειψη υπολογιστικών συσχετίσεων. Τρία από τα πιο συχνά χρησιμοποιούμενα χαρακτηριστικά της αληθινής τυχαιότητας είναι: (i) το απρόβλεπτο, το οποίο είναι ένα μέτρο της ισχυρής μη υπολογιστικότητας των bits στην ακολουθία, (ii) ομοιόμορφη κατανομή των δυαδικών ψηφίων, (iii) έλλειψη προτύπων. Αξίζει να σημειωθεί ότι το (iii) συνεπάγεται τα (i) και (ii), ωστόσο, το αντίστροφο δεν ισχύει.

Θα χρειαστούμε τους παρακάτω ορισμούς:

- Μέση ελάχιστη εντροπία (Average min-entropy): Όπως αναφέραμε και παραπάνω για την πρόβλεψη μιας τυχαίας μεταβλητής Α έχουμε $maxaPr\,[A = a]$, και min-entropy $H\infty(A) = -log\,(maxaPr\,[A = a])$. Ας θεωρήσουμε τώρα ένα ζευγάρι (πιθανών συσχετισμένων) μεταβλητών A, B. Αν ένας κακόβουλος χρήστης γνωρίζει την τιμή του B, έστω b, τότε για την πρόβλεψη του Α θα έχουμε $maxaPr[A = a|B = b]$. Οπότε, η επιτυχία ενός εισβολέα να μαντέψει την τιμή του A δεδομένου του B είναι κατά μέσο όρο $Eb{\leftarrow}B\,[maxaPr[A = a \mid B = b]]$. Ορίζουμε τη μέση ελάχιστη εντροπία ως:

$$\mathrm{H}\infty(A \mid B) = -\log(E_{b\leftarrow B}[\max_a \Pr[A = a \mid B = b]] = -\log(E_{b\leftarrow B}[2^{-\mathrm{H}\infty(A|B=b)}].$$

H conditional ελάχιστη εντροπία ποσοτικοποιεί την ποσότητα των πληροφοριών που απαιτούνται για να περιγράψει το αποτέλεσμα μιας τυχαίας μεταβλητής A, δεδομένου ότι η τιμή μιας άλλης τυχαίας μεταβλητής B είναι γνωστή.

- (Εντροπία/Entropy).Η εντροπία μιας τυχαίας μεταβλητής W με συνάρτηση πυκνότητας πιθανότητας p, ορίζεται ως:

$$\mathrm{H}(W) = -\sum_{i=1}^{n} p(x_i)\log_2\, p(x_i)$$

- Ελάχιστη εντροπία/Min-entropy). Η ελάχιστη εντροπία μιας τυχαίας μεταβλητής W ορίζεται ως:

$$\mathrm{H}\infty(W) = -\log_2(\max_a \Pr[W = a]).$$

- (Μέση εξαρτημένη ελάχιστη εντροπία/Average Conditional Min-entropy). Η μέση εξαρτημένη ελάχιστη εντροπία του W δεδομένου του W′, ορίζεται ως

$$\mathrm{H}\infty(W \mid W') = -\log\,(\mathrm{E}_{b\leftarrow W'}[2^{-H\infty(W|W'=b)}]),$$

όπου Ε υποδηλώνει προσδοκία (53). (54)

7.5 Εισαγωγή στους εξαγωγείς (Extractors)

Η πρακτική χρήση κρυπτογραφικών πρωτοκόλλων απαιτεί συχνά τη διανομή και αποθήκευση μυστικών κλειδιών. Τα κλειδιά πρέπει να περιέχουν υψηλό επίπεδο εντροπίας, αλλά πρέπει εύκολα και με ακρίβεια να μπορούν να αναπαραχθούν. Ωστόσο, η δημιουργία τυχαιότητας είναι δαπανηρή και η αποθήκευση ή αναπαραγωγή της εν λόγω τυχαιότητας μπορεί να είναι εξαιρετικά δύσκολη.

Τα κλειδιά υψηλής εντροπίας είναι δύσκολο να απομνημονευτούν, ενώ τα κλειδιά χαμηλής εντροπίας ενδέχεται να καταστήσουν ένα πρωτόκολλο ανασφαλές, ανεξάρτητα από το πόσο ασφαλές είναι το ίδιο το πρωτόκολλο. Ενώ η ικανότητα των ανθρώπων να παράγουν και να θυμούνται κωδικούς υψηλής εντροπίας μπορεί να είναι μικρή, υπάρχει μια πληθώρα από εύκολα προσβάσιμες πληροφορίες που ενώ περιέχουν κάποια εντροπία δεν είναι ομοιόμορφα τυχαίες, όπως είναι και η βιομετρική πληροφορία. Εξαιτίας αυτού, θα πρέπει να δημιουργηθούν εργαλεία για να δημιουργούν και να αποθηκεύουν κλειδιά. Ένα ασφαλές σκίτσο (secure sketch) παράγει ένα σκίτσο της μυστικής πληροφορίας το οποίο αποκαλύπτει ελάχιστες πληροφορίες σχετικά με το αρχική πληροφορία, αλλά επιτρέπει την ανάκτησή της από οποιαδήποτε άλλη πληροφορία που είναι κοντά στην αρχική. Ένας ασαφής εξαγωγέας επιτρέπει σε δύο ‘’ομάδες’’ με θορυβώδη μυστικά να συμφωνήσουν σε μια τυχαία τιμή. Ένα σκίτσο είναι επαναχρησιμοποιήσιμο εάν πολλά σκίτσα του ίδιου μυστικού δεν αποκαλύπτουν πρόσθετες πληροφορίες σχετικά με αυτό το μυστικό και ένα σκίτσο είναι ανθεκτικό εάν ένας αντίπαλος δεν μπορεί να δημιουργήσει ένα νέο δεδομένο έγκυρο σκίτσο ενός μυστικού γνωρίζοντας ένα μόνο παράδειγμα.

7.6 Ασαφής εξαγωγέας (Fuzzy extractor)

Ένα σημαντικό γενικό πρόβλημα είναι η μετατροπή θορυβωδών μη ομοιόμορφων εισόδων σε αξιόπιστα αναπαραγωγίσιμες, ομοιόμορφα τυχαίες συμβολοσειρές. Για το σκοπό αυτό, προτείνουμε έναν ασαφή εξαγωγέα (fuzzy extractor). Ένας ασαφής εξαγωγέας έχει τη δυνατότητα να παράγει μία ομοιόμορφα τυχαία συμβολοσειρά από μία θορυβώδη είσοδο, όπως θα μπορούσαν να είναι τα βιομετρικά δεδομένα. Αυτό γίνεται με τρόπο ανθεκτικό στο θόρυβο. Δηλαδή, αν η είσοδος αλλάξει αλλά είναι πολύ κοντινή της αρχικής, ο εξαγωγέας αναπαράγει ακριβώς την ίδια συμβολοσειρά που είχε δημιουργήσει για την αρχική είσοδο. Για να μπορεί, λοιπόν, να αναπαράγει ακριβώς

την ίδια αυτή συμβολοσειρά για εισόδους που είναι πολύ κοντινές μεταξύ τους, κατά την πρώτη είσοδο παράγει επίσης και μία δεύτερη βοηθητική συμβολοσειρά, η οποία μάλιστα μπορεί να είναι και δημόσια χωρίς αυτό να σημαίνει ότι μειώνεται η ασφάλεια που οφείλει να παρέχει η πρώτη συμβολοσειρά.

Επομένως, ένας ασαφής εξαγωγέας θα μπορούσε να χρησιμοποιηθεί για την κρυπτογράφηση ή για την αυθεντικοποίηση της καταχώρισης ενός χρήστη, χρησιμοποιώντας ως κλειδί τα βιομετρικά χαρακτηριστικά του. Δηλαδή, η ομοιόμορφα τυχαία συμβολοσειρά θα μπορούσε στην ουσία να χρησιμοποιηθεί ως το κλειδί για την κρυπτογράφηση ή την αυθεντικοποίηση, ενώ η βοηθητική συμβολοσειρά να παραμείνει αποθηκευμένη για αναπαραχθεί πάλι από το βιομετρικό χαρακτηριστικό την επόμενη φορά που ο χρήστης χρειάζεται να αυθεντικοποιηθεί.

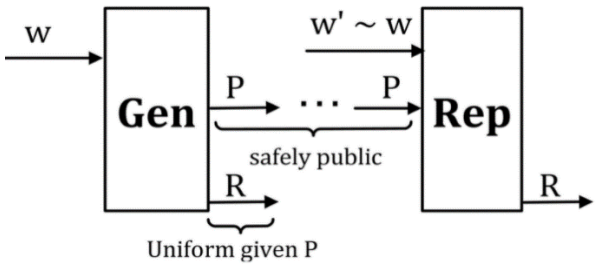
Παρατηρούμε ότι πέρα από τη βοηθητική συμβολοσειρά, δε χρειάζεται να αποθηκευτεί και η ομοιόμορφα τυχαία, πράγμα που κάνει το βιομετρικό χαρακτηριστικό να λειτουργεί ως κλειδί. Αυτό που είναι εξαιρετικά σημαντικό όμως είναι ότι με αυτή την τεχνική, ο καταχωρημένος χρήστης μπορεί να αποθηκευτεί κρυπτογραφημένος μεν αλλά σε μία μη κρυφή βάση δεδομένων δε, παίρνοντας όμως σαν δεδομένο ότι μόνο όταν παρουσιαστεί το σωστό και μόνο βιομετρικό χαρακτηριστικό θα μπορέσει να προχωρήσει η αποκρυπτογράφησή του.

Ανακεφαλαιώνοντας, λοιπόν, επιτρέπει σε κάποιον να εξαγάγει ένα τυχαίο κλειδί R από ένα βιομετρικό w και στη συνέχεια να αναπαραγάγει επιτυχώς το R από οποιοδήποτε βιομετρικό ŵ που είναι κοντά στο w. Αποτελείται από ένα ζεύγος αλγορίθμων ‘’γέννεσης΄΄, που δημιουργεί τις δύο συμβολοσειρές και ‘’αναπαραγωγής’’, για να αναπαραχθεί η συμβολοσειρά R. Ο αλγόριθμος αναπαραγωγής θα χρησιμοποιήσει τη βοηθητική συμβολοσειρά P.

Ορισμός: Ένας $(M, m, l, t,)$ - ασαφής εξαγωγέας είναι ένα ζευγάρι αλγορίθμων, ‘’γέννεσης’’ (Gen) και ‘’αναπαραγωγής’’ (Rep), με τις ακόλουθες ιδιότητες:

1. Ο αλγόριθμος Gen με είσοδο ένα βιομετρικό στοιχείο $w \in M$ εξάγει μια συμβολοσειρά $R \in \{0,1\}^l$ και μια βοηθητική συμβολοσειρά $P \in \{0,1\}^*$.
2. Ο αλγόριθμος Rep με είσοδο ένα προσεγγιστικό βιομετρικό του αρχικού ŵ $\in M$ και τη συμβολοσειρά $P \in \{0,1\}^*$ θα εξάγει το R, μόνο αν $dis(w, \hat{w}) < t$, δηλαδή αν το προσεγγιστικό βιομετρικό και το πρότυπο είναι αρκετά όμοια, και αν οι P, R προέρχονται από τον αλγόριθμο Gen με είσοδο το πρότυπο βιομετρικό w.

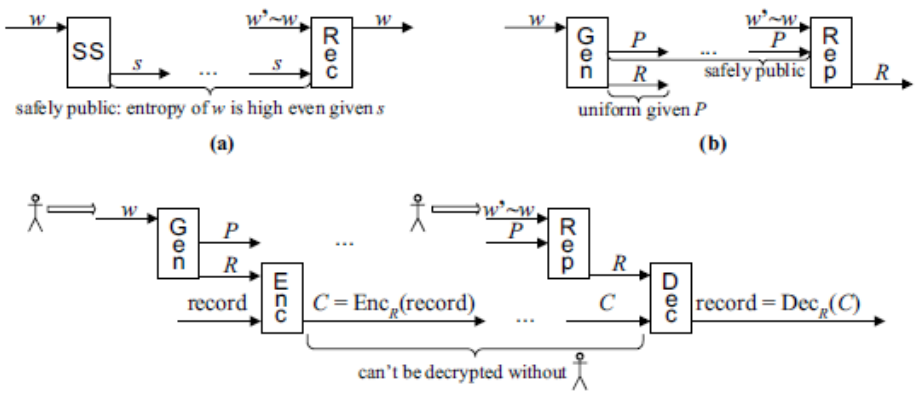
3. Οι παράμετροι ασφάλειας πιστοποιούν ότι για κάθε κατανομή W στον M, ελάχιστης εντροπίας m, η σειρά R είναι ομοιόμορφα κατανεμημένη ακόμα και για αυτούς που γνωρίζουν τη δημόσια σειρά P.
   Αν $((R,P) \leftarrow Gen(W),\ τότε\ SD\big((R,P),(U_l,P)\big) \leq e.$



Εικόνα17: Fuzzy Extractor *(55)*

Ως ένα παράδειγμα του τρόπου χρήσης ασαφών εξαγωγέων, στην περίπτωση ελέγχου ταυτότητας κωδικού πρόσβασης, ο server μπορεί να αποθηκεύσει $(P, f\ (R))$.Όταν ο χρήστης εισάγει w', κοντά στο w, ο server αναπαράγει το πραγματικό R χρησιμοποιώντας το P και ελέγχει εάν το $f\ (R)$ ταιριάζει με αυτό που έχει αποθηκευτεί.

Η σχεδόν ομοιόμορφη λοιπόν έξοδος τυχαίων bits από έναν ασαφή εξαγωγέα μπορεί να χρησιμοποιηθεί σε οποιοδήποτε κρυπτογραφικό πλαίσιο που απαιτεί ομοιόμορφα τυχαία bits (π.χ. για μυστικά κλειδιά). Η ελαφρά ανομοιομορφία των bits μπορεί να μειώνει την ασφάλεια αλλά όχι την απόσταση τους από την ομοιόμορφη κατανομή.



Εικόνα***Σφάλμα! Το αρχείο προέλευσης της αναφοράς δεν βρέθηκε.***: α)Secure Sketch, b)Fuzzy Extractor, c)Παράδειγμα: χρήστης που κρυπτογραφεί χρησιμοποιώντας ένα ισχυρό, ομοιόμορφο κλειδί R που εξάγεται από βιομετρικό w μέσω ενός ασαφούς εξαγωγέα. Τόσο το P όσο και η κρυπτογραφημένη εγγραφή δεν χρειάζεται να διατηρηθούν μυστικά, γιατί κανείς δεν μπορεί να αποκρυπτογραφήσει την εγγραφή χωρίς ένα w_0 που είναι μια προσέγγισή του. *(54)*

Ως ένα βήμα στην κατασκευή ασαφών εξαγωγέων, προτείνουμε τα secure sketches. Επιτρέπουν την ακριβή ανακατασκευή μιας θορυβώδους εισόδου, ως εξής: με είσοδο ένα βιομετρικό δεδομένο w, μια διαδικασία εξάγει ένα sketch s, δηλαδή μια δημόσια συμβολοσειρά. Στη συνέχεια, δεδομένου του s και ενός βιομετρικού w' ,προσέγγιση του w, είναι δυνατή η ανάκτηση του πρότυπου w.Το sketch είναι ασφαλές με την έννοια ότι δεν αποκαλύπτει πολλά για το πρότυπο w. Διατηρεί μεγάλο μέρος της εντροπίας του ακόμη και αν είναι γνωστό. Έτσι, αντί να αποθηκευτεί το w με το φόβο ότι οι μεταγενέστερες αναγνώσεις θα είναι θορυβώδεις, είναι δυνατό να αποθηκευτεί αντί αυτού το s, χωρίς να διακυβεύεται το απόρρητο του w. Ένα secure sketch, σε αντίθεση με έναν ασαφή εξαγωγέα, επιτρέπει την ακριβή αναπαραγωγή της αρχικής εισόδου, αλλά δεν αντιμετωπίζει την ανομοιομορφία.

Τα secure sketches και οι εξαγωγείς μπορούν να θεωρηθούν ότι παρέχουν αποθήκευση ασαφών κλειδιών: επιτρέπουν την ανάκτηση του μυστικού κλειδιού (w ή R) από μια ‘’ελαττωματική’’ ανάγνωση w' του κωδικού πρόσβασης w χρησιμοποιώντας ορισμένες δημόσιες πληροφορίες (s ή P).

Επειδή διαφορετικές βιομετρικές πληροφορίες έχουν διαφορετικά μοτίβα σφαλμάτων, δεν υποθέτουμε καμία ιδιαίτερη ομοιότητα μεταξύ w' και w. Υποθέτουμε απλώς ότι το w προέρχεται από κάποιο μετρικό χώρο και ότι το w' δεν είναι κάτι περισσότερο από μία προσέγγισή του που απέχει μια ορισμένη απόσταση από το ίδιο το w σε αυτόν τον χώρο (54) (21).

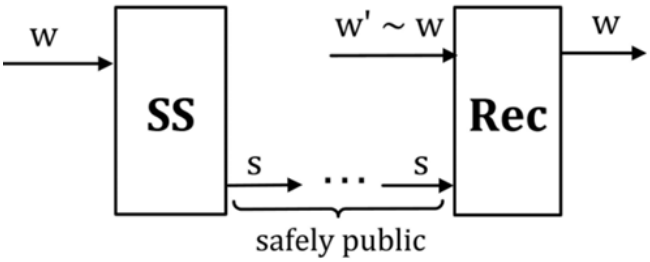
7.7 Εισαγωγή στα ασφαλή σκίτσα (Secure Sketches)

Η κύρια πρόκληση της χρήσης βιομετρικών δεδομένων στην κρυπτογραφία είναι ότι δεν μπορούν να αναπαραχθούν ακριβώς. Κάποιος θόρυβος θα εισαχθεί αναπόφευκτα στα βιομετρικά δείγματα κατά την απόκτηση και την επεξεργασία. Ορισμένες τεχνικές προσπαθούν να διορθώσουν τον θόρυβο στα δεδομένα χρησιμοποιώντας κάποιες δημόσιες πληροφορίες που προέρχονται από το αρχικό βιομετρικό πρότυπο. Μία από αυτές τις τεχνικές είναι και τα ασφαλή σκίτσα (secure sketches).

Υπάρχουν δύο βασικά στοιχεία σε ένα secure sketch. Το πρώτο είναι ο αλγόριθμος δημιουργίας των sketches: παίρνει το αρχικό βιομετρικό πρότυπο ως είσοδο και εξάγει ένα σκίτσο (δημόσια συμβολοσειρά). Το δεύτερο είναι ο αλγόριθμος βιομετρικής ανακατασκευής προτύπου, ο οποίος παίρνει ένα άλλο βιομετρικό πρότυπο, το οποίο είναι προσέγγιση του αρχικού, και το σκίτσο ως εισόδους και θα πρέπει σαν έξοδο να έχει το αρχικό βιομετρικό πρότυπο. Τα δύο αυτά βιομετρικά στοιχεία θα πρέπει να είναι αρκετά παρόμοια μεταξύ τους, σύμφωνα με κάποιο μέτρο ομοιότητας. Μια σημαντική απαίτηση είναι ότι το σκίτσο δεν πρέπει να αποκαλύπτει πάρα πολλές πληροφορίες σχετικά με το βιομετρικό δεδομένο. Την απαίτηση έρχεται να ικανοποιήσει η έννοια της ελάχιστης εντοπίας, καθώς και η έννοια της απώλειας εντροπίας, η οποία μετρά το πλεονέκτημα που δίνει το σκίτσο σε οποιονδήποτε αντίπαλο να ¨μαντέψει¨ το βιομετρικό. Αξίζει να σημειωθεί ότι η απώλεια εντροπίας είναι η χειρότερη περίπτωση για όλες τις κατανομές των βιομετρικών δεδομένων (56).

Τα secure sketches ουσιαστικά πραγματοποιούν διόρθωση σφάλματος σε ένα μήνυμα (βιομετρικό στοιχείο) χωρίς να χρησιμοποιούν πολλές πληροφορίες από το ίδιο το μήνυμα. Αποτελείται, όπως αναφέραμε από ένα ζεύγος αλγορίθμων δημιουργίας σκίτσου (δημόσιας πληροφορίας-συμβολοσειράς) (SS) και ανακατασκευής (Rec). Πιο αναλυτικά:

- Ο αλγόριθμος SS με είσοδο το πρότυπο βιομετρικό δεδομένο $w \in W$ δίνει σαν έξοδο μια βοηθητική δημόσια συμβολοσειρά $s \in \{0,1\}^*$.
- Ο αλγόριθμος Rec με είσοδο s και ŵ (βιομετρικό που είναι μια προσέγγιση του αρχικού w), δίνει σαν έξοδο το πρότυπο w, όπου προφανώς τα ŵ και w θα πρέπει να είναι αρκετά όμοια.



Εικόνα18: Secure Sketch *(55)*

Ορθότητα: Επειδή η κάθε σάρωση του ίδιου βιομετρικού δεδομένου δεν είναι πανομοιότυπη, οι μετέπειτα σαρώσεις του θα αποτελούν προσεγγίσεις της πρωτότυπης. Ωστόσο, μεταξύ των προσεγγίσεων και του πρωτότυπου θα πρέπει να υπάρχει ένα όριο

απόστασης ώστε ένας εξουσιοδοτημένος χρήστης να μπορεί να έχει πρόσβαση κάθε φορά παρά τις μικροδιαφορές στις σαρώσεις του. Δηλαδή, για όλα τα $w, \hat{w}$ θα πρέπει $d(w, \hat{w}) \leq t$ (όπου t παράμετρος απόστασης) και

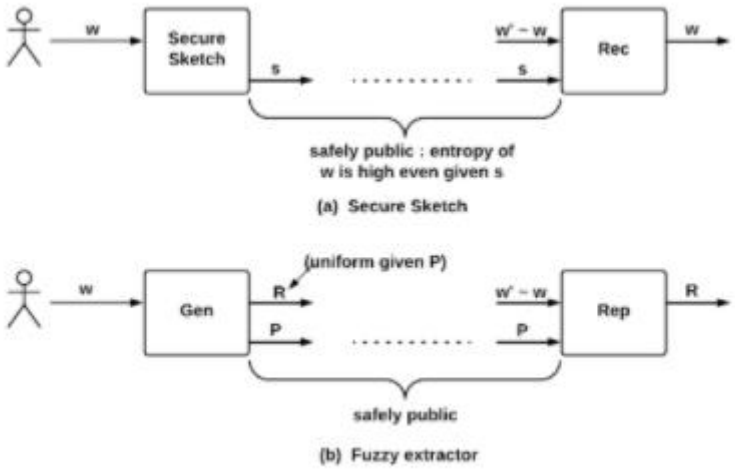
$$Pr[Rec(s, \hat{w}) = w; s \leftarrow \$SS(w)] \geq 1 - \varepsilon. \quad (19)$$

Ασφάλεια: Όταν συζητάμε για την ασφάλεια, μας ενδιαφέρει η πιθανότητα που έχει ένας κακόβουλος χρήστης να προβλέψει μια τυχαία τιμή (π.χ. μαντεύει ένα μυστικό κλειδί). Η καλύτερη στρατηγική του αντιπάλου, οπότε, είναι να μαντέψει την πιο πιθανή τιμή. Έτσι, για την πρόβλεψη μιας τυχαίας μεταβλητής A θα έχουμε $maxaPr\,[A = a]$, και, αντίστοιχα, η ελάχιστη εντροπία $H\infty(A) = -log\,(maxκPr\,[A = a])$, η οποία χαρακτηρίζεται από το μέγιστο αριθμό k τέτοιο ώστε για κάθε $a \in A$ η πιθανότητα $P(A = \alpha) \leq 2^{-k}$.

Η ελάχιστη εντροπία μιας κατανομής μας δείχνει πόσα σχεδόν ομοιόμορφα τυχαία bits μπορούν να εξαχθούν από αυτήν. Η έννοια του «σχεδόν» ορίζεται ως εξής: η στατιστική απόσταση μεταξύ δύο κατανομών πιθανότητας A και B είναι $SD(A, B) = \frac{1}{2}\sum_v |\Pr(A = v) - \Pr(B = v)|$.

7.8 Κατασκευή ασαφών εξαγωγέων από ασφαλή σκίτσα

Τα ασφαλή σκίτσα αποτελούν δομικά στοιχεία για τους ασαφείς εξαγωγείς. Η διαφορά είναι ότι οι ασαφείς εξαγωγείς επιστρέφουν μια ομοιόμορφη συμβολοσειρά, ενώ το ασφαλές σκίτσο επιστρέφει μια μη ομοιόμορφη συμβολοσειρά. Επειδή το ασφαλές σκίτσο μπορεί να ανακατασκευάσει την αρχική είσοδο από ορισμένα θορυβώδη δεδομένα, μπορεί να χρησιμοποιηθεί για την κατασκευή των εξαγωγέων.



Εικόνα 19: (a) Secure Sketch (b) Fuzzy Extractor *(54)*

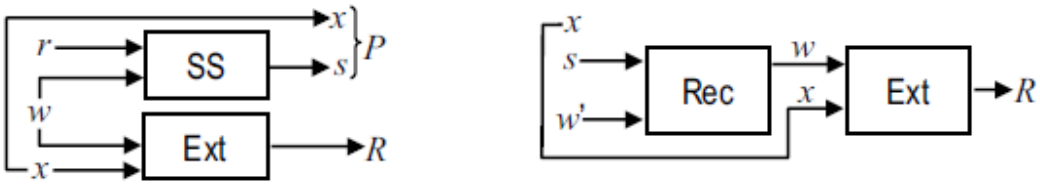
Το ασφαλές σκίτσο για μία είσοδο w, εξάγει ένα σκίτσο s. Έπειτα, δεδομένου του s και μιας τιμής πλησίον του w, είναι δυνατή η ανάκτηση του w. Ο ασαφής εξαγωγέας εξάγει μια ομοιόμορφα τυχαία συμβολοσειρά R από την είσοδό της w με ανοχή ως προς το θόρυβο. Ανοχή θορύβου σημαίνει ότι εάν η είσοδος αλλάξει σε κάποια w ′ αλλά παραμείνει κοντά, η συμβολοσειρά R μπορεί να αναπαραχθεί ακριβώς.

Οι ασαφείς εξαγωγείς επιτρέπουν σε κάποιον να εξαγάγει μία τυχαία συμβολοσειρά R (χρησιμοποιώντας τον αλγόριθμο παραγωγής Gen) από το βιομετρικό w και στη συνέχεια να αναπαραγάγει επιτυχώς την R (χρησιμοποιώντας τον αλγόριθμο αναπαραγωγής Rep) από οποιαδήποτε συμβολοσειρά w ′ που είναι προσέγγιση του w. Για έναν αποτελεσματικό ασαφή εξαγωγέα, οι αλγόριθμοι Gen και Rep πρέπει να εκτελούνται σε πολυωνυμικό χρόνο (50).

Προκειμένου λοιπόν να μετατρέψουμε τα βιομετρικά δεδομένα σε ομοιόμορφα τυχαίες συμβολοσειρές και να διατηρηθεί η υψηλή εντροπία, θα χρησιμοποιήσουμε αυτήν την κατασκευή.

Εφαρμόζουμε τον αλγόριθμο SS στο βιομετρικό *w* για να εξάγουμε τη βοηθητική συμβολοσειρά (σκίτσο) s και έναν ισχυρό εξαγωγέα Ext με τυχαιότητα x (ένας ισχυρός εξαγωγέας επιτρέπει σε κάποιον να εξαγάγει σχεδόν όλη την ελάχιστη εντροπία από κάποια μη ομοιόμορφη τυχαία μεταβλητή, βλέπε 8.2.3) ο οποίος με είσοδο το βιομετρικό w εξάγει το κλειδί R.Το ζεύγος (s,x) αποθηκεύεται ως το βοηθητικό string P.

Για να αναπαράγουμε την R από μία προσέγγιση του βιομετρικού δεδομένου $\hat{w}$ και το P=(s,x), πρώτα χρησιμοποιούμε τον αλγόριθμο Rec με εισόδους τα $\hat{w}$ και s, για να παραχθεί το βιομετρικό w και έπειτα τον Ext με εισόδους w και x για να παραχθεί το R.



Εικόνα 20:Κατασκευή fuzzy extractor από secure sketch *(54)*

Πρώτον, για να γίνει εφαρμογή του ισχυρού εξαγωγέα στο βιομετρικό w, υποθέτουμε ότι αναπαρίσταται με στοιχεία του W χρησιμοποιώντας n bits. Δεύτερον, έπειτα από την εξαγωγή του secure sketch s, το w έχει μόνο conditional min-entropy και τεχνικά πρέπει να χρησιμοποιήσουμε average-case strong extractor.

Πιο συγκεκριμένα αν έχουμε ένα $(M, m, \tilde{m}, t)$ −secure sketch (που αποτελείται από το ζεύγος αλγορίθμων (SS, Rec) και Ext έναν average-case$(n, \tilde{m}, l, t)$ −strong extractor, τότε θα έχουμε τον παρακάτω (M, m, l, t, e) −fuzzy extractor:

- $Gen(w; r, x)$: με είσοδο $P(SS(w; r), x)$, $R = Ext(w; x)$ και έξοδο (R, P)
- $Rep(w', (s, x))$: ανάκτηση του wμέσω $Rec(w', s)$ και έξοδο $R = Ext(w; x)$

Πρόσθετες ιδιότητες των secures ketches και fuzzy extractor (53):

- Επαναχρησιμοποίηση (Reusability): ένα σκίτσο θεωρείται επαναχρησιμοποιήσιμο εάν παρατηρώντας πολλά διαφορετικά σκίτσα της ίδιας τιμής αποκαλύπτει ελάχιστες πρόσθετες πληροφορίες σχετικά με αυτήν την τιμή.
- Ανθεκτικότητα (Robustness) : Ένα σκίτσο θεωρείται ανθεκτικό/ισχυρό εάν ένας αντίπαλος δεν μπορεί να παράγει ένα διαφορετικό έγκυρο σκίτσο του βιομετρικού w αφού δει ένα σκίτσο του w.
- Εσωτερικά ασφαλές (Insider Secure):ένας ασαφής εξαγωγέας θεωρείται ασφαλής εσωτερικά εάν ένας αντίπαλος που είναι ικανός να δει πολλαπλά σκίτσα ενός μυστικού, και παρατηρεί το κλειδί που εξάγεται, δεν μπορεί να

μάθει πληροφορίες σχετικά με το κλειδί που εξάγεται από ένα μη τροποποιημένο άγνωστο σκίτσο (57)

7.9 Average-case extractor

Όπως έχει αναφερθεί στο εδάφιο 7.8, ένας ισχυρός εξαγωγέας επιτρέπει να εξαγάγει σχεδόν όλη την ελάχιστη εντροπία από κάποια μη ομοιόμορφη τυχαία μεταβλητή W. Σε πολλές περιπτώσεις, το W αντιπροσωπεύει την αβεβαιότητα του αντιπάλου σχετικά με κάποιο μυστικό w, που εξαρτάται από κάποιες πληροφορίες i, για τις οποίες όμως υπάρχουν πιθανότητες να γίνουν αντιληπτές από τον αντίπαλο.

Ορισμός 1: Έστω Ext: $\{0,1\}^n \to \{0,1\}^l$ μία πολυωνυμικού χρόνου συνάρτηση πιθανότητας η οποία χρησιμοποιεί r bits τυχαιότητας (r σε αριθμό τυχαία bits). Ο εξαγωγέας Ext είναι ένας (n, m, l, e) −strong extractor αν για όλες τις κατανομές W στο $\{0,1\}^n$ ελάχιστης εντροπίας m, έχουμε $SD((Ext(W;X),X),(U_l,X)) \le e$, όπου X ομοιόμορφη κατανομή στον $\{0,1\}^r$.

Ορισμός 2: Έστω Ext: $\{0,1\}^n \to \{0,1\}^l$ μία πολυωνυμικού χρόνου συνάρτηση πιθανότητας η οποία χρησιμοποιεί r bits τυχαιότητας. Ο εξαγωγέας Ext είναι ένας average-case$(n, \acute{\alpha}, l, e)$ −strong extractor αν για όλα τα ζεύγη των τυχαίων μεταβλητών (W,I), όπου το W είναι μία συμβολοσειρά n-bit τέτοια ώστε $\overline{H}\infty(W \mid I) \ge m$, να έχουμε $SD((Ext(W;X),(X,I),(U_l,X,I)) \le e$, όπου X ομοιόμορφη κατανομή στο $\{0,1\}^r$.

7.10 Ασφαλή Σκίτσα για Μεταβατικούς Μετρικούς χώρους

Υπάρχει μία γενική τεχνική για την κατασκευή ασφαλών σκίτσων σε μεταβατικούς μετρικούς χώρους. Ας ορίσουμε αρχικά τους χώρους αυτούς. Μια αναδιάταξη π σε έναν μετρικό χώρο M είναι μια ισομετρία εάν διατηρεί αποστάσεις, δηλαδή,

$dis(a,b) = dis(\pi(a), \pi(b))$. Ένα σύνολο $\Pi = \{\pi_i\}_{i \in I}$, λειτουργεί μεταβατικά στο χώρο M, αν για κάθε δύο στοιχεία $a, b \in M$ υπάρχουν $\pi_i \in \Pi$ τέτοια ώστε $\pi_i(a) = b$.

Κατασκευάζοντας ένα secure sketch λειτουργούμε ως εξής: Έστω ένα σύνολο C= $\{w_0, ...w_{K-1}\}$ K στοιχείων στο χώρο M. Για τον αλγόριθμο SS για μία είσοδο $w \in M$, διαλέγουμε ένα ομοιόμορφα τυχαίο $b \in C$ και ένα ομοιόμορφα τυχαίο $\pi \in \Pi$, τέτοιο ώστε $\pi(w) = b$ και έχουμε ως έξοδο $SS(w) = \pi$ (είναι σημαντικό κάθε $\pi \in \Pi$, να είναι ανεξάρτητο από τον τρόπο με τον οποίο επιλέχθηκε και, ειδικότερα, ανεξάρτητο από τα b και w: ο αριθμός των πιθανών εξόδων SS πρέπει να είναι |Π|). Για τον αλγόριθμο Rec, μέσω του οποίου πρέπει να ανακτηθεί το w από το w' και το σκίτσο π ισχύει: βρίσκεται το πιο κοντινό b' του $\pi(w')$ και έχουμε ως έξοδο $\pi^{-1}(b')$.

Ας είναι Γ ο αριθμός των στοιχείων $\pi \in \Pi$, τέτοιος ώστε $\min_{w,b} |\{\pi \mid \pi(w) = b\}| \geq \Gamma$, τότε για κάθε w, b θα υπάρχουν τουλάχιστον Γ επιλογές του π.

Κεφάλαιο 8. Απομακρυσμένος έλεγχος πρόσβασης μέσω Secure Sketches και Fuzzy Extractors

Μέχρι τώρα δεν ελέγχαμε την περίπτωση της τροποποίησης των δημόσιων βοηθητικών δεδομένων. Στο κεφάλαιο αυτό αναφερόμαστε σε επεκτάσεις των τεχνικών των secure sketches και fuzzy extractors, ώστε να πραγματοποιείται με ασφάλεια απομακρυσμένος έλεγχος πρόσβασης για αυτή την περίπτωση. Τέλος, παρουσιάζουμε περισσότερο ασφαλή λύση που βασίζεται στη χρήση ενός πρωτοκόλλου ανταλλαγής κλειδιών.

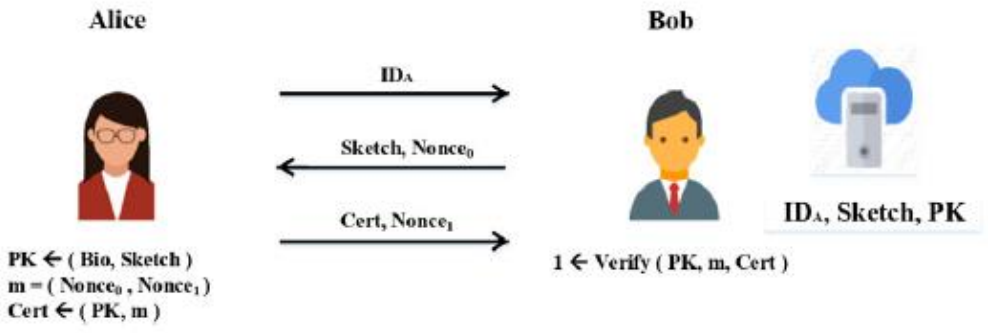
8.1 Απομακρυσμένος έλεγχος πρόσβασης

Ο έλεγχος ταυτότητας χρηστών που βασίζεται σε βιομετρικά στοιχεία έχει χρησιμοποιηθεί ευρέως σε πολλές πραγματικές εφαρμογές όπως η ασφάλεια κινητής τηλεφωνίας, οι οικονομικές συναλλαγές και οι έλεγχοι αναγνώρισης (58).Υπάρχουν πολλά ελκυστικά χαρακτηριστικά που φέρουν τα βιομετρικά δεδομένα σε σχέση με τους συμβατικούς κωδικούς πρόσβασης. Για παράδειγμα, οι άνθρωποι πρέπει να θυμούνται πολλούς ασφαλείς κωδικούς πρόσβασης για διάφορους λογαριασμούς και να ενημερώνουν συχνά τους κωδικούς αυτούς για λόγους ασφαλείας. Αντίθετα, τα βιομετρικά στοιχεία συνδέονται μόνιμα και μοναδικά με ένα άτομο, επομένως είναι και πιο βολικό να χρησιμοποιούνται για τον έλεγχο ταυτότητας χρήστη.

Ο έλεγχος ταυτότητας χρήστη που βασίζεται σε βιομετρικά στοιχεία οδηγεί επίσης σε ορισμένα ζητήματα ασφάλειας και χρηστικότητας. Πρώτον, η βιομετρική δεν είναι ανακλητή. Εάν τα βιομετρικά στοιχεία έχουν τεθεί σε κίνδυνο, τότε ο χρήστης ενδέχεται να χάσει την ασφάλειά του για πάντα. Δεύτερον, οι εξουσιοδοτημένοι χρήστες ενδέχεται να ανησυχούν για την ασφάλεια των βιομετρικών στοιχείων τους που είναι αποθηκευμένα στον διακομιστή ελέγχου ταυτότητας. Επομένως, κανένα βιομετρικό στοιχείο δεν πρέπει να αποθηκεύεται ως απλό κείμενο από την πλευρά του

διακομιστή επειδή τα βιομετρικά στοιχεία ενδέχεται να περιέχουν πληθώρα προσωπικών πληροφοριών (π.χ. DNA).

Δύο οντότητες, οι οποίες μοιράζονται έναν κωδικό πρόσβασης, και που επικοινωνούν μέσω ενός μη ασφαλούς δικτύου, θέλουν να επικυρώσουν ο ένας τον άλλον και να συμφωνήσουν σε ένα κλειδί που θα χρησιμοποιηθεί για την προστασία της επακόλουθης επικοινωνίας τους. Αυτό ονομάζεται πρόβλημα ελέγχου ταυτότητας με ανταλλαγή κλειδιών (password-authenticated key exchange). Εάν μία από τις οντότητες είναι ο χρήστης και η άλλη είναι διακομιστής, τότε αυτό μπορεί να θεωρηθεί ως πρόβλημα απομακρυσμένου ελέγχου πρόσβασης χρήστη (59).



Εικόνα 21: Αυθεντικοποίηση χρηστών με βάση τα βιομετρικά τους στοιχεία (60).

Για παράδειγμα, στην παραπάνω εικόνα, ο διακομιστής Bob διατηρεί μια βάση δεδομένων για την αποθήκευση των εγγεγραμμένων πληροφοριών από όλους τους εγγεγραμμένους χρήστες, η οποία περιλαμβάνει τον χρήστη Alice με ταυτότητα ID_A. Ένα ασφαλές σκίτσο (δηλαδή, μια "κρυπτογραφημένη" μορφή βιομετρικών) χρησιμοποιείται για την ανάκτηση των αρχικών βιομετρικών στοιχείων από μια προσέγγιση αυτών των αρχικών βιομετρικών.

Εστιάζουμε στον απομακρυσμένο έλεγχο ταυτότητας χρηστών που βασίζεται σε βιομετρικά στοιχεία χρησιμοποιώντας ασαφή εξαγωγέα που επιτρέπει στον εξουσιοδοτημένο χρήστη Alice να πιστοποιεί τον εαυτό της σε έναν απομακρυσμένο διακομιστή, τον Bob, χρησιμοποιώντας τα βιομετρικά της. Συγκεκριμένα, η Alice βασίζεται στο εγγεγραμμένο σκίτσο της που είναι αποθηκευμένο στον διακομιστή προκειμένου να αντλήσει ένα δημόσιο κλειδί για τη δημιουργία ενός πιστοποιητικού

που σχετίζεται με ένα μήνυμα (π.χ. nonce). Στη συνέχεια, ο Bob επαληθεύει το πιστοποιητικό βάσει του εγγεγραμμένου δημόσιου κλειδιού της Alice (βλ. Εικ. 12). Τονίζουμε ότι καμία πληροφορία δεν αποθηκεύεται τοπικά από την πλευρά του χρήστη και ότι κανένα βιομετρικό δεν αποθηκεύεται σε απλό κείμενο από την πλευρά του διακομιστή (δηλαδή, βιομετρικό απόρρητο).

Ο ασαφής εξαγωγέας είναι μια πολλά υποσχόμενη προσέγγιση για την κατασκευή ενός συστήματος ελέγχου ταυτότητας χρήστη (απομακρυσμένου) που βασίζεται σε βιομετρικά στοιχεία. Οι Dodis et al. (21) εισήγαγαν επίσημα την έννοια των ασφαλών σκίτσων και των ασαφών εξαγωγέων. Χρησιμοποίησαν βιομετρικά στοιχεία για να αντλήσουν ένα κρυπτογραφικό κλειδί για διάφορες κρυπτογραφικές εφαρμογές, όπως έλεγχο ταυτότητας βάσει κωδικού πρόσβασης. Όσον αφορά συγκεκριμένες επιθέσεις στον ασαφή εξαγωγέα, οι Boyen et al. (61) εισήγαγαν μια έννοια που ονομάζεται «ισχυρά σκίτσα». Παρέχουν μια γενική μετατροπή για την αντιμετώπιση ενεργών επιθέσεων όπου ο αντίπαλος είναι σε θέση να τροποποιήσει το δημόσιο σκίτσο (ή βοηθητικά δεδομένα) και να θέσει σε κίνδυνο την ασφάλεια των ασαφών εξαγωγέων .

8.2 Έλεγχος πρόσβασης και πιστοποίησης με Secure sketches

Τα δύο κύρια μειονεκτήματα των βιομετρικών δεδομένων, είναι ότι δεν είναι ομοιόμορφα κατανεμημένα και ότι δεν μπορούν να αναπαραχθούν ακριβώς. Για να ξεπεραστούν αυτά τα εμπόδια δημιουργήθηκαν οι τεχνικές των secure sketches και fuzzy extractors οι οποίες επιτρέπουν την αποστολή κάποιων βοηθητικών δημόσιων πληροφοριών από τον server στον χρήστη. Κατασκευάζουν ένα δημόσιο string το οποίο αποθηκεύεται στον server και αποστέλλεται στον χρήστη. Με απλά λόγια αυτό το δημόσιο string κωδικοποιεί τις πληροφορίες που απαιτούνται για την ανάκτηση του μυστικού και της επακόλουθης εξαγωγής. Έχουν κατασκευαστεί έτσι ώστε να είναι ασφαλή ακόμα και όταν ο αντίπαλος γνωρίζει αυτό το δημόσιο string ή αλλιώς παρακολουθεί το κανάλι επικοινωνίας μεταξύ server και χρήστη.

Ωστόσο, δεν υπάρχει κάποια μέθοδος που να παρέχει ασφαλή έλεγχο ταυτότητας στην παρουσία ενός ενεργού αντιπάλου ο οποίος μπορεί να τροποποιήσει τα μηνύματα που αποστέλλονται μεταξύ του διακομιστή και του χρήστη. Ένας αντίπαλος που μεταβάλλει τη δημόσια συμβολοσειρά που αποστέλλεται σε έναν χρήστη μπορεί να είναι σε θέση να μάθει τα βιομετρικά δεδομένα αυτού του χρήστη στο σύνολό τους.

Μία λύση για τον χρήστη είναι να αποθηκεύσει ο ίδιος το string αντί να το αποκτήσει από τον διακομιστή, ή να πιστοποιήσει το string χρησιμοποιώντας άλλους τρόπους. Η συγκεκριμένη λύση, όμως, καταργεί τον σκοπό της χρήσης βιομετρικών δεδομένων στην πρώτη θέση, δηλαδή, την αποφυγή αποθήκευσης πρόσθετων κρυπτογραφικών πληροφοριών από τον χρήστη , ακόμη και αν αυτές οι πληροφορίες δεν χρειάζεται να διατηρηθούν μυστικές.

Μία άλλη λύση είναι ο αμοιβαίος έλεγχος ταυτότητας, ο οποίος συνεπάγεται ότι κατά την επικοινωνία μέσω ενός μη ασφαλούς δικτύου , ο χρήστης και ο διακομιστής δεν μπορούν να δημιουργήσουν με ασφάλεια ένα κοινόχρηστο κλειδί περιόδου λειτουργίας με το οποίο να κρυπτογραφούν και να ελέγχουν τα μελλοντικά μηνύματα καθώς ο χρήστης μπορεί να μοιραστεί ακούσια ένα κλειδί με έναν αντίπαλο που μπορεί στη συνέχεια να αποκρυπτογραφήσει τυχόν δεδομένα που αποστέλλονται από αυτόν τον χρήστη καθώς και να ελέγξει αυθαίρετα δεδομένα.

Θα παρουσιάσουμε δύο τεχνικές, η πρώτη μπορεί να θεωρηθεί ως μία γενική λύση που προστατεύει απέναντι στην τροποποίηση της δημόσιας πληροφορίας όταν γίνεται χρήση ασφαλών σκίτσων ή ασαφών εξαγωγέων και η δεύτερη τεχνική εστιάζει στον απομακρυσμένο έλεγχο ταυτότητας και στην ανταλλαγή κλειδιών.

Οι τεχνικές των ασφαλών σκίτσων και ασαφών εξαγωγέων χρειάστηκε λοιπόν να επεκταθούν. Θεωρούμε την έννοια των ισχυρών σκίτσων και ασαφών εξαγωγέων που προστατεύουν από αυτό το είδος επίθεσης. Δεδομένου ότι ενδιαφερόμαστε για την περίπτωση που τα μέρη επικοινωνούν μέσω ενός μη εξουσιοδοτημένου καναλιού, ωστόσο, θέλουμε να κατασκευάσουμε ισχυρούς ασαφείς εξαγωγείς που επιπλέον προστατεύουν από κακόβουλες τροποποιήσεις της δημόσιας πληροφορίας. Πλέον, θα πρέπει να υπάρχει η δυνατότητα εάν ο αντίπαλος στέλνει οποιαδήποτε τροποποιημένη τιμή της δημόσιας συμβολοσειράς, τότε με μεγάλη πιθανότητα, να απορριφθεί.

8.2.1 Μοντελοποίηση σφαλμάτων

Καθώς η διόρθωση σφαλμάτων αποτελεί βασική προϋπόθεση, είναι απαραίτητο να αναπτυχθεί κάποιο μοντέλο των τύπων σφαλμάτων που ενδέχεται να προκύψουν. Σύμφωνα με τον Boyen (62), το σφάλμα σε διάφορες βιομετρικές αναγνώσεις θεωρήθηκε ότι βρίσκεται υπό τον έλεγχο του αντιπάλου, με τον περιορισμό ότι ο

αντίπαλος μπορούσε να καθορίσει μόνο σφάλματα ανεξάρτητα από δεδομένα (π.χ. σταθερές μετατοπίσεις). Αυτό όμως δεν είναι ένα ρεαλιστικό μοντέλο στην πράξη καθώς μπορεί κάποια χαρακτηριστικά των βιομετρικών δεδομένων να είναι πιο ευαίσθητα σε λάθη.

Θεωρούμε ένα πιο γενικό μοντέλο σφάλματος, όπου τα σφάλματα μπορεί να εξαρτώνται από τα δεδομένα και συνεπώς να συσχετίζονται όχι μόνο το ένα με το άλλο αλλά και με το ίδιο το βιομετρικό μυστικό. Επιπλέον, καθώς ενδιαφερόμαστε τελικά για τη μοντελοποίηση της ΄΄φύσης΄΄, όπως εκδηλώνεται στις φυσικές διεργασίες που προκαλούν διακυμάνσεις στις βιομετρικές μετρήσεις, δεν απαιτείται τα υπολογιστικά λάθη να είναι εύκολα υπολογιστικά. Ο μόνος περιορισμός που κάνουμε είναι ότι τα σφάλματα πρέπει να είναι «μικρά» και, συγκεκριμένα, να είναι μικρότερα από το επιθυμητό όριο διόρθωσης σφαλμάτων, καθώς η διόρθωση σφαλμάτων που δεσμεύεται σε οποιαδήποτε πραγματική εφαρμογή θα πρέπει να επιλεγεί με τρόπο ώστε να διασφαλιστεί η ορθότητα με μεγάλη πιθανότητα. Πιο αναλυτικά:

Ορίζουμε πρώτα ότι ένας χώρος πιθανοτήτων (Ω,P) είναι ένα σύνολο Ω και μία συνάρτηση $P:\Omega\to[0,1]$, τέτοια ώστε $\sum_{\omega\in\Omega}P(\omega)=1$. Μια τυχαία μεταβλητή W που ορίζεται από το χώρο πιθανότητας (Ω,P) και παίρνει τιμές σε ένα σύνολο M, είναι μία συνάρτηση $W:\Omega\to\mathrm{M}$. Για μία τέτοια τυχαία μεταβλητή ορίζουμε $w\leftarrow W$ στο οποίο ένα $r\in\Omega$ επιλεγμένο σύμφωνα με την P, και στο w εκχωρείται η τιμή $W(r)$. Αν ένας χώρος πιθανότητας (Ω,P) στον οποίο ορίζονται δύο μεταβλητές W και W', οι οποίες παίρνουν τιμές σε έναν μετρικό χώρο M με συνάρτηση απόστασης d, τότε λέμε ότι όταν $d(W,W')\le t$ τότε για κάθε $r\in\Omega$ ισχύει $d(W(r),W'(r))\le t$.

Ένα δείγμα $W=\{W_i\}_{i=0}$ με t-όριο διόρθωσης σφάλματος είναι ένα σύνολο, είναι μία σειρά τυχαίων μεταβλητών $W_i:\Omega\to\mathrm{M}$ τέτοια ώστε για κάθε i να ισχύει $d(W_0,W_i)\le t$, όπου W_0 το πρότυπο βιομετρικό δεδομένο και W_i είναι το βιομετρικό δεδομένο του χρήστη την i-οστή φορά που θα σκανάρει τα βιομετρικά στοιχεία του. Ανεξάρτητα από το πρωτόκολλο το οποίο χρησιμοποιείται, ένας αντίπαλος μπορεί πάντα να εξαπατήσει τον server όταν μαντέψει σωστά τα βιομετρικά δεδομένα ενός χρήστη.

Τα ακόλουθα λήμματα δεσμεύουν την πιθανότητα αυτής της επίθεσης. Πρώτον, δείχνουμε ότι η ελάχιστη εντροπία κάθε W_i είναι στη χειρότερη $\log Vol_t^M$ bits

μικρότερη από αυτή του W_0. Όπου $\log Vol_t^M(x) = |\{x' \in M \mid d(x', x) \le t\}|$ και $\log Vol_t^M = \max_{x \in M}\{Vol_t^M(x)\}$.Επιπλέον, δείχνουμε ότι το W_i δεν είναι πιο εύκολο να το μαντέψει κανείς από το W_0 υποθέτοντας ότι το σκίτσο του (SS (W_0))είναι διαθέσιμο.

Λήμμα 1 : Έστω W_0, W_i είναι τυχαίες μεταβλητές που λαμβάνουν τιμές σε ένα χώρο M και ικανοποιούν τη σχέση $d(W_0, W_i) \le t$ και έστω B μια αυθαίρετη τυχαία μεταβλητή. Τότε,

$$\bar{\mathrm{H}}\infty(W_i \mid B) \ge \bar{\mathrm{H}}\infty(W_0 \mid B) - \log Vol_t^M .$$

Απόδειξη: Έστω x=W_i και B=b. Όταν $d(W_0, W_i) \le t$, ισχύει ότι

$\Pr[W_i = x \mid B = b] \le \sum_{x' \mid d(x,x') \le t} \Pr[W_0 = x' \mid B = b] \le Vol_t^M \cdot 2^{-H\infty(W_0 \mid B=b)}$, το οποίο σημαίνει $H\infty(W_i = x \mid B = b) \ge H\infty(W_0 \mid B = b) - \log Vol_t^M$.Δεδομένου ότι η ανισότητα ισχύει για κάθε b, ακολουθεί το παρακάτω λήμμα.

Λήμμα 2: Έστω W_0, W_i είναι τυχαίες μεταβλητές που λαμβάνουν τιμές σε ένα χώρο M και ικανοποιούν τη σχέση $d(W_0, W_i) \le t$ και έστω B μια αυθαίρετη τυχαία μεταβλητή. Έστω επίσης ένα secure sketch (SS, Rec). Τότε:

$$\bar{H}\infty(W_i \mid SS(W_0), B) \ge \bar{H}\infty(W_0 \mid SS(W_0), B) .$$

Απόδειξη: 'Όταν $d(W_0, W_i) \le t$ ισχύει ότι $\mathrm{Re}\,c(W_i, SS(W_0)) = W_0$, που σημαίνει ότι για οποιοδήποτε x,b,pub θα είναι :

$$\Pr[W_0 = \mathrm{Re}\,c(x, pub) \mid SS(W_0) = pub, B = b] \ge \Pr[W_i = x \mid SS(W_0) = pub, B = b].$$

Το παραπάνω λήμμα ισχύει και για έναν fuzzy extractor αν αντικαταστήσουμε το $SS(W_0)$ με το pub. (61)

8.2.2 Ισχυρά ασφαλή σκίτσα (Robust Secure Sketches)

Επαναλαμβάνουμε ότι ένα ασφαλές σκίτσο, παίρνοντας σαν είσοδο ένα πρότυπο βιομετρικό στοιχείο εξάγει μία δημόσια συμβολοσειρά P(pub), η οποία επιτρέπει την ανάκτηση του πρότυπου από μία προσέγγισή του και ένας ασαφής εξαγωγέας επιτρέπει την δημιουργία μίας σχεδόν ομοιόμορφης συμβολοσειράς, με τη βοήθεια της δημόσιας

P και της προσέγγισης του προτύπου. Θυμίζουμε επίσης ότι αυτή τη δημόσια συμβολοσειρά δε παρέχει αρκετές πληροφορίες για το πρότυπο δεδομένο, ώστε να είναι αδύνατο μία κακόβουλη οντότητα να ανακτήσει το πρότυπο βιομετρικό. Με αυτό τον τρόπο διασφαλίζεται το απόρρητο της πληροφορίας. Ωστόσο, οφείλουμε να ελέγξουμε και την περίπτωση όπου αυτή η δημόσια πληροφορία μεταφέρεται μέσω ενός μη ασφαλούς καναλιού και έτσι δίνεται η δυνατότητα σε έναν εισβολέα να την τροποποιήσει. Για να αντιμετωπίσουμε τέτοιου είδους επίθεση ορίζουμε την έννοια των ισχυρών σκίτσων και ισχυρών ασαφών εξαγωγέων.

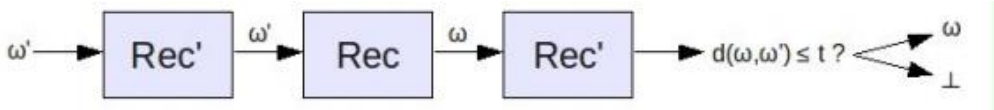
Καθορίζουμε πρώτα την περίπτωση όπου το πρότυπο βιομετρικό δεδομένο και το αντίστοιχο προσεγγιστικό του δεν είναι αρκετά όμοια μεταξύ τους, δηλαδή όταν $d(w, w') > t$, καθώς δεν υπάρχει κάποια εγγύηση για την έξοδο των αλγορίθμων Rec και Rep σε αυτήν την περίπτωση. Η λύση για αυτή την περίπτωση είναι ένα καλά διαμορφωμένο σκίτσο.

Ορισμός 1: Ένα (m, m΄, t) - ασφαλές σκίτσο (SS, Rec) λέγεται ότι είναι καλά διαμορφωμένο/σχηματισμένο εάν ικανοποιεί τις ακόλουθες τροποποιήσεις:

(i) Ο αλγόριθμος Rec μπορεί τώρα να επιστρέψει είτε ένα στοιχείο στο χώρο M, όταν η δημόσια συμβολοσειρά είναι και η αναμενόμενη, άρα επιτυγχάνεται και η πρόσβαση στο σύστημα, ή το διακριτό σύμβολο $\perp$ που δεν ανήκει στον M, και σημαίνει την παύση της διαδικασίας όταν η δημόσια συμβολοσειρά έχει τροποποιηθεί και

(ii) για όλα τα $w' \in M$ και αυθαίρετα P΄, εάν $\text{Rec}(w', P') \neq \perp$ τότε $d(w', \text{Rec}(w', P)) \leq t.'$

Είναι απλό να μετατραπεί οποιοδήποτε ασφαλές σκίτσο (SS, Rec) σε ένα καλά σχηματισμένο ασφαλές σκίτσο (SS, Rec΄).Ο αλγόριθμος Rec΄ εκτελεί τον Rec και στη συνέχεια βεβαιώνει ότι η έξοδος του πρότυπου βιομετρικού w βρίσκεται σε απόσταση t από την είσοδο του προσεγγιστικού w΄. Εάν βρίσκεται στη σωστή απόσταση τότε εξάγεται το πρότυπο βιομετρικό w, διαφορετικά, εξάγεται $\perp$, και η διαδικασία σταματά.



Εικόνα 22: *(63)*(Καλά διαμορφωμένο σκίτσο) *(63)*

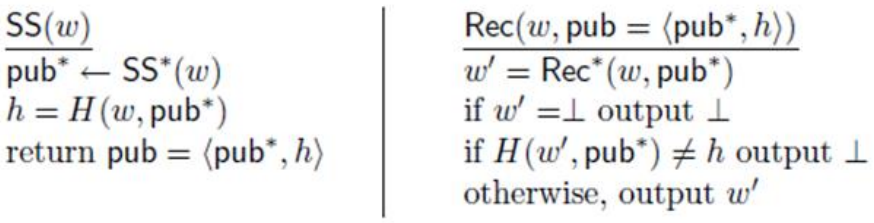
Στην περίπτωση όμως που η δημόσια συμβολοσειρά αποστέλλεται μέσω ενός μη ασφαλούς δικτύου, δίνοντας έτσι τη δυνατότητα σε έναν αντίπαλο να την τροποποιήσει κατά τη μεταφορά της, η λύση είναι ένα ισχυρό ασφαλές σκίτσο. Ένα ισχυρό ασφαλές σκίτσο δίνει πολύ μεγάλη πιθανότητα στο χρήστη να είναι σε θέση να εντοπίσει μία τροποποίηση της δημόσιας συμβολοσειράς και στη συνέχεια να σταματήσει τη διαδικασία.

Ορισμός 2 (Ισχυρό ασφαλές σκίτσο/Robust secure sketch): Δεδομένων των αλγορίθμων (SS, Rec) και τυχαίων μεταβλητών $W = \{W_0, W_1,\ldots, W_n\}$ στον μετρικό χώρο (M, d), έστω το ακόλουθο σενάριο μεταξύ ενός αντιπάλου A και ενός χρήστη:

- Ο χρήστης υπολογίζει τη δημόσια συμβολοσειρά P μέσω του αλγορίθμου SS με είσοδο το βιομετρικό του δεδομένο w_0,
- και στέλνει την P στον αντίπαλο A.
- Στη συνέχεια, ο αντίπαλος A, δοκιμάζει $(P_1 \ldots P_n)$ τα οποία είναι τροποποιήσεις του σωστού P, για κάθε βιομετρικό στοιχείο.
- Αν καταφέρει μια δημόσια συμβολοσειρά που έχει τροποποιηθεί να γίνει δεκτή, τότε ο αντίπαλος έχει αποκτήσει πλέον πρόσβαση στο σύστημα.

Χρησιμοποιώντας τον 1, ορίζουμε ότι οι (SS, Rec) είναι ένα (m,m΄΄,t,n,δ) – ισχυρό σκίτσο σε ένα μετρικό χώρο (M,d) αν είναι ένα καλά σχηματισμένο (m,m΄΄,t)- ασφαλές σκίτσο για όλα τα δείγματα με όριο t και $H\infty(W_0) \geq m$ και όλοι οι αντίπαλοι έχουν Pr[Succ]≤δ, όπου Succ συμβολίζουμε την επιτυχή επίθεση του αντιπάλου.

Σε γενικές γραμμές, ένα ισχυρό σκίτσο είναι μια ισχυρότερη έκδοση ενός καλά σχηματισμένου σκίτσου που διαμορφώνεται σύμφωνα με την ακόλουθη κατασκευή. Έστω $H:\{0,1\}^* \rightarrow \{0,1\}^k$ μία hash συνάρτηση. Κατασκευάζουμε ένα ισχυρό ασφαλές σκίτσο (SS,Rec) από ένα καλά σχηματισμένο σκίτσο (SS*,Rec*) ως εξής:



Εικόνα 23:Αλγόριθμοι κατασκευής ισχυρού σκίτσου *(61)*

- Από τον αλγόριθμο SS* με είσοδο το βιομετρικό δεδομένο w παίρνουμε ως έξοδο τη δημόσια συμβολοσειρά pub*.
- Έπειτα χρησιμοποιείται hash συνάρτηση πάνω στο βιομετρικό δεδομένο και στη συμβολοσειρά pub* δίνοντας μια τιμή h και με βάση τα δύο τελευταία έχουμε τη νέα δημόσια συμβολοσειρά pub. Η τιμή h επικυρώνει το ανακτημένο βιομετρικό δεδομένο.
- Από τον αλγόριθμο ανάκτησης Rec* με εισόδους τώρα το βιομετρικό δεδομένο και την αρχική συμβολοσειρά pub* θα ανακτήσουμε ένα άλλο βιομετρικό στοιχείο το οποίο θα πρέπει να είναι όμοιο με το αρχικό, διαφορετικά απορρίπτεται.
- Επίσης, ακόμα και στην περίπτωση που είναι όμοια, εφαρμόζεται η hash συνάρτηση και αν το αποτέλεσμα είναι η σωστή τιμή h, τότε η διαδικασία είναι επιτυχής, διαφορετικά σταματά.

Αυτό δεν έχει καμία ιδιαίτερη επίδραση καθώς όταν η τιμή h είναι διαφορετική από τη σωστή, τότε η κακόβουλη οντότητα γνωρίζει ούτως ή άλλως ότι η τιμή του w΄ διαφέρει από την πραγματική w. Η τροποποίηση αυτή έχει μικρή αλλά θετική επίδραση στην πιθανότητα επιτυχίας του κακόβουλου χρήστη καθώς ακόμα και στην περίπτωση που η τιμή h είναι σωστή, δεν αποτελεί και οριστική εγγύηση ότι τα δύο βιομετρικά στοιχεία είναι όμοια.

Θεώρημα: Αν το ζεύγος (SS*, Rec*) είναι ένα καλά σχηματισμένο (m, m΄, t)- ασφαλές σκίτσο σε έναν μετρικό χώρο (M, d) και μία hash συνάρτηση $H:\{0,1\}^{*}\to\{0,1\}^{k}$, τότε το ζεύγος των αλγορίθμων (SS, Rec) είναι ένα
(m, m΄, t, n, δ)-ισχυρό σκίτσο σε έναν μετρικό χώρο (M,d) για οποιονδήποτε αντίπαλο που θέτει q_H αιτήματα στην H, όπου:

$\delta=(q_{\mathrm{H}}{}^{2}+n)2^{-k}+(3q_{\mathrm{H}}+2nVol_{t}^{M}2^{-m'}$ και $m''=m'-\log(3q_{\mathrm{H}}+2)$.

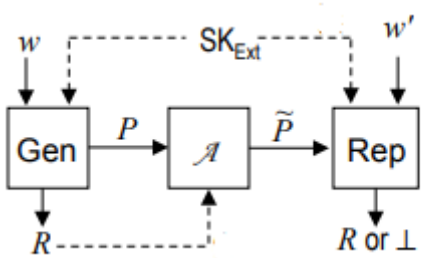
Όταν $k \geq m' + \log(q_H + 2)$, σύμφωνα με τα παραπάνω έχουμε $\delta \leq (4q_H + 2nVol_t^M)2^{-m'}$. (61)

8.2.3 Ισχυροί ασαφείς εξαγωγείς (Robust Fuzzy Extractors)

Οι ασαφείς εξαγωγείς προστατεύουν από μία επίθεση στην οποία μια κακόβουλη οντότητα γνωρίζει την τιμή της δημόσιας συμβολοσειράς και προσπαθεί να αντλήσει περισσότερες πληροφορίες για το εξαγόμενο κλειδί . Ωστόσο, ο ορισμός του ασαφή εξαγωγέα δεν εγγυάται τίποτα για το αν ο αντίπαλος μπορεί να τροποποιήσει τη δημόσια πληροφορία καθώς αποστέλλεται στον χρήστη. Δηλαδή, δεν υπάρχει κάποια εγγύηση για την έξοδο του αλγορίθμου Rep, όπου σαν είσοδο έχουμε το προσεγγιστικό βιομετρικό στοιχείο και τη δημόσια συμβολοσειρά , όταν η τιμή αυτής είναι διαφορετική από την πραγματική.

Προτείνεται λοιπόν η έννοια των ισχυρών ασαφών εξαγωγέων, που είναι ασφαλή σε αυτή την επίθεση. Πιο συγκεκριμένα, ο αλγόριθμος Rep έχει πλέον τη δυνατότητα να εξάγει και μία συμβολική τιμή αποτυχίας. Επομένως, όταν ένας αντίπαλος τροποποιήσει τη δημόσια συμβολοσειρά, τότε με πολύ μεγάλη πιθανότητα η έξοδος θα δώσει αυτή τη συμβολική τιμή.

Ορισμός 3 (Ισχυρός ασαφής εξαγωγέας/Robust fuzzy extractor): Δεδομένων των αλγορίθμων (Ext, Rec) και τυχαίων μεταβλητών W = {W_0, W_1,…, W_n } στον μετρικό χώρο (M, d), έστω το ακόλουθο σενάριο μεταξύ ενός server και ενός χρήστη:



Εικόνα 24:Robust Fuzzy Extractor (Ισχυρός ασαφής εξαγωγέας) *(64)*

- Ο χρήστης μέσω του αλγορίθμου Ext (που παρουσιάζεται αναλυτικά στο εδάφιο 7.8) και με είσοδο τα βιομετρικά του δεδομένα, εξάγει την ομοιόμορφη συμβολοσειρά R(κλειδί) και τη δημόσια συμβολοσειρά P(pub).
- Στέλνει το ζεύγος (R,pub) στον αντίπαλο A.

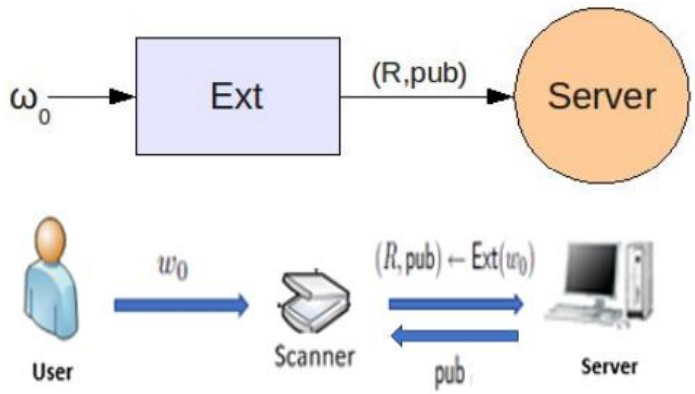
- Στη συνέχεια, ο αντίπαλος Α, τροποποιεί τη δημόσια πληροφορία, εξάγοντας (pub_1… pub_n) με $pub_i \neq pub$ για όλα τα βιομετρικά δεδομένα. Αν μία τροποποιημένη συμβολοσειρά δεν απορριφθεί, τότε ο αντίπαλος επιτυγχάνει την πρόσβαση στο σύστημα.

  Ορίζουμε, λοιπόν, ότι το ζεύγος των αλγορίθμων (Ext, Rec) είναι ένας (m,l,t,e, n,δ) –ισχυρός ασαφής εξαγωγέας σε ένα μετρικό χώρο (M,d) αν είναι ένα καλά σχηματισμένο (m,m΄΄,t)- ασφαλές σκίτσο για όλα τα δείγματα με όριο t και $H_\infty(W_0) \geq m$ και όλοι οι αντίπαλοι έχουν $Pr[\text{Succ}] \leq \delta$, όπου Succ συμβολίζουμε την επιτυχή επίθεση του αντιπάλου. (61)

8.3 Εφαρμογή για αμοιβαίο έλεγχο ταυτότητας

Η εφαρμογή ενός ισχυρού ασαφούς εξαγωγέα για την επίτευξη αμοιβαίου ελέγχου ταυτότητας ή επαλήθευσης κλειδιών μέσω ενός μη ασφαλούς καναλιού είναι άμεση. Έστω στο σενάριό μας ότι ακολουθείται ένα πρωτόκολλο που επιτυγχάνει ανταλλαγή κλειδιών μέσω αμοιβαίου ελέγχου ταυτότητας, βασισμένο σε ομοιόμορφα κατανεμημένο κλειδί μήκους l, θα εφαρμόσουμε έναν (m, l, t, e, n, δ)-ισχυρό ασαφή εξαγωγέα για οποιοδήποτε βιομετρική είσοδο W_0 με $H_\infty(W_0) \geq m$.

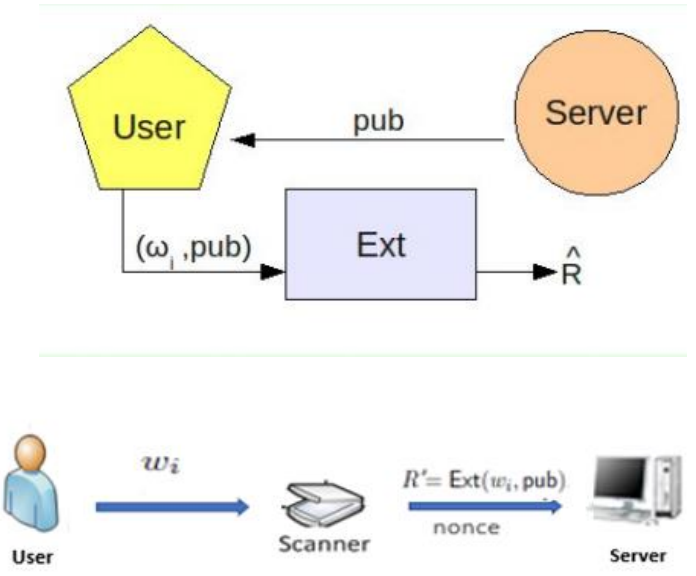
Δύο οντότητες, ένας χρήστης και ένας server, θέλουν να επικυρώσουν ο ένας τον άλλον και να συμφωνήσουν σε ένα κλειδί. Αρχικά, ο χρήστης σκανάρει τα βιομετρικά του δεδομένα (w_0) και μέσω του αλγορίθμου Ext (που παρουσιάζεται αναλυτικά στο εδάφιο 7.8) θα εξάγει την ομοιόμορφη R και τη δημόσια συμβολοσειρά pub (P).Στη συνέχεια, ο χρήστης καταχωρεί το ζεύγος (R,pub) στον server όπου και αποθηκεύονται. Το βήμα αυτό φαίνεται από τις παρακάτω εικόνες.



Εικόνα 25:Βήμα 1ο – Αρχικοποίηση *(63)*

Την επόμενη φορά που ο χρήστης χρειάζεται να αποκτήσει πρόσβαση, θα σκανάρει ξανά τα βιομετρικά δεδομένα του w_i, τα οποία αποτελούν προσέγγιση των πρότυπων. Ο server θα στείλει την pub και το nonce (τυχαίος αριθμός που χρησιμοποιείται μόνο μία φορά σε μια κρυπτογραφική επικοινωνία) στον χρήστη.

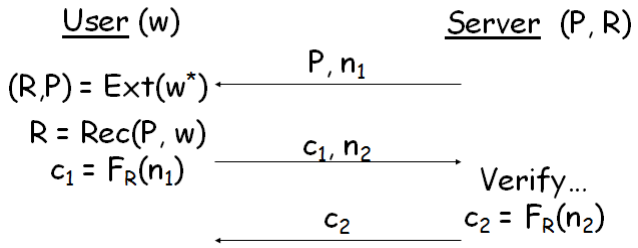
Μέσω του αλγορίθμου Ext που παίρνει ως είσοδο τη δημόσια συμβολοσειρά pub και το προσεγγιστικό βιομετρικό δεδομένο w_i,ο χρήστης θα εξάγει το κλειδί R΄ και θα το στείλει στον server μαζί με το nonce .



Εικόνα 26: Βήμα 2ο- Αυθεντικοποίηση του χρήστη *(63)*

Η διαδικασία συνεχίζεται με τον χρήστη να χρησιμοποιεί το κλειδί R' και ο server το R. Δηλαδή, αν στον χρήστη σταλθεί η σωστή δημόσια συμβολοσειρά pub από τον server και το πρότυπο βιομετρικό στοιχείο με το προσεγγιστικό που θα προκύψει από τη μετέπειτα σάρωση είναι αρκετά όμοια μεταξύ τους, τότε ο χρήστης θα έχει τη

δυνατότητα να εξάγει το σωστό $R' = R$, ώστε και οι δύο να καταλήξουν να χρησιμοποιούν το ίδιο κλειδί. Αν η ομοιόμορφη συμβολοσειρά απορριφθεί, η διαδικασία σταματά.



Εικόνα 27: Αυθεντικοποίηση

Η ασφάλεια του παραπάνω πρωτοκόλλου ενάντια σε έναν κακόβουλο χρήστη που παρακολουθεί όλα τα μηνύματα που ανταλλάσσονται μεταξύ ενός χρήστη και server, αποδεικνύεται από τις παρακάτω παρατηρήσεις:

- Όταν μία κακόβουλη οντότητα, για να αποκτήσει πρόσβαση στο σύστημα, στέλνει στον server μία τροποποιημένη δημόσια πληροφορία ,η διαδικασία του ελέγχου ταυτότητας θα τον απορρίψει, εκτός από μία πιθανότητα το πολύ δ. Έτσι, εκτός από αυτήν την πιθανότητα, ο αντίπαλος περιορίζεται στην προώθηση της σωστής τιμής της δημόσιας συμβολοσειράς.
- Η ασφάλεια δε στηρίζεται στη γνώση της ομοιόμορφης συμβολοσειράς R καθώς η R παραμένει ομοιόμορφα τυχαία παρά τη γνώση της P και αναπαράγεται επιτυχώς μόνο αν τα βιομετρικά στοιχεία είναι αρκετά όμοια μεταξύ τους. Ακόμα και σε αυτήν την περίπτωση χρήσης σωστής P, η κακόβουλη οντότητα δεν επιτυγχάνει να επιτεθεί.

Αν είναι ε_{Π}, η μέγιστη πιθανότητα επιτυχίας ενός κακόβουλου χρήστη, τότε, χρησιμοποιώντας έναν ισχυρό εξαγωγέα, η πιθανότητα επιτυχίας του θα γίνει $\varepsilon+\varepsilon_{\Pi}+\delta$. (61)

8.3.1 Βελτιωμένη λύση για τον αμοιβαίο έλεγχο ταυτότητας

Τα ισχυρά σκίτσα και οι ασαφείς εξαγωγείς παρέχουν έναν γενικό μηχανισμό για την αντιμετώπιση των επιθέσεων της τροποποίησης της δημόσιας πληροφορίας. Ωστόσο, παραμένει σημαντικό να διερευνήσουμε τρόπους που θα μπορούσαν να βελτιώσουν περισσότερο τη λύση αυτή. Η λύση που περιγράφεται παρακάτω έχει τα πλεονεκτήματα ότι είναι ασφαλής στο πρότυπο μοντέλο και μπορεί να επιτύχει βελτιωμένα όρια ως προς την απώλεια εντροπίας.

Έστω, λοιπόν, $W = \{W_0, W_1,\ldots, W_n\}$ μια ακολουθία τυχαίων μεταβλητών όπου το W_0 αντιπροσωπεύει την αρχική καταγεγραμμένη τιμή των βιομετρικών δεδομένων του χρήστη και το W_i υποδηλώνει την i –οστή τιμή για αυτή την i-φορά σάρωσή τους, δηλαδή τις προσεγγιστικές τιμές των αντίστοιχων βιομετρικών στοιχείων. Δεδομένου ενός καλά σχηματισμένου ασφαλή σκίτσου (SS*, Rec*) και μίας δημόσιας πληροφορίας τροποποιημένη από τον αντίπαλο, pub_i*, τότε μέσω του αλγορίθμου Rec με είσοδο την τροποποιημένη δημόσια σειρά και ένα προσεγγιστικό βιομετρικό W_i εξάγεται το πρότυπο W_i' με ελάχιστη εντροπία σύμφωνα με το θεώρημα .

Η μέση ελάχιστη εντροπία για κάθε βιομετρικό W_i' είναι ‘’υψηλή’’ για κάθε τιμή δημόσιας συμβολοσειράς pub_i* και από τη στιγμή που ο αντίπαλος επιτυγχάνει μόνο όταν καταφέρει να εξάγει μία τιμή $h_i=H(W_i', pub_i*)$, όπου Η μία hash συνάρτηση, είναι ανίκανος να επιτύχει, με πιθανότητα μεγαλύτερη από $2^{-H\infty(W_i')}$, στην i-οστή προσπάθεια. Εκτός από μια μικρή πιθανότητα, η τιμή $h_i = H(W_0, pub*)$ δεν μειώνει πολύ την εντροπία του W_0.

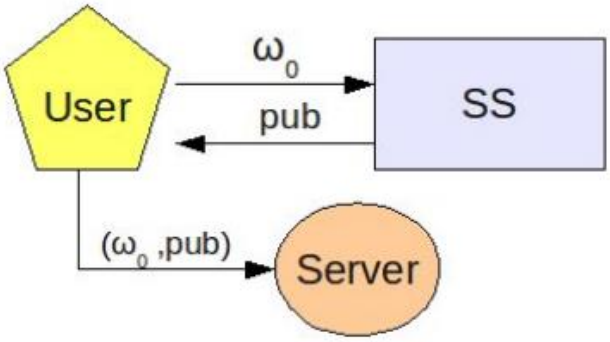
Για να αποφευχθεί και αυτή η μικρή πιθανότητα επιτυχίας, ο χρήστης μπορεί να χρησιμοποιήσει επίσης ένα ‘’τεστ ισότητας’’ (equality test) χρησιμοποιώντας την ανακτημένη τιμή του βιομετρικού W_i'για να ελέγχει αν η δημόσια πληροφορία έχει τροποποιηθεί. Έτσι, θα μειωθεί κατά πολύ η ικανότητα του αντιπάλου να μαντέψει την τιμή W_i'.

Θα πρέπει αυτό το τεστ να είναι ασφαλές για βιομετρικά δεδομένα που προέρχονται όχι μόνο από ομοιόμορφες κατανομές, αλλά και από τυχαίες. Επίσης θα πρέπει να διασφαλίζεται ότι κάθε προσπάθεια του αντιπάλου είναι μία εικασία μιας πιθανής τιμής του βιομετρικού W_i'. Τέλος, δεδομένου ότι προορίζεται να εκτελεστεί σε ένα μη ασφαλές δίκτυο, πρέπει να είναι «μη εύπλαστο» κατά κάποιο τρόπο, ώστε ο αντίπαλος να μην μπορεί να εκτελέσει man in the middle επίθεση .Ο αντίπαλος δεν θα πρέπει να

αποκτήσει πληροφορίες σχετικά με το πρότυπο βιομετρικό W_0 του χρήστη (τουλάχιστον με υπολογιστική έννοια) παρακολουθώντας τη διαδικασία. Ως το υποκείμενο τεστ ισότητας θα χρησιμοποιηθεί το πρωτόκολλο PAK(Password-Authenticated Key Exchange) (61).

8.3.2 Το πρωτόκολλο PAK (Password-Authenticated Key Exchange)

Ένα πρωτόκολλο ανταλλαγής κλειδιών με έλεγχο ταυτότητας με κωδικό πρόσβασης (PAKE) επιτρέπει σε δύο χρήστες που μοιράζονται μόνο έναν κωδικό πρόσβασης να δημιουργήσουν ένα κοινόχρηστο μυστικό κλειδί υψηλής εντροπίας, ανταλλάσσοντας μηνύματα μέσω ενός μη ασφαλούς δικτύου. Τα πρωτόκολλα PAKE έχουν ελάχιστες απαιτήσεις για τα μακροπρόθεσμα μυστικά που πρέπει να κατέχουν οι χρήστες και επομένως είναι ενδιαφέροντα τόσο θεωρητικά όσο και στην πράξη. Ένα από τα πρωτόκολλα PAKE του οποίου η ασφάλεια έχει μελετηθεί στο αποδεκτό πλαίσιο ασφαλείας είναι το πρωτόκολλο PAK (59), (65), (66). Πρόκειται για ένα πρωτόκολλο PAKE με αρκετά επιθυμητά χαρακτηριστικά: χαμηλό κόστος υπολογισμού και επικοινωνίας και αποδείξεις ασφαλείας σε δύο διαφορετικά μοντέλα ασφάλειας: το μοντέλο με βάση την προσομοίωση των Boyko, MacKenzie και Patel (59) και το λεγόμενο Find-then-Guess (FtG) μοντέλο Bellare, Pointcheval και Rogaway (67).
Έστω ένα πρωτόκολλο PAK(Password-Authenticated Key Exchange) και ένα καλά σχηματισμένο ασφαλές σκίτσο (SS, Rec). Θα κατασκευάσουμε ένα τροποποιημένο πρωτόκολλο PAK. Έστω δύο οντότητες, ένας χρήστης και ένας server θέλουν να επικοινωνήσουν μεταξύ τους και θέλουν να συμφωνήσουν σε έναν κοινό κωδικό. Ακολουθείται η παρακάτω διαδικασία (61):



Εικόνα 28: Υπολογισμός δημόσιας συμβολοσειράς από το βιομετρικό δεδομένο και καταχώρηση στον server *(63)*

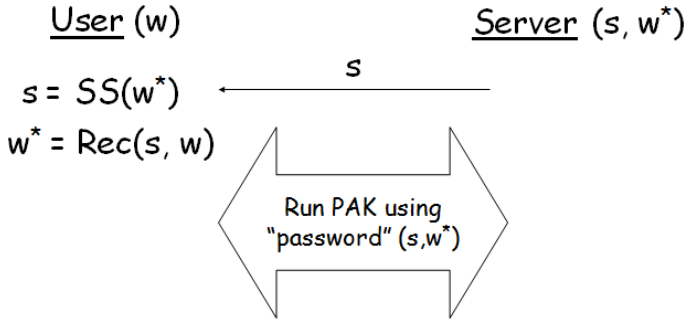
Αρχικά, ο χρήστης σκανάρει τα βιομετρικά δεδομένα του (w_0) και υπολογίζει τη δημόσια συμβολοσειρά (pub), μέσω του αλγορίθμου SS με είσοδο το πρότυπο βιομετρικό στοιχείο. Το πρότυπο βιομετρικό δεδομένο και η δημόσια συμβολοσειρά καταχωρούνται και αποθηκεύονται στον server.

Server:

- Στέλνει τη δημόσια πληροφορία , pub, στον χρήστη.
- Ορίζει τη δική του ταυτότητα και την ταυτότητα του χρήστη σύμφωνα με τη δημόσια συμβολοσειρά pub με κοινό κωδικό το πρότυπο βιομετρικό w_0.

Χρήστης:

- Την επόμενη φορά που ο χρήστης θα σκανάρει τα βιομετρικά δεδομένα του, δημιουργείται μία προσέγγιση των πρότυπων w^*.Μέσω του αλγορίθμου SS με είσοδο το προσεγγιστικό δεδομένο εξάγει τη δημόσια συμβολοσειρά pub^*.
- Μέσω του αλγορίθμου Rec, με είσοδο αυτή τη δημόσια σειρά και το προσεγγιστικό βιομετρικό θα εξάγει το βιομετρικό δεδομένο w΄.
- Η διαδικασία συνεχίζεται και ο χρήστης δημιουργεί τη δική του ταυτότητα και του server , σύμφωνα με το pub^*, χρησιμοποιώντας τον κωδικό w΄. Αν αυτό το βιομετρικό που εξάγεται δεν είναι αρκετά όμοιο με το πρότυπο, τότε ο χρήστης απορρίπτεται.



Εικόνα 29:Πρωτόκολλο PAK

Είναι εύκολο να δούμε ότι ισχύει η ορθότητα, καθώς εάν ο χρήστης και ο διακομιστής αλληλοεπιδρούν χωρίς καμία παρέμβαση από κάποιον αντίπαλο τότε:

(i) η ταυτότητα που χρησιμοποιεί ο server είναι ίδια με του χρήστη,

(ii) η ταυτότητα του χρήστη είναι ίδια με του server και

(iii) οι κωδικοί πρόσβασης w_0 και w΄ είναι ίδιοι.

Εδώ θα πρέπει να εισάγουμε συγκεκριμένους περιορισμούς ώστε η παραμόρφωση που θα προκληθεί να είναι φραγμένη στο t καθώς για τα τυχαία δείγματα θα πρέπει να εισαχθούν με συγκεκριμένη πιθανότητα που θα έχει υπολογιστεί.

Ορισμός: Έστω (M,d) ένας μετρικός χώρος. Μια υπολογίσιμη πιθανοτική κατανομή δειγμάτων που φράσσεται από την μεταβλητή t είναι μια ακολουθία από Boolean κύκλους $W = \{W_0, ...\}$ και μία παράμετρο l, τέτοια ώστε για κάθε i, ο κύκλος W_i υπολογίζει μία συνάρτηση από το $\{0,1\}^l$ στο M, και επιπλέον για κάθε $r \in \{0,1\}^l$ έχουμε $d(W_0(r), W_i(r)) \leq t$.

Στην εφαρμογή μας, το W μπορεί να εξάγεται από ένα πιθανοτικό πολυώνυμο ενός κακόβουλου χρήστη, διασφαλίζοντας τόσο ότι το σύνολο περιέχει μόνο έναν πολυωνυμικό αριθμό κυκλωμάτων και ότι κάθε τέτοιο κύκλωμα έχει πολυώνυμο μέγεθος (ώστε να είναι δυνατό να αξιολογηθεί αποτελεσματικά).

Θεώρημα: Έστω Π, ένα ασφαλές πρωτόκολλο ανταλλαγής κωδικών (σύμφωνα με τον παραπάνω ορισμό) και έστω A, ένα πιθανοτικό πολυώνυμο σε ρόλο κακόβουλου χρήστη A. Αν (SS, Rec) είναι ένα καλά σχηματισμένο (m, m΄,t) -ασφαλές σκίτσο σε έναν μετρικό χώρο (M,d), και $W = \{W_0, ...\}$ είναι μια υπολογίσιμη κατανομή δειγμάτων που φράσσεται από την μεταβλητή t (βλέπε ορισμό) με $H_\infty(W_0) \geq m$, τότε η πιθανότητα επιτυχίας ενός αντιπάλου να επιτεθεί στο πρωτόκολλο Π' είναι το πολύ $q_s 2^{-m''} + negl(k)$, όπου q_s είναι το πλήθος των προσπαθειών του αντιπάλου να υποδυθεί έναν εξουσιοδοτημένο χρήστη και $m'' = m' - \log Vol_t^M$.

Κάθε on-line επίθεση από τον αντίπαλο αντιπροσωπεύει μία μόνο «εικασία» του πραγματικού κωδικού πρόσβασης. Αυτό είναι το καλύτερο που μπορεί να κάνει ένας αντίπαλος. Ακόμα κι αν ο αντίπαλος αλλάξει την τιμή s, δηλαδή τη δημόσια πληροφορία, η τιμή που ανακτήθηκε από τον χρήστη εξακολουθεί να έχει «αρκετά υψηλή» ελάχιστη εντροπία. Με την ασφάλεια του πρωτοκόλλου PAK, η ικανότητα του αντιπάλου να μαντέψει το πρότυπο βιομετρικό w μειώθηκε. Τέλος, μπορεί να χρησιμοποιηθεί απλά ένα ασφαλές σκίτσο και όχι ένας ασαφής εξαγωγέας καθώς το πρωτόκολλο PAK δεν χρειάζεται ομοιόμορφα ''μυστικά''. Αυτή η προσέγγιση

λειτουργεί ακόμη και όταν η υπολειμματική ελάχιστη εντροπία είναι μικρή. Μπορεί ενδεχομένως να εφαρμοστεί ακόμη και σε λανθασμένα πληκτρολογημένους κωδικούς πρόσβασης.

8.3.3 Σύγκριση των δύο τεχνικών

Είναι δύσκολο να συγκρίνουμε την ασφάλεια που προσφέρουν οι δύο τεχνικές μας, καθώς η ακριβής σύγκριση εξαρτάται από μια σειρά υποθέσεων. Το κύριο πλεονέκτημα της τεχνικής του αμοιβαίου ελέγχου ταυτότητας με χρήση του πρωτοκόλλου PAK είναι ότι η κρυπτανάλυση δεν βασίζεται σε τυχαία στιγμιότυπα και η ασφάλεια στηρίζεται στην πρόβλεψη της τυχαίας πιθανότητας (random oracle). Από την άλλη πλευρά, η λύση που βασίζεται σε ισχυρούς ασαφείς εξαγωγείς είναι απλούστερη και πιο αποτελεσματική.

Η λύση του πρωτοκόλλου PAK δεν απαιτεί εξαγωγή τυχαιότητας και επομένως εξοικονομεί $2\log\delta^{-1}$ bits εντροπίας σε σύγκριση με λύσεις που εφαρμόζουν εξαγωγείς τυχαιότητας στα ανακτημένα βιομετρικά δεδομένα. Για παράδειγμα, αν μια πιθανή τιμή στην πράξη είναι $\delta \leq 2^{-64}$, αυτό έχει ως αποτέλεσμα πιθανή εξοικονόμηση τουλάχιστον 128 bits εντροπίας.

Όταν η εντροπία των αρχικών βιομετρικών δεδομένων είναι υψηλή και οι δύο προσεγγίσεις να συνδυαστούν και να χρησιμοποιηθεί ένα πρωτόκολλο PAK (Password-Authenticated Key Exchange) με οποιοδήποτε ισχυρό σκίτσο. Εάν γίνει αυτό, δεν απαιτείται πρόσθετη εξαγωγή, και έτσι αποφεύγουμε και πάλι την απώλεια $2\log\delta^{-1}$ bits εντροπίας.

Ωστόσο, η λύση του αμοιβαίου ελέγχου ταυτότητας με το πρωτόκολλο PAK προσφέρει ένα σαφές πλεονέκτημα ακόμα και όταν η εντροπία των αρχικών βιομετρικών δεδομένων είναι χαμηλή. Αν και σε αυτήν την περίπτωση ο αντίπαλος μπορεί να επιτεθεί με μία εξαντλητική επίθεση λεξικού (dictionary attack), αυτό είναι το καλύτερο που μπορεί να κάνει. Αντίθετα, η λύση που βασίζεται σε ισχυρά σκίτσα δεν θα ήταν κατάλληλη σε αυτήν την περίπτωση, καθώς ο αντίπαλος θα μπορούσε να προσδιορίσει τα μυστικά βιομετρικά δεδομένα του χρήστη με αναζήτηση των βιομετρικών στοιχείων με ασύγχρονο τρόπο στην βάση που έχουν αποθηκευτεί. (61)

Αμοιβαίος έλεγχος ταυτότητας με ισχυρούς ασαφείς εξαγωγείς	**Αμοιβαίος έλεγχος ταυτότητας με χρήση του πρωτοκόλλου PAK**
Απλός και αποτελεσματικός	Περισσότερο πολύπλοκος
Καθολική χρήση	Εξειδικευμένη χρήση (αυθεντικοποίηση/ανταλλαγή κλειδιών)
Προστασία ιδιωτικότητας (ο server δε γνωρίζει τα βιομετρικά δεδομένα του χρήστη)	Μη προστασία ιδιωτικότητας
Βασίζεται σε τυχαία στιγμιότυπα (Random Oracle)	Δε βασίζεται σε τυχαία στιγμιότυπα
Ακολουθεί το θεώρημα της εντροπίας για τυχαία στιγμιότυπα	Καλύτερη εντροπία με βάση το θεώρημα

Πίνακας 2: Σύγκριση των δύο τεχνικών

Κεφάλαιο 9. Επίλογος

Στην ενότητα αυτή συνοψίζουμε τη συνεισφορά και τα αποτελέσματα της εργασίας και παραθέτουμε σκέψεις για μελλοντικές επεκτάσεις της.

9.1 Σύνοψη

Η εξέλιξη της τεχνολογίας σε συνδυασμό με την διασφάλιση του απορρήτου αυτών των πληροφοριών, μας οδήγησε στο να διερευνήσουμε τρόπους πιστοποίησης περισσότερο αδιάβλητους. Αναζητήσαμε λοιπόν χαρακτηριστικά τα οποία είναι μοναδικά, αμετάβλητα και των οποίων η χρήση θα βοηθήσει ως προς την ασφάλεια της πρόσβασης σε ένα σύστημα. Αυτά τα χαρακτηριστικά είναι τα βιομετρικά. Ωστόσο, τα βιομετρικά δεδομένα αν παραβιαστούν, δε μπορούν να αλλάξουν όπως οι κοινοί κωδικοί πρόσβασης . Γι' αυτό το λόγο χρειάστηκε να δημιουργηθούν τεχνολογίας προστασίας που κωδικοποιούν τα δεδομένα αυτά και δίνουν τη δυνατότητα ταύτισης χωρίς την ανάγκη επαναφοράς τους στην αρχική μορφή. Η παρούσα εργασία, λοιπόν, μελέτησε τους τρόπους διαχείρισης των βιομετρικών δεδομένων σε κρυπτογραφικές εφαρμογές, ώστε να παρέχουν τη μέγιστη ασφάλεια για την πρόσβαση σε ένα σύστημα. Χρειάστηκε πρώτα να μελετηθούν ζητήματα που θα μπορούσαν να αποτελέσουν εμπόδιο για την εύρυθμη λειτουργία ενός βιομετρικού συστήματος. Για το λόγο αυτό έγινε μία εισαγωγή στα βιομετρικά συστήματα όπου αναφέρονται τα βασικά στάδια, τι ρόλο υπηρετούν, τι είδους λάθη μπορούν να συμβούν και για ποιο λόγο συμβαίνουν. Πέρα από όλα αυτά τα ζητήματα που έπρεπε να ληφθούν υπόψιν παρουσιάστηκαν ακόμα διάφορες επιθέσεις που μπορούν να συμβούν σε ένα βιομετρικό σύστημα και στην συνέχεια, αναφέρθηκαν μοντέλα προστασίας από τις επιθέσεις αυτές. Έπειτα από τη μελέτη όλων των παραπάνω ζητημάτων, η εργασία εστίασε σε δύο τεχνολογίες προστασίας βιομετρικών δεδομένων, τα ασφαλή σκίτσα και τους ασαφείς εξαγωγείς ,οι οποίες συνδυάζουν το μετασχηματισμό των δεδομένων, τη μέτρηση εύρωστων αποστάσεων και την κρυπτογραφία των βιομετρικών δεδομένων με στόχο την αυθεντικοποίηση χωρίς την επαναφορά των δεδομένων στην αρχική τους μορφή. Ωστόσο, για να επιτύχουμε ακόμα μεγαλύτερη ασφάλεια μελετήθηκαν επεκτάσεις των

παραπάνω τεχνολογιών, τα ισχυρά ασφαλή σκίτσα και οι ισχυροί ασαφείς εξαγωγείς, καθώς και η ταυτόχρονη χρήση ενός πρωτοκόλλου ανταλλαγής κλειδιών.
Αρχικά στο κεφάλαιο 2 παρουσιάστηκε η γνωστική περιοχή της διπλωματικής αναλύοντας τις έννοιες της βιομετρίας, των βιομετρικών χαρακτηριστικών και συστημάτων και της αυθεντικοποιησης και ταυτοποίησης του χρήστη.

Στο κεφάλαιο 3 αναλυθήκαν οι προϋποθέσεις που πρέπει να χαρακτηρίζουν τα βιομετρικά δεδομένα και συστήματα για να μπορούν να αποτελέσουν κομμάτι της αυθεντικοποίησης του χρήστη π.χ. τα βιομετρικά δεδομένα πρέπει να πληρούν χαρακτηριστικά όπως η οικουμενικότητα, η σταθερότητα, η μοναδικότητα και η συλλεκτικότητα, ενώ στα βιομετρικά συστήματα θα πρέπει να λαμβάνονται υπόψη ζητήματα όπως η επίδοση, η αποδοχή και η αντοχή στην πλαστογράφηση.

Επιπλέον, αναλύθηκε η αναγκαιότητα επίλυσης δυο βασικών προβλημάτων ώστε τα βιομετρικά δεδομένα να μπορούν να χρησιμοποιηθούν παρέχοντας ασφαλείς εφαρμογές. Αρχικά αναλύθηκε η μη ομοιόμορφη κατανομή τους, καθώς δεν προσφέρονται αποδεδειγμένες εγγυήσεις ασφαλείας εάν χρησιμοποιούνται για παράδειγμα ως κλειδί, και δεύτερον, η μη ακριβής αναπαραγωγή τους, αφού δύο βιομετρικές σαρώσεις του ίδιου χαρακτηριστικού είναι σπάνια πανομοιότυπες.

Έπειτα, η διπλωματική εργασία επικεντρώθηκε στην αυθεντικοποίηση του χρήστη μέσω βιομετρικών τεχνικών. Στο κεφάλαιο 4 περιγράφονται αναλυτικά τα τρία στάδια της αυθεντικοποίησης. Η εγγραφή του χρήστη αποτελεί το πρώτο στάδιο, όπου το βιομετρικό δείγμα αποκτάται από μια βιομετρική συσκευή και παράγει μια ηλεκτρονική αναπαράσταση σημάτων πολλών διαστάσεων (π.χ. δακτυλικό αποτύπωμα). Τα προβλήματα που μελετήθηκαν στο πρώτο στάδιο αυθεντικοποίησης είναι οι εξωγενείς αιτίες όπως μία χαμηλής ποιότητας σάρωσης του βιομετρικού και οι εγγενείς αιτίες, όπως η αλλοίωση των χαρακτηριστικών με την πάροδο του χρόνου.

Μια βασική χρήση των βιομετρικών δεδομένων είναι η ψηφιακή τους αναπαράσταση και επεξεργασία μέσω της αυθεντικοποίησης. Η ψηφιακή αναπαράσταση των βιομετρικών δεδομένων αποτελεί το δεύτερο στάδιο της αυθεντικοποίησης όπου σκοπός είναι η αποθήκευση και όχι η διαφοροποίηση μεταξύ τους. Τα βιομετρικά δεδομένα δεν αποθηκεύονται με την αρχική τους μορφή αλλά με τη μορφή διανυσμάτων. Καλούμε αυτή τη μεταγενέστερη μορφή ως βιομετρικό πρότυπο. Τέλος, στο τρίτο στάδιο περιγράφηκε η σύγκριση μεταξύ των προτύπων. Στόχος είναι η

διαφοροποίηση του κάθε προτύπου και για να επιτευχθεί αυτό εφαρμόστηκε ένα είδος ομοιότητας ή απόστασης μεταξύ τους. Για το λόγο αυτό, υποθέσαμε ότι το αρχικό βιομετρικό στοιχείο προέρχεται από κάποιο μετρικό χώρο, και ότι μία προσέγγισή του θα απέχει το πολύ μία απόσταση t από το αρχικό σε αυτό το χώρο. Παρουσιάστηκαν συγκεκριμένες μετρικές, για τις αποστάσεις Hamming, Set Distance και Edit Distance. Το νέο πρότυπο που δημιουργείται έπειτα από την εφαρμογή της απόστασης είναι αυτό που τελικά συγκρίνεται για να προκύψει ταυτοποίηση.

Τα παραγόμενα βιομετρικά πρότυπα, που είναι απαραίτητα για την ψηφιακή επεξεργασία των βιομετρικών δεδομένων, αναλυθήκαν εκτενώς και επιπλέον παρουσιάστηκε η σύγκριση μεθοδολογιών για την παραγωγή αυτών των βιομετρικών προτύπων. Αναλυτικότερα, στο κεφάλαιο 5 μελετήθηκαν οι κατωφλιακοί παράγοντες ώστε οι μεθοδολογίες παραγωγής βιομετρικών προτύπων να εξάγουν πρότυπα τα οποία θα προσφέρονται για ασφαλή αυθεντικοποίηση.

Αρχικά, περιγράφηκαν οι μεθοδολογίες για την παραγωγή βιομετρικών προτύπων μέσω των βιομετρικών αλγόριθμων. Για την εξαγωγή του συνόλου σημαντικών και διακριτικών χαρακτηριστικών, που αντιπροσωπεύουν το υποκείμενο βιομετρικό χαρακτηριστικό (πρότυπο), παρουσιάστηκε αναλυτικά ο αλγόριθμος Mindtcp, ο οποίος δέχεται ως είσοδο μια εικόνα δακτυλικού αποτυπώματος και ανιχνεύει αυτόματα λεπτομερή στοιχεία στο δακτυλικό αποτύπωμα. Στη συνέχεια, χρειάστηκε να μελετηθεί ένας αλγόριθμος βιομετρικής αντιστοίχισης ώστε να συγκρίνει τα νέα δεδομένα που εισάγει ο χρήστης με τα αποθηκευμένα πρότυπα στη βάση δεδομένων, παράγοντας βαθμολογίες που αντιπροσωπεύουν την ομοιότητα μεταξύ της εισόδου και του προτύπου. Για τη σύγκριση, λοιπόν, μεταξύ των προτύπων παρουσιάστηκε αναλυτικά ο αλγόριθμος βιομετρικής αντιστοίχισης BOZORTH3.

Ωστόσο, ένα ακόμα πρόβλημα που μελετήθηκε είναι ότι ο αλγόριθμος αυτός θα πρέπει να αντιμετωπίζει κάποιες παραλλαγές που μπορεί να υπάρχουν στα βιομετρικά δεδομένα. Κάποιες από τις αιτίες που δημιουργούν τις παραλλαγές αυτές είναι η ενδοατομική και η διατομική μεταβλητότητα, η γεννετική ομοιότητα μεταξύ συγγενών, αλλοιώσεις, και προβληματικές σαρώσεις κατά το στάδιο της εγγραφής. Για να είναι λοιπόν, το σύστημά μας λειτουργικό αλλά και ασφαλές είναι κρίσιμη η επιλογή ενός κατωφλιακού παράγοντα, καθώς δε θα θέλαμε να πετύχουμε την πλήρη ταύτιση γιατί ο αλγόριθμος θα απέρριπτε ακόμα και τους εξουσιοδοτημένους χρήστες, ενώ

ταυτόχρονα δε θα θέλαμε να έχουμε και υψηλά επίπεδα ανοχής γιατί αυτό θα έκανε το σύστημά μας ευάλωτο στην εξαπάτηση από μη εξουσιοδοτημένους χρήστες. Για αυτό γίνεται και η χρήση των δεικτών FMR (false matching rate) και FNMR(false non-matching rate).

Στο 6^{ο} κεφάλαιο έγινε μια ολοκληρωμένη μελέτη του βιομετρικού συστήματος δακτυλικών αποτυπωμάτων και εξετάστηκαν οι ευπάθειες σε διάφορα επίπεδά του. Ενδεικτικά αναφέρονται οι περισσότερο πιθανές επιθέσεις σε διάφορα τρωτά σημεία των βιομετρικών συστημάτων:

Ως προς τον αισθητήρα	**Ως προς τον εξαγωγέα χαρακτηριστικων**	**Ως προς τον συγκριτή**	**Ως προς τα κανάλια επικοινωνίας**	**Ως προς τη βάση δεδομένων**
Spoofing/ mimicry attack	Παράκαμψη εξαγωγής χαρακτηριστικών	Τροποποίηση των δεικτών ομοιότητας	Eaves dropping attack (παθητική παρακολούθηση)	Αναδημιουργία προτύπου (Template reconstruction)
Επίθεση επιβολής βίας	Επίθεση Δούρειος ίππος (Trojan horse attack)	Επίθεση επανάληψης (Replay attack)	Man-in-the-middle attack	Μη εξουσιοδοτημένη τροποποίηση προτύπου (Unauthorized template modification)
Επίθεση επιβολής βίας		Αντικατάσταση υλικού hardware/software	Brute force attack (επίθεση ωμής βίας)	Παράκαμψη (Circumvention)
Denial of service attack (Άρνηση εξυπηρέτησης		Hill climbing attack (Επίθεση αναρρίχησης)	Replay attack (επίθεση επανάληψης)	

Πίνακας 3: Ο πίνακας αναφέρει πιθανές επιθέσεις σε διάφορα τρωτά σημεία των βιομετρικών συστημάτων:

Τέλος παρουσιάστηκαν τέσσερα μοντέλα απειλών για ένα βιομετρικό σύστημα δακτυλικών αποτυπωμάτων. Ένα μοντέλο απειλής είναι ένας τρόπος αναγνώρισης διαφόρων επιθέσεων (ή πιθανών απειλών) σε ένα σύστημα. Τα μοντέλα αυτά είναι τα ακόλουθα: 1)μοντέλο Ratha et al., 2) μοντέλο fishbone, 3) μοντέλο Nagar et al., 4)Bartlow and Cukic framework. Στον παρακάτω πίνακα παρουσιάζονται αυτά τα

μοντέλα, όπου συγκρίνονται με βάση τον αριθμό των πιθανών επιθέσεων που είναι ικανά να εντοπίσουν και τέλος αναφέρεται ποια είναι η καταλληλότερη εφαρμογή για το καθένα.

Μοντέλο απειλής	**Ταξινόμηση**	**Εφαρμογή**
Ratha et al.	8 ευάλωτα σημεία με αποτέλεσμα 8 τύπους επιθέσεων	Ένα γενικό μοντέλο χωρίς λεπτομέρειες για συγκεκριμένες επιθέσεις
Fishbone	5 αιτίες οδηγούν σε αποτυχία του βιομετρικού συστήματος	Χρήσιμο κατά το σχεδιασμό τεχνικών βιομετρικής ασφάλειας
Nagar et al.	Σημαντικές ευπάθειες και 4 υποκείμενες αιτίες τους	Καθορίζει τις ευπάθειες για σύστημα ελέγχου ταυτότητας με βιομετρικά δεδομένα
Bartlow and Cukic framework	3 επίπεδα με 20 πιθανά σημεία επίθεσης	Κατάλληλο για δοκιμές και επικύρωση τεχνικών ασφαλείας

Πίνακας 4: Πίνακας σύγκρισης των μοντέλων απειλών

Στο κεφάλαιο 7, για την ανάγκη της προστασίας του απορρήτου των βιομετρικών δεδομένων μελετήθηκαν δύο κρυπτογραφικά σχήματα, τα ασφαλή σκίτσα και οι ασαφείς εξαγωγείς. Τα σχήματα αυτά δίνουν τη δυνατότητα να εξαχθεί ένα κλειδί υψηλής εντροπίας από θορυβώδη δεδομένα, όπως είναι τα βιομετρικά.

Παρουσιάστηκε αρχικά η έννοια της εντροπίας, που αφορά την τυχαιότητα των κλειδιών, παράγοντας που παίζει μεγάλο ρόλο στην ασφάλεια της κρυπτογραφίας, αφού αν ένα κλειδί δεν είναι πραγματικά τυχαίο λειτουργεί σαν ένας αδύναμος κοινός κωδικός πρόσβασης. Ακόμα, για να είναι δυνατή η εξαγωγή των βιομετρικών κλειδιών μελετήθηκε η χρήση κάποιων δημόσιων πληροφοριών ή αλλιώς βοηθητικών δεδομένων (helper data) μέσω των βιομετρικών κρυπτοσυστημάτων. Η εργασία επικεντρώθηκε σε δύο αντιφατικές απαιτήσεις που θα πρέπει να ικανοποιούν αυτές οι βιομετρικά εξαρτώμενες πληροφορίες. Πρώτον, θα πρέπει να περιέχουν επαρκείς πληροφορίες που να επιτρέπουν την αντιστοιχία μεταξύ ενός πρότυπου βιομετρικού στοιχείου που είναι ήδη αποθηκευμένο στο σύστημα με το αντίστοιχο στοιχείο που θα

καταχωρήσει ο χρήστης την επόμενη φορά που θα το σκανάρει ώστε να αποκτήσει πρόσβαση στο σύστημα, και δεύτερον, δεν πρέπει να διαρρεύσουν κρίσιμες πληροφορίες σχετικά με το πρότυπο.

Έπειτα από την ανάλυση της εντροπίας και των εξαγόμενων κλειδιών, το πρώτο κρυπτογραφικό σχήμα που παρουσιάστηκε είναι ο ασαφής εξαγωγέας (fuzzy extractor). Ένας ασαφής εξαγωγέας εξάγει μια ομοιόμορφα τυχαία σειρά R από την είσοδο ενός βιομετρικού w με ένα τρόπο ανθεκτικό στο θόρυβο, δηλαδή αν η είσοδος αλλάξει σε w′ αλλά παραμείνει σχετικά ίδια, η σειρά R μπορεί να αναπαραχθεί ακριβώς. Για να διευκολύνει την αναπαραγωγή του R, ο εξαγωγέας, όταν χρησιμοποιείται για πρώτη φορά, δίνει σαν έξοδο και μια δημόσια βοηθητική σειρά P, χωρίς να μειωθεί η ασφάλεια της R. Η R δεν είναι αποθηκευμένη, έτσι τα βιομετρικά δεδομένα του χρήστη ενεργούν στην πραγματικότητα ως κλειδί, και η εγγραφή μπορεί να αποθηκευτεί κρυπτογραφημένα σε μια μη κρυφή, ακόμα με τη σιγουριά ότι η εγγραφή θα αποκρυπτογραφείται μόνο όταν παρουσιάζονται σωστά βιομετρικά δεδομένα.

Ως ένα βήμα για την κατασκευή των εξαγωγέων ασάφειας, παρουσιάστηκε ένα άλλο θεμελιακό στοιχείο, που ονομάζεται ασφαλές σκίτσο (secure sketch). Αυτό επιτρέπει την ακριβή ανακατασκευή μιας θορυβώδους εισόδου ως εξής: για είσοδο ένα βιομετρικό δεδομένο w, μια διαδικασία δίνει ως έξοδο ένα σκίτσο s. Στη συνέχεια, δεδομένου του s και μιας τιμής w′ κοντά στο w, δηλαδή ενός προσεγγιστικού βιομετρικού που προέρχεται από μία μετέπειτα σάρωση, είναι δυνατόν να ανακτήσουμε το πρότυπο βιομετρικό w. Το σκίτσο είναι ασφαλές, υπό την έννοια ότι δεν αποκαλύπτει πολλά για το βιομετρικό w, καθώς το w διατηρεί μεγάλο μέρος της εντροπίας του ακόμη και αν το s είναι γνωστό. Έτσι, αντί να αποθηκεύσουμε το w, από φόβο ότι αργότερες αναγνώσεις θα είναι θορυβώδεις, είναι δυνατό να αποθηκεύσουμε το s στη θέση του, διατηρώντας μεγάλο μέρος του απορρήτου του βιομετρικού w.

Στο κεφάλαιο 8 παρουσιάστηκε ο απομακρυσμένος έλεγχος πρόσβασης και πιστοποίησης μέσω των ασφαλών σκίτσων και ασαφών εξαγωγέων. Τα σχήματα αυτά έχουν κατασκευαστεί έτσι ώστε να είναι ασφαλή όταν ένας αντίπαλος παρακολουθεί το κανάλι επικοινωνίας μεταξύ server και χρήστη. Ωστόσο, ήταν απαραίτητο να μελετηθεί κάποια μέθοδος που παρέχει ασφαλή έλεγχο ταυτότητας στην παρουσία

ενός ενεργού αντιπάλου ο οποίος είναι σε θέση να τροποποιήσει τα μηνύματα που αποστέλλονται μεταξύ του διακομιστή και του χρήστη. Πιο συγκεκριμένα, μελετήθηκε η περίπτωση της τροποποίησης της δημόσιας συμβολοσειράς.

Παρουσιάστηκαν ως πρώτες λύσεις κάποιες επεκτάσεις των τεχνικών των ασφαλών σκίτσων και ασαφών εξαγωγέων, τα ισχυρά ασφαλή σκίτσα και οι ισχυροί ασαφείς εξαγωγείς, ώστε να πραγματοποιείται με ασφάλεια ο απομακρυσμένος έλεγχος πρόσβασης για αυτή την περίπτωση, καθώς και μια δεύτερη τεχνική η οποία εστιάζει στον απομακρυσμένο έλεγχο ταυτότητας και στην ανταλλαγή κλειδιών μέσω του πρωτοκόλλου PAK (Password-Authenticated Key Exchange).

Εισάχθηκε αρχικά η έννοια ενός καλά σχηματισμένου ασφαλούς σκίτσου (SS, Rec΄), πάνω στην οποία βασίζεται το ισχυρό σκίτσο. Ο αλγόριθμος ανάκτησης Rec΄ εκτελεί τον Rec και στη συνέχεια βεβαιώνει ότι η έξοδος του πρότυπου βιομετρικού w βρίσκεται σε απόσταση t από την είσοδο του προσεγγιστικού w΄. Εάν βρίσκεται στη σωστή απόσταση τότε εξάγεται το πρότυπο βιομετρικό w, διαφορετικά η διαδικασία σταματά. Στην περίπτωση όμως, που η δημόσια συμβολοσειρά αποστέλλεται μέσω ενός μη ασφαλούς δικτύου, δίνοντας έτσι τη δυνατότητα σε έναν αντίπαλο να την τροποποιήσει κατά τη μεταφορά της, η λύση είναι ένα ισχυρό ασφαλές σκίτσο. Δίνει πολύ μεγάλη πιθανότητα στο χρήστη να είναι σε θέση να εντοπίσει μία τροποποίηση της δημόσιας συμβολοσειράς και στη συνέχεια να σταματήσει τη διαδικασία.

Ένα ισχυρό σκίτσο είναι μια ισχυρότερη έκδοση ενός καλά σχηματισμένου σκίτσου. Πλέον χρησιμοποιείται μία hash συνάρτηση πάνω στο βιομετρικό δεδομένο και στη συμβολοσειρά pub* δίνοντας μια τιμή h και με βάση τα δύο τελευταία έχουμε τη νέα δημόσια συμβολοσειρά pub. Η τιμή h επικυρώνει το ανακτημένο βιομετρικό δεδομένο. Από τον αλγόριθμο ανάκτησης Rec* με εισόδους τώρα το βιομετρικό δεδομένο και την αρχική συμβολοσειρά pub* θα ανακτήσουμε ένα άλλο βιομετρικό στοιχείο το οποίο θα πρέπει να είναι όμοιο με το αρχικό, διαφορετικά απορρίπτεται.
Αυτό δεν έχει καμία ιδιαίτερη επίδραση καθώς όταν η τιμή h είναι διαφορετική από τη σωστή, τότε η κακόβουλη οντότητα γνωρίζει ούτως ή άλλως ότι η τιμή του w΄ διαφέρει από την πραγματική w. Η τροποποίηση αυτή έχει μικρή αλλά θετική επίδραση στην πιθανότητα επιτυχίας του κακόβουλου χρήστη καθώς ακόμα και στην περίπτωση που η τιμή h είναι σωστή, δεν αποτελεί και οριστική εγγύηση ότι τα δύο βιομετρικά στοιχεία είναι όμοια.

Στη συνέχεια μελετήθηκε η περίπτωση χρήσης του ισχυρού ασαφούς εξαγωγέα. Ο αλγόριθμος Rep έχει πλέον τη δυνατότητα να εξάγει και μία συμβολική τιμή αποτυχίας. Επομένως, όταν ένας αντίπαλος τροποποιήσει τη δημόσια συμβολοσειρά, τότε με πολύ μεγάλη πιθανότητα η έξοδος θα δώσει αυτή τη συμβολική τιμή**.** Παρουσιάστηκε το σενάριο όπου ο χρήστης σκανάρει τα βιομετρικά του δεδομένα (w_0) και μέσω του αλγορίθμου Ext εξάγει την ομοιόμορφη R και τη δημόσια συμβολοσειρά pub (P).Στη συνέχεια, ο χρήστης καταχωρεί το ζεύγος (R,pub) στον server όπου και αποθηκεύονται. Την επόμενη φορά που ο χρήστης χρειάζεται να αποκτήσει πρόσβαση, θα σκανάρει ξανά τα βιομετρικά δεδομένα του w_i, τα οποία αποτελούν προσέγγιση των πρότυπων. Ο server θα στείλει την pub και το nonce στον χρήστη.

Στη συνέχεια, με τη δημόσια συμβολοσειρά pub και το προσεγγιστικό βιομετρικό δεδομένο w_i, μέσω του αλγορίθμου Ext, ο χρήστης θα εξάγει το κλειδί R΄ και θα το στείλει στον server μαζί με το nonce . Η διαδικασία συνεχίζεται με τον χρήστη να χρησιμοποιεί το κλειδί R' και ο server το R. Ωστόσο, για να καταλήξουν ο χρήστης και ο server στο ίδιο κλειδί $R' = R$, θα πρέπει να έχει σταλεί η σωστή δημόσια συμβολοσειρά και τα βιομετρικά στοιχεία είναι αρκετά όμοια μεταξύ τους.

Οπότε, με τις παραπάνω επεκτάσεις, καταλήξαμε στο ότι μία κακόβουλη οντότητα, για να αποκτήσει πρόσβαση στο σύστημα, στέλνοντας στον server μία τροποποιημένη δημόσια πληροφορία ,η διαδικασία του ελέγχου ταυτότητας θα τον απορρίψει, εκτός από μία πιθανότητα το πολύ δ. Έτσι, εκτός από αυτήν την πιθανότητα, ο αντίπαλος περιορίζεται στην προώθηση της σωστής τιμής της δημόσιας συμβολοσειράς. Επίσης, ακόμα και στην περίπτωση χρήσης σωστής P, η κακόβουλη οντότητα δεν επιτυγχάνει να επιτεθεί, καθώς η ασφάλεια δε στηρίζεται στη γνώση της ομοιόμορφης συμβολοσειράς R, μιας και η R παραμένει ομοιόμορφα τυχαία παρά τη γνώση της P , και αναπαράγεται επιτυχώς μόνο αν τα βιομετρικά στοιχεία είναι αρκετά όμοια μεταξύ τους.

Τα ισχυρά σκίτσα και οι ασαφείς εξαγωγείς παρέχουν έναν γενικό μηχανισμό για την αντιμετώπιση των επιθέσεων της τροποποίησης της δημόσιας πληροφορίας. Για να βελτιώσουμε τη γενική λύση παρουσιάστηκε ένα πρωτόκολλο ανταλλαγής κλειδιών με έλεγχο ταυτότητας με κωδικό πρόσβασης (PAKE) που επιτρέπει σε δύο χρήστες που μοιράζονται μόνο έναν κωδικό πρόσβασης να δημιουργήσουν ένα κοινόχρηστο μυστικό κλειδί υψηλής εντροπίας, ανταλλάσσοντας μηνύματα μέσω ενός μη ασφαλούς

δικτύου, έχοντας ελάχιστες απαιτήσεις για τα μακροπρόθεσμα μυστικά που πρέπει να κατέχουν.

Παρουσιάστηκε το παρακάτω σενάριο, όπου ο χρήστης, αρχικά, σκανάρει τα βιομετρικά δεδομένα του (w_0) και υπολογίζει τη δημόσια συμβολοσειρά (pub), μέσω του αλγορίθμου SS με είσοδο το πρότυπο βιομετρικό στοιχείο. Το πρότυπο βιομετρικό δεδομένο και η δημόσια συμβολοσειρά καταχωρούνται και αποθηκεύονται στον server.Στη συνέχεια, ο server στέλνει τη δημόσια πληροφορία στον χρήστη και ορίζει τη δική του ταυτότητα και την ταυτότητα του χρήστη σύμφωνα με τη δημόσια συμβολοσειρά pub με κοινό κωδικό το πρότυπο βιομετρικό w_0.Την επόμενη φορά που ο χρήστης θα σκανάρει τα βιομετρικά δεδομένα του, δημιουργείται μία προσέγγιση των πρότυπων w^*. Μέσω του αλγορίθμου SS με είσοδο το προσεγγιστικό δεδομένο εξάγει τη δημόσια συμβολοσειρά pub^*. Μέσω του αλγορίθμου Rec, με είσοδο αυτή τη δημόσια σειρά και το προσεγγιστικό βιομετρικό θα εξάγει το βιομετρικό δεδομένο w΄.Η διαδικασία συνεχίζεται και ο χρήστης δημιουργεί τη δική του ταυτότητα και του server , σύμφωνα με το pub^*, χρησιμοποιώντας τον κωδικό w΄. Αν αυτό το βιομετρικό που εξάγεται δεν είναι αρκετά όμοιο με το πρότυπο, τότε ο χρήστης απορρίπτεται.

Εάν ο χρήστης και ο διακομιστής αλληλοεπιδρούν χωρίς καμία παρέμβαση από κάποιον αντίπαλο τότε η ταυτότητα που χρησιμοποιεί ο server είναι ίδια με του χρήστη, η ταυτότητα του χρήστη είναι ίδια με του server και οι κωδικοί πρόσβασης w_0 και w΄ είναι ίδιοι. Το καλύτερο, λοιπόν, που καταλήγει να κάνει ένας αντίπαλος είναι μία εικασία του πραγματικού βιομετρικού. Ακόμα κι αν ο αντίπαλος αλλάξει την τιμή της δημόσιας πληροφορίας, η τιμή που ανακτήθηκε από τον χρήστη εξακολουθεί να έχει «αρκετά υψηλή» ελάχιστη εντροπία. Με την ασφάλεια του πρωτοκόλλου PAK, η ικανότητα του αντιπάλου να μαντέψει το πρότυπο βιομετρικό μειώθηκε.

Συγκρίνοντας τις δύο τεχνικές, συμπεράναμε ότι η χρήση του πρωτοκόλλου PAK, αν και περισσότερο πολύπλοκη δεν απαιτεί εξαγωγή τυχαιότητας όπως απαιτεί η τεχνική που εφαρμόστηκαν οι ισχυροί ασαφείς εξαγωγείς. Έτσι έχουμε και εξοικονόμηση $2\log\delta^{-1}$ bits εντροπίας. Συνεπώς, η τεχνική του αμοιβαίου ελέγχου ταυτότητας με χρήση του πρωτοκόλλου PAK, μπορεί να χρησιμοποιηθεί για βιομετρικά δεδομένα και με υψηλή αλλά και όχι εντροπία. Στην περίπτωση δεδομένων χαμηλής εντροπίας, το μόνο που μπορεί να κάνει ένας αντίπαλος για να επιτεθεί είναι μία εξαντλητική επίθεση λεξικού (dictionary attack). Η λύση που παρουσιάστηκε με τα ισχυρά ασφαλή σκίτσα, επίσης δεν είναι ασφαλής για δεδομένα με χαμηλή εντροπία καθώς ο αντίπαλος θα

μπορούσε να επιτεθεί με αναζήτηση των βιομετρικών στοιχείων με ασύγχρονο τρόπο στην βάση που έχουν αποθηκευτεί.

9.2 Συμπεράσματα

Από την ανάλυση και την μελέτη που έγινε, αναδείχθηκε ότι τα βιομετρικά εργαλεία όντως μπορούν να χρησιμοποιηθούν από την ασφάλεια υπολογιστικών συστημάτων, καθώς παρέχουν μοναδικά γνωρίσματα που μπορούν να χρησιμοποιηθούν για να καθορίσουν την ταυτότητα ενός χρήστη.

Παρόλα αυτά, η ψηφιακή τους αναπαράσταση και επεξεργασία ελλοχεύει κινδύνους και ευπάθειες, καθώς κανένα βιομετρικό στοιχείο δεν αναμένεται να πληροί όλες τις προϋποθέσεις που απαιτούνται από τα συστήματα ασφαλείας. Για το λόγο αυτό ήταν σημαντικό να περιγραφούν οι ιδιότητες που πρέπει να πληρούν τα βιομετρικά δεδομένα όπως η οικουμενικότητα, η μοναδικότητα, η σταθερότητα και να μελετηθούν οι βιομετρικοί αλγόριθμοι που θα επεξεργαστούν τα δεδομένα αυτά, καθώς περιλαμβάνουν διαδικασίες όπως η αξιολόγηση ποιότητας, η βελτιστοποίηση, και η εξαγωγή των χαρακτηριστικών.

Βασικός πυλώνας της χρήσης των βιομετρικών εργαλείων είναι η χρήση τους για αυθεντικοποίηση του χρήστη. Η αυθεντικοποίηση γίνεται μέσω ενός βιομετρικού συστήματος. Ουσιαστικά, είναι ένα σύστημα αναγνώρισης προτύπων που αποκτώντας βιομετρικά δεδομένα από ένα άτομο, στη συνέχεια εξάγει ένα σύνολο χαρακτηριστικών και τέλος το συγκρίνει με το εγγεγραμμένο πρότυπο που βρίσκεται στη βάση δεδομένων του συστήματος. Για αυτό το λόγο ήταν σημαντικό να μελετηθεί η αρχιτεκτονική των βιομετρικών συστημάτων και οι ευπάθειες που παρουσιάζουν και δίνουν τη δυνατότητα σε έναν κακόβουλο χρήστη να επιτεθεί στο σύστημα. Ερευνήθηκαν, λοιπόν, όλοι οι πιθανοί τρόποι επίθεσης στα διάφορα επίπεδα ενός βιομετρικού συστήματος και επιπλέον, ήταν απαραίτητο να μελετηθούν κάποια μοντέλα απειλών, δηλαδή τρόποι με τους οποίους θα μπορούσαν να αναγνωριστούν αυτές οι διάφορες επιθέσεις ή πιθανές απειλές σε ένα σύστημα. Η διερεύνηση όλων των πιθανών σημείων που μπορούν να καταστήσουν ένα σύστημα ευάλωτο σε επιθέσεις αποτελεί θεμέλιο για την κατασκευή ενός συστήματος ακόμα πιο ισχυρού ενάντια σε κακόβουλους χρήστες-διαχειριστές.

Ωστόσο, οι κρυπτογραφικές εφαρμογές βασίζεται παραδοσιακά σε ομοιόμορφα κατανεμημένες και επακριβώς αναπαραγωγίσιμες τυχαίες συμβολοσειρές. Αν και τα

βιομετρικά δεδομένα χρησιμοποιούνται για την παραγωγή τέτοιων συμβολοσειρών, δε συνάδουν πολλές φορές με την ομοιόμορφη κατανομή, ούτε αναπαράγονται ακριβώς κάθε φορά που μετριούνται. Αυτό ώθησε στο να δημιουργηθούν τεχνικές οι οποίες μετασχηματίζουν τα βιομετρικά χαρακτηριστικά ώστε να ελαττωθούν τα παραπάνω προβλήματα.

Πιο συγκεκριμένα, μελετήθηκαν οι τεχνικές των ασφαλών σκίτσων και ασαφών εξαγωγέων. Οι ασαφείς εξαγωγείς επιτρέπουν την εξαγωγή μίας ομοιόμορφα κατανεμημένης συμβολοσειράς και μίας δημόσιας, από το βιομετρικό στοιχείο και στη συνέχεια δίνουν τη δυνατότητα αναπαραγωγής της συμβολοσειράς αυτής από οποιοδήποτε βιομετρικό που είναι προσέγγιση του αρχικού δεδομένης της δημόσιας συμβολοσειράς. Ενώ, τα ασφαλή σκίτσα επιτρέπουν την ακριβή ανακατασκευή μιας θορυβώδους εισόδου, όπως είναι τα βιομετρικά δεδομένα. Για είσοδο ένα βιομετρικό, μια διαδικασία εξάγει ένα σκίτσο (συμβολοσειρά), το οποίο μπορεί να είναι δημόσιο. Στη συνέχεια, δεδομένου του σκίτσου και ενός βιομετρικού κοντά στο αρχικό, είναι δυνατή η ανάκτηση του αρχικού βιομετρικού.

Τέλος, οι τεχνικές των ασφαλών σκίτσων και ασαφών εξαγωγέων χρησιμοποιήθηκαν για τον απομακρυσμένο έλεγχο πρόσβασης, καθώς η δημόσια συμβολοσειρά που εξάγουν κωδικοποιεί τις πληροφορίες που απαιτούνται για την ανάκτηση του μυστικού και της επακόλουθης εξαγωγής. Ωστόσο, ήταν σημαντικό να μελετηθεί και η περίπτωση ενός ενεργού αντιπάλου ο οποίος μπορεί να τροποποιήσει τα μηνύματα που αποστέλλονται μεταξύ του διακομιστή και του χρήστη. Ένας αντίπαλος που μεταβάλλει τη δημόσια συμβολοσειρά που αποστέλλεται σε έναν χρήστη μπορεί να είναι σε θέση να μάθει τα βιομετρικά δεδομένα αυτού του χρήστη στο σύνολό τους. Γι΄αυτό το λόγο οι τεχνικές των ασφαλών σκίτσων και ασαφών εξαγωγέων επεκτάθηκαν ώστε να είναι σε θέση να εντοπίσουν τέτοιου είδους επίθεση. Οι νέες τεχνικές που μελετήθηκαν είναι τα ισχυρά ασφαλή σκίτσα και οι ισχυροί ασαφείς εξαγωγείς.

Για να ελαχιστοποιηθεί ακόμα περισσότερο η πιθανότητα επίθεσης τροποποίησης της δημόσιας συμβολοσειράς ελέγχθηκε η χρήση ενός πρωτοκόλλου ανταλλαγής κλειδιών PAK (Password-Authenticated Key Exchange). Πρόκειται για ένα προσφέρει σαφές πλεονέκτημα καθώς δε βασίζεται σε ομοιόμορφα ΄΄μυστικά΄΄, άρα δε χρειάζεται πρόσθετη εξαγωγή τυχαιότητας και επομένως είναι λειτουργικό ακόμα και για δεδομένα με χαμηλή εντροπία. Με την ασφάλεια του πρωτοκόλλου PAK, η ικανότητα

του αντιπάλου να μαντέψει το πρότυπο βιομετρικό μειώθηκε, αφού και στην περίπτωση τροποποίησης των δημόσιων πληροφοριών, ο χρήστης θα είναι πλέον σε θέση να χρησιμοποιήσει την ανακτημένη τιμή του βιομετρικού του για να ελέγξει αν η δημόσια πληροφορία έχει τροποποιηθεί. Καταλήγουμε, επίσης, ότι μεγαλύτερη ασφάλεια μας προσφέρει η χρήση του πρωτοκόλλου PAK, για δεδομένα με οποιαδήποτε εντροπία , ωστόσο, οι λύση με τα ισχυρά σκίτσα επειδή είναι λιγότερο πολύπλοκη προσφέρεται για δεδομένα με υψηλή εντροπία.

9.3 Πιθανές εφαρμογές

Πιστοποιημένη Συμφωνία Κλειδιού: Εδώ, ένας αξιόπιστος διακομιστής αποθηκεύει τα "πραγματικά" βιομετρικά δεδομένα W ενός χρήστη. Περιοδικά, ο χρήστης αποκτά μία καινούρια βιομετρική υπογραφή W' που μοιάζει, αλλά δεν είναι πανομοιότυπη με το W. Ο εξυπηρετητής και ο χρήστης τότε επιδιώκουν να πιστοποιήσουν αμοιβαία ο ένας τον άλλον και να συμφωνήσουν σε ένα κλειδί R πάνω σε ένα δίκτυο που μπορεί να μην είναι ασφαλές.

Ενθυλάκωση Κλειδιού: Εδώ, ένας χρήστης (μόνος του) χρησιμοποιεί τα βιομετρικά του δεδομένα W για να κατασκευάσει ένα τυχαίο κλειδί R μαζί με κάποια δημόσια πληροφορία P, και στη συνέχεια αποθηκεύει την P σε έναν μη αξιόπιστο εξυπηρετητή. Το κλειδί R μπορεί τότε να χρησιμοποιηθεί, για παράδειγμα για να κρυπτογραφηθεί κάποιο αρχείο για μία μακροχρόνια αποθήκευση. Σε μεταγενέστερη χρονική στιγμή, ο χρήστης αποκτά μια νέα βιομετρική πληροφορία W'. Αφού ανακτήσει την υπογραφή P από τον εξυπηρετητή, ο χρήστης ανακτά το R (με το οποίο μπορεί να αποκρυπτογραφήσει το αρχείο). Η πρόκληση εδώ είναι ότι η τιμή P που παρέχεται από το δίσκο ενδέχεται να μην είναι η ίδια με αυτή που αποθήκευσε αρχικά ο χρήστης. Σε αυτή τη δεύτερη περίπτωση ο χρήστης ουσιαστικά τρέχει ένα πρωτόκολλο συμφωνίας κλειδιού με τον εαυτό του σε δύο σημεία στο χρόνο.

Βιβλιογραφία

1. *Γεροντίδης Ευγένιος (2012), Βιομετρικά Συστήματα Ασφαλείας. Τεχνικές Υλοποίησης και Εφαρμογές τους, pp.7-29, Πτυχιακή Εργασία.*

2. *Σφυράκης Παναγίωτης (2008), Η Χρήση των Βιομετρικών Συστημάτων ως Μέσο Προστασίας των Πολιτών και των Πληροφοριών. Η Αναγκαιότητα Αποδοχής από τους Πολίτες, pp.8-12 και 22-27, Πτυχιακή Εργασία.*

3. *S. Karamizadeh, S. Abdullah, A. Manaf, M. Zamani and A. Hooman, "An Overview of Principal Component Analysis," Journal of Signal and Information Processing, Vol. 4 No. 3B, 2013, pp. 173-175. doi: 10.4236/jsip.2013.43B031.*

4. Jain, Anil K. Biometric Recognition: Overview and Recent Advances. *Lecture Notes in Computer Science.* **s.l. : Springer Berlin Heidelberg, σσ. 13–19.**

5. *A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349.*

6. *Jain A.K. (2007) Biometric Recognition: Overview and Recent Advances. In: Rueda L., Mery D., Kittler J. (eds) Progress in Pattern Recognition, Image Analysis and Applications. CIARP 2007. Lecture Notes in Computer Science, vol 4756. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-76725-1_2.*

7. *D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003.*

8.
http://portal.tee.gr/portal/page/portal/teetkm/DRASTHRIOTHTES/SEMINARIA/PALAIOTERA_SEMINARIA/SHMEIWSEIS_ASFALEIA_PLHROFORIAKWN_SYSTHMATWN/Tautopoihsh_kai_authentikopoihsh_me_biometrika_systhmata.pdf. **[Ηλεκτρονικό]**

9. *Brislawn, C.: The FBI fingerprint image compression specification. In: Topiwala, P. (ed.) Wavelet Image and Video Compression, pp. 271–288. Kluwer (1998).*

10. *Brislawn, C., Quirk, M.: Image compression with the JPEG-2000 standard. In: Driggers, R. (ed.) Encyclopedia of Optical Engineering, pp. 780–785. Marcel Dekker (2003).*

11. *Duda, Richard & Hart, Peter & G.Stork, David. (2001). Pattern Classification.*

12. *A. K. Jain, P. Flynn, A. Ross, Handbook of Biometrics, Springer, 2007.*

13. ***Rahul Chatterjee, M. Sadegh Riazi, Tanmoy Chowdhury, Emanuela Marasco, Farinaz Koushanfar, and Ari Juels. 2019. Multisketches: Practical Secure Sketches Using Off-the-Shelf Biometric Matching Algorithms. In Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19). Association for Computing Machinery, New York, NY, USA, 1171–1186. DOI:https://doi.org/10.1145/3319535.3363208.***

14. ***Ko, K. (2007), User's Guide to NIST Biometric Image Software (NBIS), NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.IR.7392 (Accessed March 19, 2021).***

15. ***G. Watson, W. Tabbasi, Michael and S. Janet, "User's Guide to NIST Fingerprint Image Software 1 (NFIS2)," 2006. [Online]. Available: http://cs.dm.u-tokai.ac.jp/paper/2006/bio/nfis2.pdf.***

16. ***S. Maddala, S. R. Tangellapally, J. S. Bartunek and M. Nilsson, "Implementation and evaluation of NIST Biometric Image Software for fingerprint recognition," in IEEE Xplore, Conference: Biosignals and Biorobotics Conference (BRC), 2011.***

17. ***D. Lee, K. Choi, and J. Kim, "A robust fingerprint matching algorithm using local alignment," in Pattern Recognition, 2002. Proceedings. 16th International Conference on, vol. 3. IEEE, 2002, pp. 803–806.***

18. ***Y. Zhang and F. Koushanfar, "Robust privacy-preserving fingerprint authentication," 2016 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), McLean, VA, USA, 2016, pp. 1-6, doi: 10.1109/HST.2016.7495547.***

19. ***Multisketches.*** **Chatterjee, Rahul, και συν. s.l. : ACM, 2019. Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security.**

20. ***Ματάμης Παναγιώτης (2004), Βιομετρικά κλειδιά, κρυπτογραφία και υποδομήδιανομής, Πτυχιακή εργασία.***

21. ***Dodis Y., Reyzin L., Smith A. (2004) Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In: Cachin C., Camenisch J.L. (eds) Advances in Cryptology - EUROCRYPT 2004. EUROCRYPT 2004. Lecture Notes in Computer Science, vol 3027. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-24676-3_31.***

22. ***Z. Akhtar, C. Micheloni, and G. L. Foresti, "Biometric liveness detection: Challenges and research opportunities," IEEE Security & Privacy, vol. 13, no. 5, pp. 63–72, 2015. [Online]. Available: https://doi.org/10.1109/MSP.2015.116.***

23. ***E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," ACM Comput. Surv., vol. 47, no. 2, pp. 28:1–28:36, 2014. [Online]. Available: https://doi.org/10.1145/2617756.***

24. ***C. Roberts, "Biometric attack vectors and defences," Comput. Secur., vol. 26, no. 1, pp. 14–25, Feb. 2007. [Online]. Available: http://dx.doi.org/10.1016/j.cose.2006.12.008.***

25. ***S. Yoon, J. Feng, and A. K. Jain, "Altered fingerprints: Analysis and detection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 3, pp. 451–464, 2012. [Online]. Available: https://doi.org/10.1109/TPAMI.2011.161.***

26. ***A. K. Jain, A. A. Ross, and K. Nandakumar, Introduction to Biometrics. Springer Publishing Company, Incorporated, 2011., Κεφάλαιο 7.***

27. ***F. Standaert, "Introduction to side-channel attacks," in Secure Integrated Circuits and Systems, 2010, pp. 27–42. [Online]. Available: https://doi.org/10.1007/978-0-387-71829-3 2.***

28. ***K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," in Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14- 16, 2001, Proceedings, no. Generators, 2001, pp. 251–261. [Online]. Available: https://doi.org/10.1007/3-540-44709-1 21.***

29. ***J. Galbally, S. Carballo, J. Fierrez, and J. Ortega-Garcia, "Vulnerability´ assessment of fingerprint matching based on time analysis," in Biometric ID Management and Multimodal Communication, Joint COST 2101 and 2102 International Conference, BioID MultiComm 2009, Madrid, Spain, September 16-18, 2009. Proceedings, 2009, pp. 285–292. [Online]. Available: https://doi.org/10.1007/978-3-642- 04391-8 37.***

30. ***M. Durmuth, D. Oswald, and N. Pastewka, "Side-channel attacks ¨ on fingerprint matching algorithms," in Proceedings of the 6th International Workshop on Trustworthy Embedded Devices, TrustED@CCS 16, Vienna, Austria, October 28, 2016, 2016, pp. 3– 13. [Online]. Available: http://doi.acm.org/10.1145/2995289.2995294.***

31. ***J. Waddle and D. A. Wagner, "Towards efficient second-order power analysis," in Cryptographic Hardware and Embedded Systems - CHES 2004: 6th International Workshop Cambridge, MA, USA, August 11-13, 2004. Proceedings, 2004, pp. 1–15. [Online]. Available: https://doi.org/10.1007/978-3-540-28632-5 1.***

32. ***S. Yang and I. M. Verbauwhede, "A secure fingerprint matching technique," in Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and***

Applications, ser. WBMA '03. New York, NY, USA: ACM, 2003, pp. 89–94. [Online]. Available: http://doi.acm.org/10.1145/982507.982524.

33. *U. Uludag and A. K. Jain, "Attacks on biometric systems: a case study in fingerprints," in Security, Steganography, and Watermarking of Multimedia Contents VI, San Jose, California, USA, January 18-22, 2004, Proceedings, 2004, pp. 622–633. [Online]. Available: https://doi.org/10.1117/12.530907.*

34. *Ratha N. K.,Connell J. H.,Bolle R. M., "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol. 40, no. 3, p. , 2001. [Online]. Available: http://www.cedar.buffalo.edu/ govind/CSE717/papers/.*

35. *A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process, vol. 2008, pp. 113:1–113:17, Jan. 2008. [Online]. Available: http://dx.doi.org/10.1155/2008/579416.*

36. *Wayman, James L., Technical Testing and Evaluation of Biometric Identification Devices. Boston, MA: Springer US, 1996, pp. 345–368. [Online]. Available: https://doi.org/10.1007/0-306-47044-6 17.*

37. *Bartlow N., Cukic B., "The vulnerabilities of biometric systems - anintegrated look and old and new ideas," Technical report, 2005.*

38. *A.Adler, Biometric System Security. Boston, MA: Springer US, 2008, pp. 381–402. [Online]. Available: https://doi.org/10.1007/978-0- 387-71041-9 19.*

39. *A. Hadid, N. W. D. Evans, S. Marcel, and J. Fierrez, "Biometrics ´ systems under spoofing attack: An evaluation methodology and lessons learned," IEEE Signal Process. Mag., vol. 32, no. 5, pp. 20–30, 2015. [Online]. Available: https://doi.org/10.1109/MSP.2015.2437652.*

40. *J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia, and D. Maio, "An evaluation of direct ´ attacks using fake fingers generated from ISO templates," Pattern Recognition Letters, vol. 31, no. 8, pp. 725–732, 2010. [Online]. Available: https://doi.org/10.1016/j.patrec.2009.09.032.*

41. *J. Feng, A. K. Jain, and A. Ross, "Detecting altered fingerprints," in 20th International Conference on Pattern Recognition, ICPR 2010, Istanbul, Turkey, 23-26 August 2010, 2010, pp. 1622–1625. [Online]. Available: https://doi.org/10.1109/ICPR.2010.401.*

42. *J. Shelton, K. S. Bryant, S. Abrams, L. Small, J. Adams, D. Leflore, A. Alford, K. Ricanek, and G. V. Dozier, "Genetic & evolutionary biometric security: Disposable feature extractors for mitigating biometric replay attacks," in Proceedings of the*

Conference on Systems Engineering Research, CSER 2012, St. Louis, MO, USA, March 19-22, 2012, 2012, pp. 351–360. [Online]. Available: https://doi.org/10.1016/j.procs.2012.01.072.

43. *K. Tiri, D. Hwang, A. Hodjat, B. Lai, S. Yang, P. Schaumont, and I. Verbauwhede, "A side-channel leakage free coprocessor ic in 0.18m cmos for embedded aes-based cryptographic and biometric processing," 2005.*

44. *K. J. Arun A. Ross, Jidnya Shah, "Toward reconstructing fingerprints from minutiae points," pp. 5779 – 5779 – 13, 2005. [Online]. Available: https://doi.org/10.1117/12.604477.*

45. *S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security & Privacy, vol. 1, no. 2, pp. 33–42, 2003. [Online]. Available: https://doi.org/10.1109/MSECP.2003.1193209.*

46. *A. K. Jain, A. Ross, and U. Uludag, "Biometric security: Challenges and solutions," in 13th European Signal Processing Conference, EUSIPCO 2005, Antalya, Turkey, September 4-8, 2005, 2005, pp. 1–4. [Online]. Available: http://ieeexplore.ieee.org/document/7078369/.*

47. *M. Martinez-Diaz, J. Fierrez-Aguilar, F. Alonso-Fernandez, J. OrtegaGarcia, and J. A. Siguenza, "Hill-climbing and brute-force attacks on biometric systems: A case study in match-on-card fingerprint verification," in Proceedings 40th Annual 2006 International Carnahan Conference on Security Technology, Oct 2006, pp. 151–159.*

48. *B. Tams, "Attacks and countermeasures in fingerprint based biometric cryptosystems," CoRR, vol. abs/1304.7386, 2013. [Online]. Available: http://arxiv.org/abs/1304.7386.*

49. *A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125–143, June 2006.*

50. *Joshi, M., Mazumdar, B., & Dey, S. (2018). Security Vulnerabilities Against Fingerprint Biometric System. ArXiv, abs/1805.07116.*

51. *Joshi, M., Mazumdar, B., & Dey, S. (2018). Security Vulnerabilities Against Fingerprint Biometric System. ArXiv, abs/1805.07116.*

52. *Χατζόπουλος Ιωάννης (2020), Βιομετρικές τεχνικές αναγνώρισης ατόμων με χρήση σημάτωνEEG, Πτυχιακή εργασία.*

53. ***Goldenberg, David, "Adaptive learning and cryptography" (2010). Dissertations, Theses, and MastersProjects. Paper 1539623564.https://dx.doi.org/doi:10.21220/s2-e7e2-bx24.***

54. ***Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data.*** **Dodis, Yevgeniy, και συν. s.l. : Society for Industrial & Applied Mathematics (SIAM), 1 2008, SIAM Journal on Computing, Τόμ. 38, σσ. 97–139.**

55. ***Nguyen T.A.T., Dang T.K. (2017) Protecting Biometrics Using Fuzzy Extractor and Non-invertible Transformation Methods in Kerberos Authentication Protocol. In: Hameurlain A., Küng J., Wagner R., Dang T., Thoai N. (eds) Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXI. Lecture Notes in Computer Science, vol 10140. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-54173-9_3.***

56. ***Sutcu, Y., Li, Q., & Memon, N. (2013). Secure Sketches for Protecting Biometric Templates. Security and Privacy in Biometrics, 69–104. doi:10.1007/978-1-4471-5230-9_4.***

57. ***Adaptive Learning And Cryptography.*** **Goldenberg, David. s.l. : College of William and Mary - Arts and Sciences, 2010.**

58. ***Anil K. Jain, Karthik Nandakumar, Arun Ross,50 years of biometric research: Accomplishments, challenges, and opportunities,Pattern Recognition Letters,Volume 79,2016,Pages 80-105,ISSN 0167-8655,https://doi.org/10.1016/j.patrec.2015.12.013.***

59. ***Boyko V., MacKenzie P., Patel S. (2000) Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman. In: Preneel B. (eds) Advances in Cryptology — EUROCRYPT 2000. EUROCRYPT 2000. Lecture Notes in Computer Science, vol 1807. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-45539-6_12.***

60. ***TIAN, Yangguang; LI, Yingjiu; SENGUPTA, Binianda; LI, Nan; and SU, Chunhua. Leakage-resilient biometricbased remote user authentication with fuzzy extractors. (2020). Theoretical Computer Science. 814,223-233. Research Collection School Of Information Systems.Available at: https://ink.library.smu.edu.sg/sis_research/5137.***

61. ***Boyen X., Dodis Y., Katz J., Ostrovsky R., Smith A. (2005) Secure Remote Authentication Using Biometric Data. In: Cramer R. (eds) Advances in Cryptology – EUROCRYPT 2005. EUROCRYPT 2005. Lecture Notes in Computer Science, vol 3494. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11426639_9.***

62. ***Xavier Boyen. 2004. Reusable cryptographic fuzzy extractors. In Proceedings of the 11th ACM conference on Computer and communications security (CCS '04). Association for Computing Machinery, New York, NY, USA, 82–91. DOI:https://doi.org/10.1145/1030083.1030096.***

63. ***https://cosec.bit.uni-bonn.de/fileadmin/user_upload/teaching/09ws/09ws-sem/biometry_security_VanessaEnd_handout.pdf.*** **[Ηλεκτρονικό]**

64. ***Dodis, Yevgeniy & Kanukurthi, Bhavana & Katz, Jonathan & Reyzin, Leonid & Smith, Adam. (2010). Robust Fuzzy Extractors and Authenticated Key Agreement From Close Secrets. IACR Cryptology ePrint Archive. 2010. 456. 10.1109/TIT.2012.2200290.***

65. ***MacKenzie, P.: The PAK Suite: Protocols for Password-Authenticated Key Exchange. DIMACS Tech-nical Report 2002-46 (2002).***

66. ***MacKenzie, P.D.: More Ecient Password-Authenticated Key Exchange. In: Naccache, D. (ed.) Topicsin Cryptology - CT-RSA 2001. LNCS, vol. 2020, pp. 361{377. Springer (2001).***

67. ***Bellare, M., Pointcheval, D., Rogaway, P.: Authenticated Key Exchange Secure Against DictionaryAttacks. In: Advances in Cryptology { EUROCRYPT 2000. LNCS, vol. 1807, pp. 139{155. Springer(2000).***

68. ***Protecting Biometrics Using Fuzzy Extractor and Non-invertible Transformation Methods in Kerberos Authentication Protocol.*** **Nguyen, Thi Ai Thao και Dang, Tran Khanh. [επιμ.] Abdelkader Hameurlain, και συν. Berlin : Springer Berlin Heidelberg, 2017. Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXI. σσ. 47–66. ISBN: 978-3-662-54173-9.**