ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ – ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ
Τμ. Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ – ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ασφάλεια βιομετρικών συστημάτων και ταυτοποίηση μέσω αυτών

Μεταπτυχιακή Φοιτήτρια: Καλαϊτζή Μαρία

ΑΜ: 3232019013

Ημερομηνίες ανάληψης - περάτωσης της Δ.Ε. : 07/10/2020- 17/02/2021

Επιβλέπων: Ριζομυλιώτης Παναγιώτης, Επίκουρος Καθηγητής

Εξεταστική Επιτροπή: Καρύδα Μαρία, Κοκολάκης Σπύρος

Σάμος, 2021

Πρόλογος και ευχαριστίες

Η παρούσα μελέτη αποτελεί διπλωματική εργασία στα πλαίσια του μεταπτυχιακού προγράμματος «Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων του τμήματος Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου. Θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της παρούσας διπλωματικής εργασίας, κ. Ριζομυλιώτη Παναγιώτη για την ευκαιρία που μου έδωσε να ασχοληθώ με το συγκεκριμένο θέμα, καθώς επίσης για την εμπιστοσύνη και την εκτίμηση που μου επέδειξε. Επίσης, θα ήθελα να ευχαριστήσω όλους τους καθηγητές για τις πολύτιμες γνώσεις που μου πρόσφεραν σε όλο το πέρας των μεταπτυχιακών σπουδών μου.

Από την εργασία αυτή, μου δόθηκε η ευκαιρία να διευρύνω τις γνώσεις μου στο τομέα της ασφάλειας βιομετρικών συστημάτων, καθώς και να γνωρίσω τις απέραντες δυνατότητες και εφαρμογές του κλάδου αυτού. Ελπίζω, η μελέτη αυτή να μου δώσει την ευκαιρία μελλοντικά να ασχοληθώ με το συγκεκριμένο αντικείμενο επαγγελματικά.

ΚΑΛΑΪΤΖΗ ΜΑΡΙΑ

Περίληψη

Η συγκεκριμένη μελέτη γίνεται στα πλαίσια της διπλωματικής μου εργασίας, η οποία θα παρουσιαστεί για το μεταπτυχιακό πρόγραμμα σπουδών Ασφάλεια Πληροφοριακών και Επικοινωνιακών Συστημάτων του τμήματος των Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων του Πανεπιστήμιου Αιγαίου.

Το θέμα αφόρα στο πώς μπορεί να επιτευχτεί η ταυτοποίηση χρηστών μέσω των βιομετρικών συστημάτων και κατά πόσο ασφαλής είναι αυτή η μέθοδος. Στόχος αυτής της διπλωματικής είναι η παρουσίαση των βιομετρικών τεχνολογιών υπό το πρίσμα της ασφάλειας πληροφοριακών συστημάτων και η ανάδειξη διάφορων τεχνικών και μεθόδων κρυπτογράφησης που χρησιμοποίει. Επιπλέον, θα γίνει περιγραφή της λειτουργικότητας και της αρχιτεκτονικής ενός τέτοιου συστήματος.

Στη παρούσα εργασία, θα γίνει εισαγωγή σε βασικές έννοιες και όρους που θα πρέπει να γνωρίζει ο αναγνώστης, ώστε να κατανοήσει το περιεχόμενο της εργασίας. Εν συνεχεία, θα αναλυθούν οι τεχνικές της αυθεντικοποίησης που χρησιμοποιούνται στα εν λόγο συστήματα και θα μελετηθούν οι μέθοδοι που χρησιμοποιεί ένα βιομετρικό σύστημα ώστε να επιτευχτεί η ταυτοποίηση των χρηστών. Επιπρόσθετα, θα αναλυθούν οι ευπάθειες και οι επιθέσεις που μπορεί να αντιμετωπίσει ένα τέτοιο σύστημα και θα αναφερθούν οι τρόποι αντιμετώπισης αυτών. Τέλος, θα γίνει η σύνοψη της συγκεκριμένης μελέτης και θα αναφερθούν εφαρμογές της βιομετρικής τεχνολογίας όπως επίσης και πεδία εφαρμογής της εν λόγο τεχνολογίας που μπορούν να υλοποιηθούν σε μελλοντικό χρονικό διάστημα.

Λέξεις κλειδιά: Βιομετρικά συστήματα, κρυπτογράφηση, αναγνώριση, ταυτοποίηση, αυθεντικοποίηση, επαλήθευση

Abstract

This study is part of my dissertation, which will be presented for the postgraduate program in Information and Communication Systems Security of the Department of Engineering Information and Communication Systems of the University of the Aegean.
The issue is how to identify users through biometric systems and how secure this method is. The aim of this dissertation is to present biometric technologies in the light of information systems security and to highlight the various encryption techniques and methods it uses. In addition, the functionality and architecture of such a system will be described.
In this paper, we will introduce basic concepts and terms that the reader should know in order to understand the content of the work. The authentication techniques used in these systems will then be analyzed and the methods used by a biometric system to achieve user identification will be studied. In addition, the vulnerabilities and attacks that such a system may face will be analyzed and the ways to deal with them will be mentioned. Finally, the specific study will be summarized and applications of biometric technology will be reported as well as fields of application of this technology that can be implemented in the future.

Keywords: Biometric systems, encryption, recognition, authentication, authentication

Περιεχόμενα

Ευρετήριο πινάκων

Ευρετήριο εικόνων

1. Εισαγωγή

1.1 Αντικείμενο διπλωματικής

Ο τομέας της ασφάλειας των πληροφοριακών συστημάτων είναι ένας από τους πλέον αναπτυσσόμενους στον χώρο της πληροφορικής, καθώς διαδραματίζει σημαντικό ρόλο στην εποχή που διανύουμε, η οποία χαρακτηρίζεται από κλοπές ταυτότητας παραβίαση των προσωπικών δεδομένων κ.α. Έτσι, αποτελεί μείζονος σημασίας η εφεύρεση συστημάτων και τεχνικών που θα διασφαλίζουν την προστασία των προσωπικών δεδομένων και γενικά των πληροφοριακών συστημάτων. Μέρος της ασφάλειας ενός πληροφοριακού συστήματος αποτελεί ο έλεγχος της ταυτότητας των χρηστών του. Αυτό γίνεται με την ταυτοποίηση και αυθεντικοποίηση του χρήστη, δυο έννοιες που θα αναλυθούν εκτενέστερα στην επόμενη υποενότητα.

Η ανάγκη για ταυτοποίηση προσώπων και εξουσιοδοτημένη πρόσβαση σε ειδικούς χώρους, εγκαταστάσεις ασφαλείας ή ευαίσθητα αρχεία οδήγησε στην ανάπτυξη διαφόρων συστημάτων ελέγχου πρόσβασης. Ως επί το πλείστον τα συστήματα χρησιμοποιούν ένα ή περισσότερα μοναδικά χαρακτηριστικά τα οποία θα αυθεντικοποιήσουν το χρήστη ώστε να του επιτρέψουν τη πρόσβαση σε οποιαδήποτε υπηρεσία, σύστημα ή ακόμη και φυσικό χώρο.
Οι ευρέως χρησιμοποιημένοι μέθοδοι ταυτοποίησης γίνονται μέσω των παραδοσιακών συστημάτων ελέγχου ταυτότητας τα οποία βασίζονται συνήθως στη χρήση μαγνητικών καρτών, ειδικών ετικετών RFID ή την πληκτρολόγηση προσωπικών κωδικών ασφαλείας. Όμως οι παραπάνω τρόποι ταυτοποίησης παρουσιάζουν συγκεκριμένα μειονεκτήματα ασφάλειας τα οποία ενδεικτικά, και ανάλογα με το σύστημα, είναι ο απομαγνητισμός ή καταστροφή της κάρτας μετά από χάραγμα της μαγνητικής λωρίδας ή μετά από έκθεση σε υψηλές θερμοκρασίες, η απώλεια των κωδικών ασφαλείας ή της κάρτας ταυτοποίησης, κτλ.

Ο βιομετρικός τρόπος ταυτοποίησης είναι μια εναλλακτική λύση που επιλύει τα παραπάνω προβλήματα των παραδοσιακών συστημάτων. Τα συστήματα που χρησιμοποιούν το βιομετρικό τρόπο ονομάζονται βιομετρικά συστήματα και χρησιμοποιούν τα φυσιολογικά χαρακτηριστικά και τα χαρακτηριστικά συμπεριφοράς για την ταυτοποίηση του κάθε ατόμου. Στις επόμενες ενότητες θα αναφέρουμε τους λόγους για τους οποίους κρίνεται τόσο σημαντική η χρήση των βιομετρικών μεθόδων και συστημάτων ως μέσο προστασίας των πολιτών αλλά και των πληροφοριών. Επίσης θα αναλύσουμε τον τρόπο λειτουργίας αυτών των συστημάτων, καθώς και τα χαρακτηριστικά τους.

1.2 Βασικές έννοιες

Πριν προχωρήσουμε περαιτέρω, θα αναλύσουμε βασικές έννοιες που θα χρειαστούν για την καλύτερη κατανόηση του περιεχομένου της εργασίας.

1.2.1 Αυθεντικοποίηση και Ταυτοποίηση

Αυθεντικοποίηση ενός υποκείμενου καλείται η διαδικασία αναγνώρισης της ταυτότητας του κατά την οποία επαληθεύεται η δηλωθείσα ταυτότητα του υποκειμένου αυτού. (Uwe Bubeck, 2003). Με λίγα λόγια, είναι η είναι η ικανότητα να αποδεικνύεται ένας χρήστης ή μια εφαρμογή ότι είναι πραγματικά αυτός που ισχυρίζεται ότι είναι.

Υπάρχουν τρεις μέθοδοι ελέγχου ταυτότητας με τους οποίους επαληθεύονται οι ταυτότητες των χρηστών και στα οποία βασίζονται τα περισσότερα συστήματα:

- Αυθεντικοποίηση από γνώση (κάτι που οι χρήστες ξέρουν) (π.χ. ερώτηση ασφαλείας, κωδικός πρόσβασης)
- Αυθεντικοποίηση από ιδιοκτησία (κάτι που οι χρήστες έχουν) (π.χ. ταυτότητα, κάρτα)
- Αυθεντικοποίηση από χαρακτηριστικά (κάτι που οι χρήστες είναι) (π.χ. αναγνώριση προσώπου, βιομετρικά δεδομένα)

Για να είναι αποτελεσματικοί, οι μηχανισμοί ελέγχου ταυτότητας θα πρέπει να αναγνωρίζουν μοναδικά μια οντότητα. Οι μηχανισμοί "Αυθεντικοποίηση από γνώση " και "Αυθεντικοποίηση από ιδιοκτησία" υστερούν στην αποτελεσματικότητα, καθώς οι πληροφορίες ελέγχου ταυτότητας θα μπορούσαν να χαθούν, να κλαπούν ή να παραβιαστούν επειδή ο χρήστης δεν είναι φυσικά συνδεδεμένος με τις πληροφορίες αυτές. Κύρια αδυναμία της μεθόδου "Αυθεντικοποίηση από γνώση" αποτελεί το γεγονός ότι είναι πολύ εύκολο κάποιος να μάθει κάτι που ξέρει κάποιος άλλος, όπως επίσης είναι πιθανό να μαντέψει τις πληροφορίες χωρίς καν να έχει πρόσβαση σε αυτές. Παρά ταύτα, είναι ευκολότερο μια πληροφορία που προέρχεται από γνώση να προστατευτεί από ένα φυσικό αντικείμενο. Αυτό οφείλεται στο γεγονός ότι ένα είδος γνώσης, αν και είναι εύκολο να αντιγραφεί, είναι πάντα πλήρως στην κατοχή του ατόμου που προσδιορίζει. Σε αντίθεση με ένα κλειδί, κάρτα ή άλλη φυσική συσκευή, που μπορεί να κλαπεί, να ξεχαστεί σε κάποιο χώρο, να πέσει κατά λάθος από μια τσέπη κτλ. (Anil K. Jain, et al., 2008)

Η τρίτη μέθοδος ελέγχου ταυτότητας, "Αυθεντικοποίηση από χαρακτηριστικό", είναι πολύ ισχυρότερος από τους δύο πρώτους, καθώς η οντότητα είναι στενά συνδεδεμένη με αυτό. Πολλά φυσιολογικά και συμπεριφοριστικά χαρακτηριστικά είναι μοναδικά για ένα άτομο. Αυτό καθιστά τα βιομετρικά αναγνωριστικά εγγενώς πιο αξιόπιστα και ικανά από τις τεχνικές που βασίζονται στη γνώση και τα διακριτικά για τη διάκριση ενός εξουσιοδοτημένου ατόμου από έναν απατεώνα. Ο τρόπος αναγνώρισης αφορά το έργο της σύγκρισης του βιομετρικού δείγματος ενός χρήστη με το σύνολο των προτύπων των χρηστών που είναι εγγεγραμμένοι στη βάση δεδομένων για την εξαγωγή της ταυτότητας του χρήστη. Ένα σημαντικό εμπόδιο με αυτόν τον τύπο ελέγχου ταυτότητας είναι το υψηλό κόστος και η δυσκολία κατασκευής αποδοτικών συσκευών που μπορούν να αποκτήσουν ένα αντιπροσωπευτικό δείγμα ενός χαρακτηριστικού για να διακρίνουν έγκυρα το ένα άτομο από το άλλο. Ωστόσο, ακόμη και αυτά τα συστήματα δεν είναι τελείως εγγυημένο ότι είναι αλάνθαστα, καθώς σε ειδικές περιπτώσεις όπως για παράδειγμα τα δείγματα DNA από ομοζυγωτικά δίδυμα δεν θα μπορούσαν ίσως να διακριθούν από τις συσκευές αναγνώρισης DNA. Σε αυτή τη περίπτωση θα

μπορούσε να γίνει ο συνδυασμός αυτής της μεθόδου με κάποιας άλλης μεθόδου, με τη χρήση ενός ακόμη δεδομένου, όπως η τοποθέτηση κάποιου κωδικού.

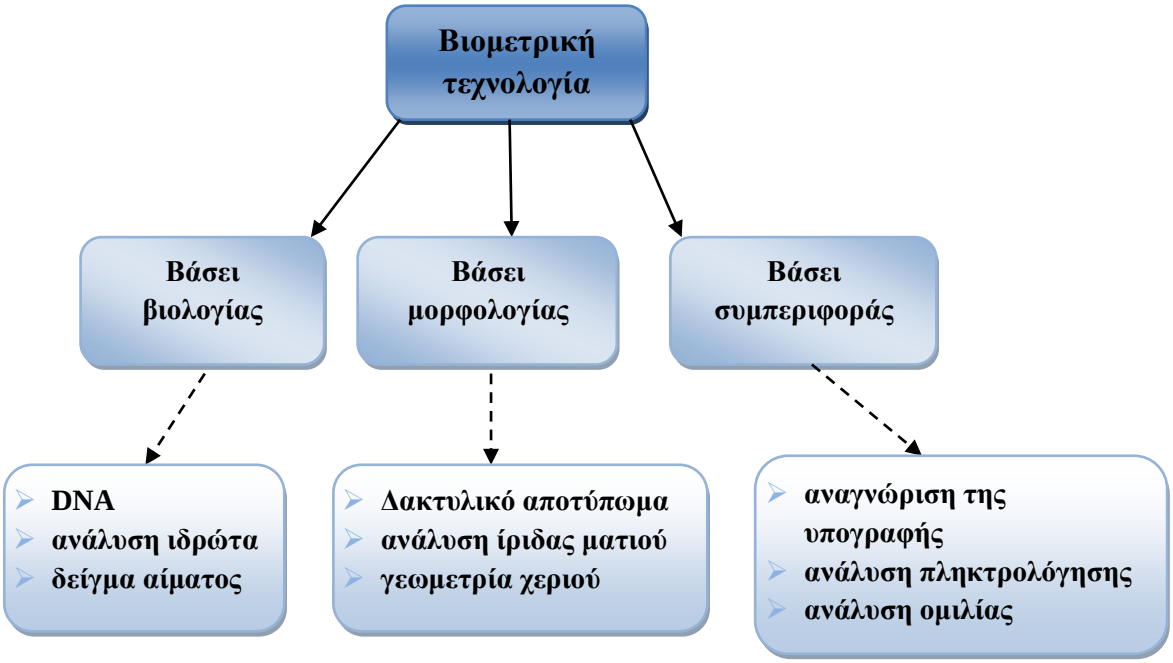
Μέθοδοι ελέγχου ταυτότητας	Πλεονεκτήματα	Μειονεκτήματα
Αυθεντικοποίηση από γνώση (κάτι που οι χρήστες ξέρουν)	✓ Εύκολη υλοποίηση και εφαρμογή ✓ Τροποποιούνται εύκολα ✓ Δεν χάνονται ✓ Αν και είναι απλά στη χρήση τους, στην περίπτωση που είναι ένας συνδυασμός αλφαριθμητικών χαρακτήρων, δεν αποκαλύπτονται εύκολα.	✓ Τα τεκμήρια αυθεντικοποίησης εύκολα μπορούν να αντιγραφούν ✓ Είναι εφικτό να τα μαντέψει κανείς χωρίς ιδιαίτερες τεχνικές γνώσεις ✓ Συνήθως μπορούν να αποκαλυφθούν με αυτοματοποιημένες μεθόδους ✓ Μπορούν να ξεχασθούν εύκολα.
Αυθεντικοποίηση από ιδιοκτησία (κάτι που οι χρήστες έχουν)	✓ Δεν αντιγράφονται εύκολα καθώς κατασκευάζονται από υλικά τα οποία δεν ευρέως διαθέσιμα	✓ Υψηλό κόστος ✓ Μπορούν να χαθούν ή να κλαπούν
Αυθεντικοποίηση από χαρακτηριστικά (κάτι που οι χρήστες είναι)	✓ Παρέχουν μεγαλύτερη ασφάλεια τις άλλες μεθόδους	✓ Δυσκολίες στην κατασκευή αξιόπιστων συσκευών αναγνώρισης με χαμηλό κόστος. ✓ Δεν είναι αλάνθαστα

Πίνακας 1.1: Πλεονεκτήματα και μειονεκτήματα μεθόδων έλεγχου ταυτότητας

Ταυτοποίηση ενός υποκείμενου καλείται η διαδικασία υποδήλωσης μιας απαίτησης που υποτίθεται ότι βεβαιώνει την ταυτότητα ενός προσώπου ή αντικειμένου. (Abhishek Nagar,2012). Με λίγα λόγια, ταυτοποίηση είναι η ικανότητα να αναγνωρίζεται μοναδικά ένας χρήστης ενός συστήματος ή μιας εφαρμογής που εκτελείται στο σύστημα ενώ η αυθεντικοποίηση είναι η διαδικασία που επιβεβαιώνει αυτή την ταυτότητα. Η ταυτοποίηση και αυθεντικοποίηση αποτελούν τα δύο μέρη ενός πρωτοκόλλου επικοινωνίας, που ενεργοποιείται όταν ένα υποκείμενο αιτείται προσπέλαση στους πόρους ενός πληροφορικού συστήματος. Σε αυτήν την επικοινωνία το πρώτο από τα δύο μέρη, δηλαδή το υποκείμενο, λέγεται, επικυρωτής, καθώς πρέπει να παρέχει τις πληροφορίες εκείνες που χρειάζονται για την απόδειξη της ταυτότητας του. Το δεύτερο μέρος, για παράδειγμα το πληροφοριακό σύστημα, λέγεται σκεπτικιστής, γιατί ελέγχει και επιβεβαιώνει την ορθότητα των πληροφοριών που του έχει δώσει ο επικυρωτής.

1.2.2 Βιομετρία και Βιομετρική τεχνολογία

Βιομετρία ορίζεται ως η επιστήμη του προσδιορισμού της ταυτότητας ενός ατόμου λαμβάνοντας υπόψη τις φυσικές, χημικές ή συμπεριφοριστικές ιδιότητες ενός ατόμου. (Anil K. Jain, et al., 2008). Ο βιομετρικός σχεδιασμός είναι ουσιαστικά ένα σύστημα που αποκτά βιομετρικά δεδομένα από ένα άτομο. Από αυτά τα δεδομένα, εξάγονται χρήσιμες πληροφορίες, σε καθορισμένη μορφή όπως χαρακτηριστικά. Για τη διαδικασία αντιστοίχισης, αυτές οι πληροφορίες συγκρίνονται με αποθηκευμένα βιομετρικά σύνολα σε μια βάση δεδομένων. Πιο συγκριμένα, η βιομετρική τεχνολογία λαμβάνει και χρησιμοποιεί πληροφορίες από τα παρακάτω πεδία:



Εικόνα 1.2: Κατηγοριοποίηση βιομετρικής τεχνολογίας

- Η βιομετρική βάσει βιολογίας χρησιμοποιεί χαρακτηριστικά σε γενετικό και μοριακό επίπεδο. Αυτά μπορεί να περιλαμβάνουν χαρακτηριστικά όπως το DNA ή το αίμα τα οποία μπορεί να αξιολογηθούν μέσω ενός δείγματος των υγρών του ανθρωπίνου σώματός.
- Η βιομετρική βάσει μορφολογίας περιλαμβάνει τη δομή του ανθρωπίνου σώματός. Σε αυτή τη περίπτωση χαρτογραφούνται με σαρωτές ασφαλείας διάφορα φυσικά χαρακτηριστικά όπως το μάτι, το δακτυλικό αποτύπωμα ή το σχήμα του προσώπου.
- Η βιομετρική βάσει συμπεριφοράς βασίζεται σε μοτίβα μοναδικά για κάθε άτομο. Ο τρόπος με τον βαδίζει, μιλάει ή ακόμα και πληκτρολογεί ένα άτομο μπορεί να αποτελέσει ένδειξη της ταυτότητάς του εάν παρακολουθούνται αυτά τα μοτίβα.

1.3 Είδη συστημάτων ελέγχου ταυτότητας /

Το σύστημα προσωπικού ελέγχου ταυτότητας είναι ένα σύστημα που επαληθεύει την ταυτότητα ενός ατόμου, το οποίο ισχυρίζεται ότι είναι. Τα δυο βασικά είδη συστημάτων έλεγχου ταυτότητας είναι το παραδοσιακό σύστημα που βασίζεται κυρίως σε υποδομές δημόσιου κλειδιού (PKI) και σε μυστικά κλειδιά και το βιομετρικό σύστημα που βασίζεται σε φυσικές, χημικές ή συμπεριφοριστικές ιδιότητες ενός ατόμου. Ο παραδοσιακός έλεγχος ταυτότητας βασίζεται στην κατοχή μυστικού κλειδιού, δηλαδή, όταν ο χρήστης διαθέτει το κλειδί, επιβεβαιώνεται η αυθεντικότητά του. (Abhishek Nagar,2012). Ο προσωπικός έλεγχος ταυτότητας με βάση το PKI είναι μια από τις πιο διαδεδομένες μεθόδους ελέγχου ταυτότητας, η οποία χρησιμοποιεί ένα ιδιωτικό κλειδί για να αποδείξει την ταυτότητα του χρήστη. Συνήθως τα κρυπτογραφικά κλειδιά είναι μεγάλα και τυχαία (π.χ. το μήκος κλειδιού του RSA είναι 128 bit), επομένως είναι δύσκολο να απομνημονευθούν. Ως αποτέλεσμα, τα κρυπτογραφικά κλειδιά αποθηκεύονται σε μια έξυπνη κάρτα της οποίας το δικαίωμα πρόσβασης προστατεύεται από προσωπικό αριθμό ταυτότητας (PIN), που είναι ένα είδος κωδικού πρόσβασης, ή αποθηκεύεται στον υπολογιστή και προστατεύεται από PIN. Οι απλοί κωδικοί πρόσβασης είναι εύκολο να σπάσουν, επομένως, θέτουν σε κίνδυνο την ασφάλεια. Από την άλλη, οι σύνθετοι κωδικοί πρόσβασης είναι δύσκολο να απομνημονευθούν. Ο παραδοσιακός έλεγχος ταυτότητας, ο οποίος

βασίζεται σε κρυπτογραφικά κλειδιά, έχει αρκετούς περιορισμούς σε σχέση με τη βιομετρική, η οποία έχει αρκετά πλεονεκτήματα ασφάλειας και χρηστικότητας.

Ο βιομετρικός έλεγχος ταυτότητας αναφέρεται στην επαλήθευση ατόμων βάσει των φυσιολογικών ή συμπεριφοριστικών τους μοτίβων, οπότε είναι αδύνατον να χαθούν ή να ξεχαστούν τα βιομετρικά χαρακτηριστικά, όπως επίσης είναι εξαιρετικά δύσκολο να αντιγραφούν, να μοιραστούν και να διανεμηθούν. (Bolle R. M. et al., 2013). Έτσι, ο βιομετρικός έλεγχος ταυτότητας είναι ένας τέλειος υποψήφιος για να αντικαταστήσει τον παραδοσιακό έλεγχο ταυτότητας που βασίζεται σε κρυπτογραφικά κλειδιά, καθώς παρέχει υψηλή ασφάλεια για έλεγχο πρόσβασης σε περιβάλλον πρόσωπο με πρόσωπο, όπως το ηλεκτρονικό εμπόριο, μέσω ανοικτού δικτύου.

Η διαδικασία του έλεγχου ταυτότητας λειτουργεί μέσω ενός μηχανισμού σύνδεσης ενός εισερχόμενου αιτήματος με ένα σύνολο αναγνωριστικών διαπιστευτηρίων. Τα διαπιστευτήρια που παρέχονται συγκρίνονται με αυτά σε ένα αρχείο σε μια βάση δεδομένων με τις πληροφορίες του εξουσιοδοτημένου χρήστη σε ένα τοπικό λειτουργικό σύστημα ή σε ένα διακομιστή ελέγχου ταυτότητας. Αν οι πληροφορίες από τη σύγκριση που θα πραγματοποιηθεί είναι ίδιες τότε ο χρήστης αυθεντικοποιείται και του επιτρέπεται η πρόσβαση σε πόρους του εκάστοτε συστήματος. (Santiago Gonzalez et al., 2003)

1.4 Δομή διπλωματικής εργασίας

Σε αυτή τη διπλωματική αναλύσαμε την ασφάλεια των βιομετρικών συστημάτων, ένα θέμα αρκετά επίκαιρο για τη εποχή που διανύουμε μιας και ο κίνδυνος υποκλοπής των δεδομένων είναι αυξημένος και έγκειται απαραίτητη μια διεξοδική λύση αυτής της πρόκλησης. Συγκεντρωτικά, λοιπόν στο πρώτο κεφάλαιο έγινε μια εισαγωγή σε βασικές έννοιες όπως η ταυτοποίηση και η αυθεντικοποίηση και αναλύθηκαν τα είδη συστημάτων ελέγχου ταυτότητας. Στο δεύτερο κεφάλαιο, αφού πρωτίστως έγινε μια ιστορική αναδρομή, στη συνέχεια μελετήσαμε την αρχιτεκτονική ενός βιομετρικού συστήματος και τις προδιαγραφές των βιομετρικών χαρακτηριστικών. Επιπρόσθετα, παρουσιάσαμε αναλυτικά τα βασικότερα είδη βιομετρικών χαρακτηριστικών, όπως το δακτυλικό αποτύπωμα, η ίριδα, τα χαρακτηριστικά του προσώπου και η φωνή και συγκρίνοντας τα ως προς την καθολικότητα, τη διάκριση, τη μονιμότητα τη συλλεκτικότητα, την απόδοση, την αποδοχή και τη καταστρατήγηση, καταλήξαμε στο συμπέρασμα ότι ίριδα έχει τη μεγαλύτερη ακρίβεια στην αναγνώριση των ατόμων και η φωνή τη μικρότερη. Στη συνέχεια, αναφέρθηκαν ορισμένα παραδείγματα χρήσης βιομετρικών συστημάτων και σχολιάστηκε η απόδοση των βιομετρικών συστημάτων με όρους FAR και FRR. Τέλος, παρουσιάστηκαν τα πλεονεκτήματα και μειονεκτήματα βιομετρικών συστημάτων, καθώς και το νομικό πλαίσιο που διέπει την εν λόγο τεχνολογία. Στο τρίτο κεφάλαιο αναφέρθηκαν επιγραμματικά οι απαιτήσεις ασφάλειας και οι ευπάθειες των βιομετρικών συστημάτων, οι επιθέσεις σε αυτά καθώς και οι τεχνικές αντιμετώπισης των ευπαθειών. Πιο συγκεκριμένα, μελετήθηκαν τεχνικές υδατογράφησης και στεγανογραφίας, και τεχνικές βασισμένες στον μετασχηματισμό χαρακτηριστικών για την αύξηση της ασφάλειας των βιομετρικών προτύπων. Στο τέταρτο κεφάλαιο εξετάστηκαν οι τρόποι με τους οποίους επιτυγχάνεται η προστασία των βιομετρικών προτύπων, όπως η τεχνική του key binding και του key generating και μελετήθηκε εις βάθος η τεχνική της βιομετρικής κρυπτογράφησης. Επιπρόσθετα, παρουσιάστηκε ο τρόπος δημιουργίας κρυπτογραφικών κλειδιών από βιομετρικά δεδομένα και τα πλεονεκτήματα που υφίστανται από τη χρήση της βιομετρικής κρυπτογράφησης. Τέλος, στο πέμπτο κεφάλαιο γίνεται μια σύνοψη της διπλωματικής και αναφέρονται ορισμένα

συμπεράσματα που προέκυψαν από την μελέτη του εν λόγο θέματος. Ακολούθως, γίνεται μια αναφορά σε μελλοντικές προοπτικές που έχει η συγκριμένη τεχνολογία και ορισμένες βελτιώσεις που μπορούν να γίνουν στα ήδη υπάρχοντα βιομετρικά συστήματα.

Εικόνα 1.3: Δομή διπλωματικής εργασίας

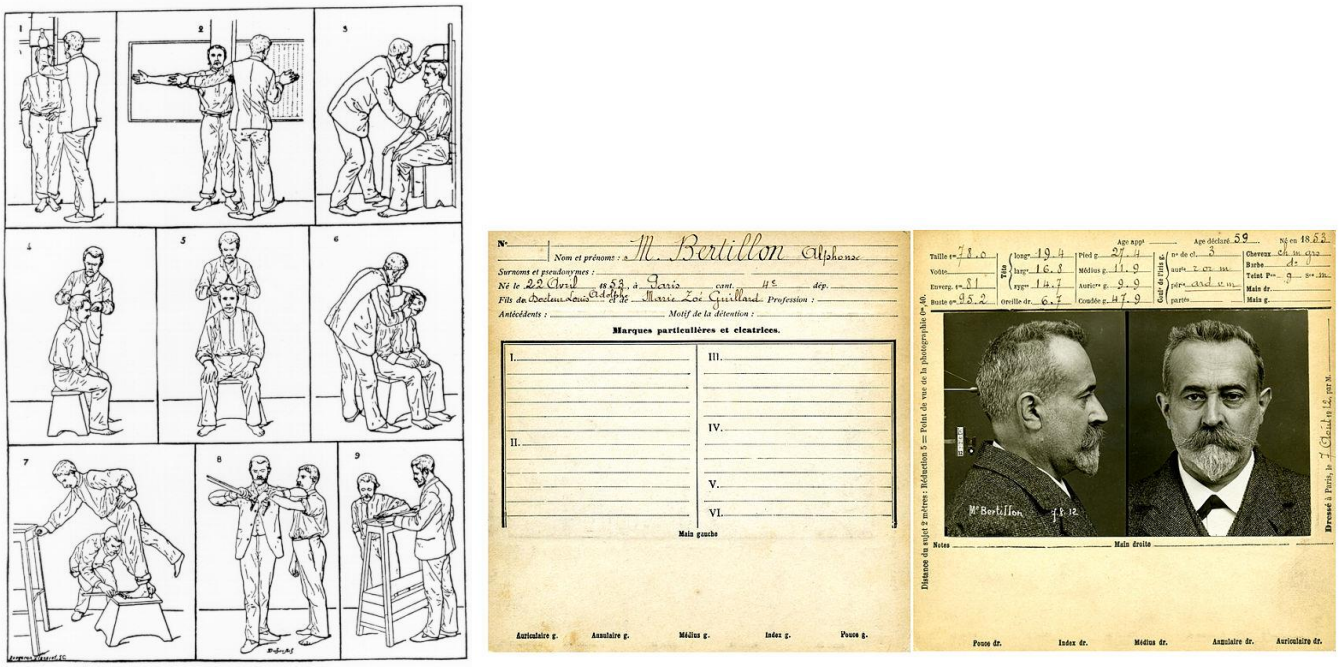
2. Βιομετρική τεχνολογία

2.1 Ιστορική αναδρομή

Η βιομετρία για πολλούς φαντάζει ως κάτι πρόσφατο, όμως κάνοντας μια ιστορική αναδρομή θα διαπιστώσουμε ότι υπήρξαν αρκετά ιστορικά γεγονότα που αποδεικνύουν ότι η χρήση των βιομετρικών μεθόδων για την εξακρίβωση της ταυτότητας των ατόμων υφίσταται από αρχαιοτάτων χρόνων. Ο πρώτος ιστορικός σταθμός παρατηρήθηκε στην αρχαία Αίγυπτο όταν χρησιμοποιήθηκαν βιομετρικές πληροφορίες (π.χ. ύψος περίμετρος, βάρος) των εργατών που κατασκεύαζαν τις πυραμίδες για την επεξεργασία της πληρωμής τους. Άλλη μια καταγραφή της χρήσης της βιομετρίας παρουσιάστηκε κατά την εποχή της Βαβυλώνας, όπου χρησιμοποιήθηκαν τα αποτυπώματα χεριών για την απόδειξη της αυθεντικότητας ορισμένων εργασιών.

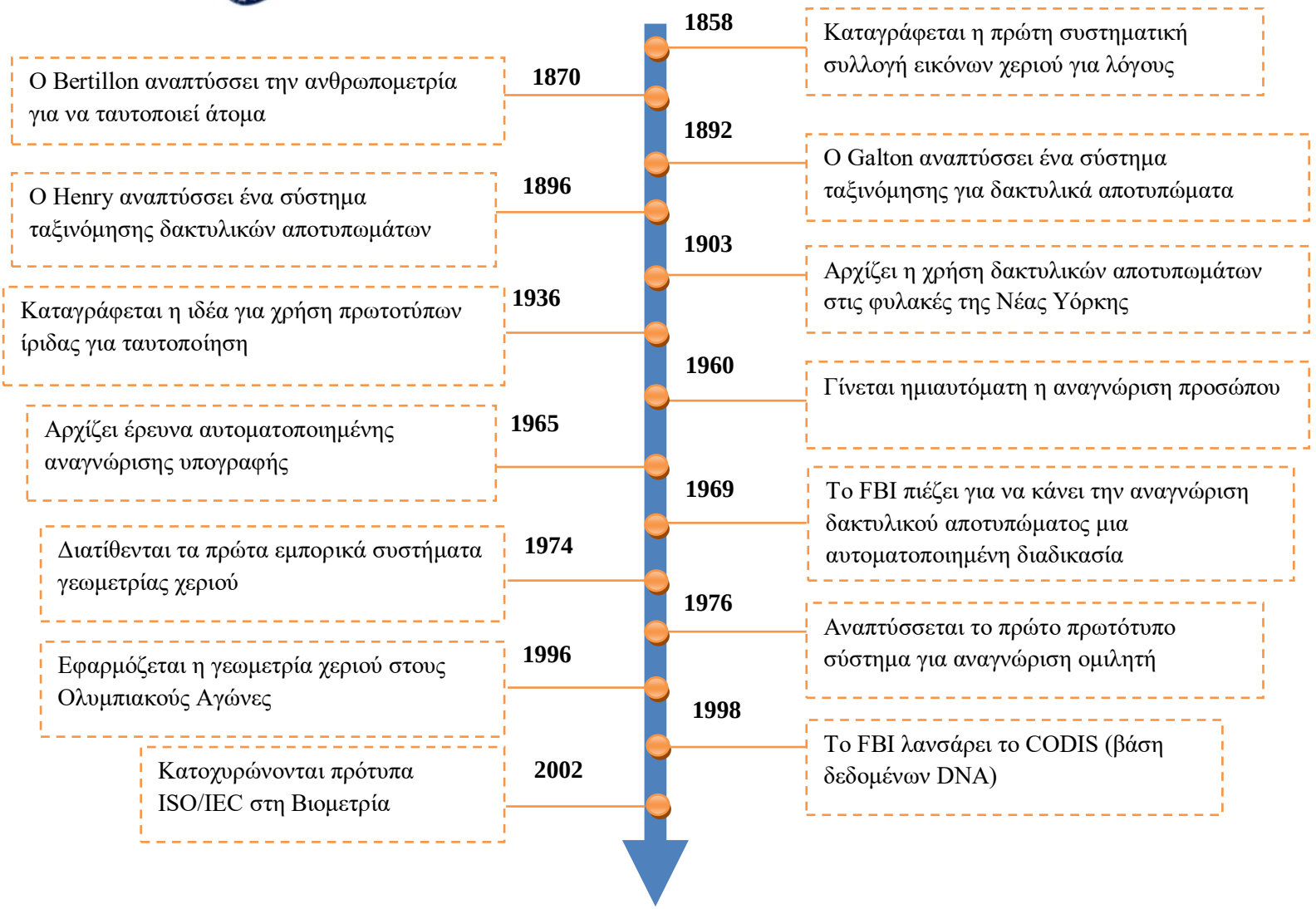
Εικόνα 2.1: Αποτυπώματα από τη συλλογή του Herschel [56]

Η πρώτη συστηματική καταγραφή βιομετρικών δεδομένων για σκοπούς ταυτοποίησης έγινε από τον William Herschel το 1858. Ο Herschel θεωρείται ο πρώτος Ευρωπαίος που σημείωσε την αξία των δακτυλικών αποτυπωμάτων για αναγνώριση. Το 1870 ήταν μια δεκαετία που χαρακτήρισε την επιστήμη της βιομετρίας, καθώς δρομολογήθηκε η ποσοτική μέτρηση των ατόμων με σκοπό την ταυτοποίηση. Το 1870, ο Alphonse Bertillon, Γάλλος αστυνομικός, ανέπτυξε μια μέθοδο γνωστή ως σύστημα Bertillon για την αναγνώριση των εγκληματιών με βάση μετρήσεις των σωμάτων τους όπως η διάμετρος κρανίου, το μήκος βραχίονα και ποδιών, το μήκος δακτύλων κτλ. Ο συνδυασμός αυτών των μεθόδων αποτέλεσε το κύριο σύστημα αναγνώρισης για τον προσδιορισμό των φυλακισμένων μέχρι τη δεκαετία του '20. Το 1888, ο Αργεντινός αστυνομικός Juan Vucetich, ήταν ο πρώτος που χρησιμοποίησε ως τεχνική ταυτοποίησης δακτυλικά αποτυπώματα με τη χρήση μελανιού. Λίγα χρόνια αργότερα, το 1893, ο Sir Francis Galton απέδειξε ότι δύο δακτυλικά αποτυπώματα δεν είναι ποτέ όμοια, ούτε καν σε ομοζυγωτικά δίδυμα. Μετά την ανακάλυψη της μοναδικότητας των δακτυλικών αποτυπωμάτων, δημιουργήθηκε σε μια βάση δεδομένων (ένα αρχείο καρτών) με τα δακτυλικά αποτυπώματα εγκληματιών, το οποίο βοήθησε στον γρήγορο εντοπισμό και στην ταυτοποίηση τους. Με το πέρασμα των δεκαετιών έγιναν αρκετές έρευνες για συστήματα αναγνώρισης ομιλίας και δακτυλικών αποτυπωμάτων. Η δεκαετία του '70 χαρακτηρίστηκε από την ανάπτυξη και την επέκταση των συστημάτων γεωμετρίας χεριού, ενώ μια δεκαετία αργότερα έκαναν την εμφάνιση τους τα συστήματα επαλήθευσης αμφιβληστροειδή, υπογραφής και τα συστήματα αναγνώρισης προσώπου. Στη πορεία, τη δεκαετία του '90 αναπτύχθηκαν τα συστήματα αναγνώρισης ίριδας.



Εικόνα 2.2: Μέθοδος Bertillonge [57]

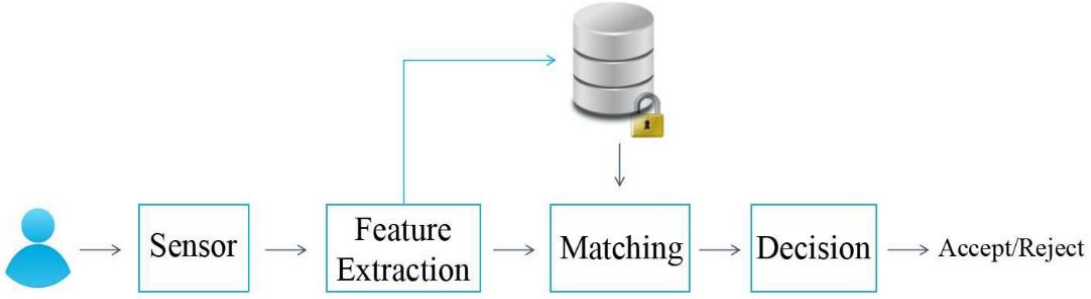
Η βασική ανάγκη της ανάπτυξης των βιομετρικών μέσων ταυτοποίησης ήταν κυρίως για εγκληματολογικούς λόγους (π.χ., παράνομοι μετανάστες, ιατροδικαστική εγκληματολογία, ταυτοποίηση φυλακισμένων), όμως στη πορεία αναπτύχτηκαν συστήματα και για εφαρμογές της καθημερινής ζωής, όπως για παράδειγμα άνοιγμα κινητού με δακτυλικό αποτύπωμα, πρόσβαση σε φυσικούς χώρους είσοδος σε πόρους πληροφοριακών συστημάτων κτλ. Ο ταχύτατος ρυθμός της ανάπτυξης και της έρευνας στο πεδίο της βιομετρικής τεχνολογίας σύντομα δημιούργησε καινούργιες μεθόδους ταυτοποίησης βασισμένες σε πρότυπα πληκτρολόγησης, πρότυπα βαδίσματος, πρότυπα ομιλίας, γεωμετρίας του αυτιού, ανάλυσης DNA κτλ. (Jain K. Et al., 2008). Η εξέλιξη των βιομετρικών τεχνολογιών είναι ραγδαία, ειδικά τα τελευταία χρόνια έχει σημειωθεί σημαντική πρόοδος και πλέον τα συστήματα βιομετρικού ελέγχου ταυτότητας έχουν αντίκρισμα σε πολυάριθμες εφαρμογές. Στο παρακάτω χρονολογικό σχεδιάγραμμα απεικονίζονται κάποια από τα πιο σημαντικά γεγονότα και εξελίξεις στο πεδίο της βιομετρίας που συνέβησαν στο πέρας των ετών.



Εικόνα 2.3: Ιστορική αναδρομή σημαντικών εξελίξεις στο χώρο της βιομετρίας

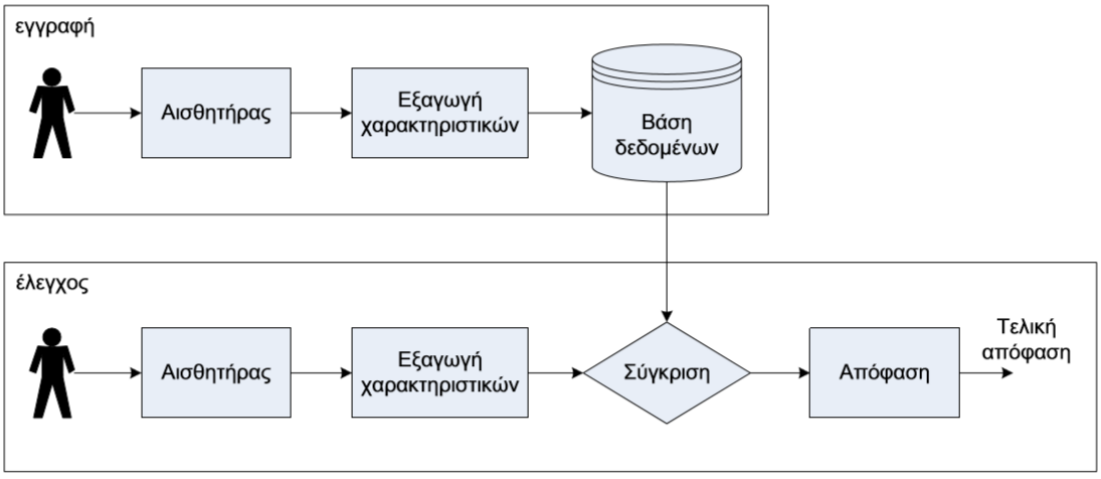
2.2 Αρχιτεκτονική βιομετρικού συστήματος

Ένα βιομετρικό σύστημα στην ουσία είναι ένα σύστημα αναγνώρισης προτύπων, το οποίο αναγνωρίζει ένα φυσικό πρόσωπο καθορίζοντας την αυθεντικότητα του με βάση ένα ή περισσότερα μοναδικά χαρακτηριστικά του. Βιομετρικά χαρακτηριστικά είναι εκείνα τα φυσικά ή συμπεριφοριστικά χαρακτηριστικά, τα οποία μπορούν να χρησιμοποιηθούν για να την αναγνώριση της ταυτότητάς του.



Εικόνα 2.4: Η γενική αρχιτεκτονική ενός βιομετρικού συστήματος [11]

Σε ένα βιομετρικό σύστημα ελέγχου ταυτότητας υπάρχουν δύο βασικά στάδια: το στάδιο της εγγραφής και το στάδιο της εξακρίβωσης/ταυτοποίησης. Στο στάδιο της εγγραφής, λαμβάνονται δείγματα βιομετρικών χαρακτηριστικών, όπως τα δακτυλικά αποτυπώματα και καταχωρούνται στην βάση δεδομένων του συστήματος. (Breebaart J. Et al.,2009). Κατά την διαδικασία της εγγραφής, το βιομετρικό χαρακτηριστικό έπειτα από την αποτύπωση του μέσω ενός αισθητήρα μετατρέπεται σε ψηφιακό σήμα. Εν συνεχεία, γίνεται ένας έλεγχος ποιότητας για να επιβεβαιωθεί ότι το εν λόγο δείγμα του βιομετρικού χαρακτηριστικού είναι κατάλληλο, ώστε να επεξεργαστεί με επιτυχία στα επόμενα στάδια επεξεργασίας. Στο αμέσως επόμενο στάδιο πραγματοποιείται μια προ-επεξεργασία για να βελτιωθούν κάποια χαρακτηριστικά του δείγματος, με σκοπό την επίτευξη μιας καλύτερης εξαγωγής των χαρακτηριστικών αυτών, τα οποία στο στάδιο της σύγκρισης θα αναζητηθούν από την βάση δεδομένων. Με την εξαγωγή κάποιων συγκεκριμένων χαρακτηριστικών αυτό που επιτυγχάνεται είναι η μείωση του χρόνου αναζήτησης από την βάση δεδομένων και η αύξηση της αξιοπιστίας της αναζήτησης. Ακολούθως τα χαρακτηριστικά (templates) που προκύπτουν από το στάδιο εξαγωγής (Feature Extractor) χρησιμοποιούνται για την ανίχνευση, γι’ αυτό το λόγο αποθηκεύονται στη βάση βιομετρικών δεδομένων (System DB) μαζί με το όνομα του ατόμου (Template name) που του αναλογούν αυτά τα χαρακτηριστικά. Στο στάδιο εξακρίβωσης/ταυτοποίησης, ο χρήστης αφού πρώτα εισχωρήσει το όνομά του ή κάποιο κρυφό κωδικό PIN (Personal Identification Number), εν συνεχεία τοποθετεί το βιομετρικό του χαρακτηριστικό. Έπειτα, εάν τα στοιχεία αυτά είναι σωστά, γίνεται σύγκριση μόνο με τα χαρακτηριστικά του αυθεντικού χρήστη που είναι αποθηκευμένα στην βάση δεδομένων του συστήματος. Στην περίπτωση της ταυτοποίησης το σύστημα πραγματοποιεί σύγκριση των χαρακτηριστικών που εξήχθησαν από το βιομετρικό χαρακτηριστικό ενός χρήστη με όλα τα χαρακτηριστικά όλων των χρηστών (N), τα οποία είναι αποθηκευμένα στην βάση του συστήματος, η διαδικασία αυτή γίνεται χωρίς την εισαγωγή κωδικού ή ονόματος. Σε περίπτωση που ο χρήστης εντοπιστεί, η έξοδος του συστήματος ταυτοποίησης θα είναι η ταυτότητα μαζί με το βιομετρικό χαρακτηριστικό που εκχωρήθηκε στην είσοδο του συστήματος. (Joseph Mwema et al., 2015). Σε αντίθετη περίπτωση, θα εμφανιστεί ένα μήνυμα που θα δηλώνει ότι ο χρήστης δεν υπάρχει στην βάση δεδομένων (user not identified).



Εικόνα 2.5: Αρχιτεκτονική εγγραφής και αρχιτεκτονική έλεγχου

Σε γενικές γραμμές, ένα βιομετρικό σύστημα απαρτίζεται από πέντε βασικές μονάδες: τον αισθητήρα, τη μονάδα εξαγωγής χαρακτηριστικών, τη βάση δεδομένων όπου αποθηκεύονται τα βιομετρικά πρότυπα, τη μονάδα σύγκρισης και τη μονάδα απόφασης. (Cavoukian Ann et al.,2016)

Ο αισθητήρας αποτελεί τη διασύνδεση μεταξύ του χρήστη και του βιομετρικού συστήματος και η λειτουργία που επιτελεί είναι η συγκέντρωση των βιομετρικών χαρακτηριστικών του χρήστη. Ακολούθως, η μονάδα εξαγωγής χαρακτηριστικών είναι υπεύθυνη για την επεξεργασία των δεδομένων αυτών, ώστε να υλοποιηθεί η εξαγωγή της πιο χρήσιμης πληροφορίας που θα ξεχωρίζει τους χρήστες μεταξύ τους. Ως επί το πλείστον, δημιουργείται ένα διάνυσμα χαρακτήρων (feature vector) που είναι η βιομετρική υπογραφή του χρήστη. Κατά τη διαδικασία εγγραφής, το σύνολο των χαρακτηριστικών (σύνολο συλλογής) που αντλήθηκαν από τα βιομετρικά δεδομένα συλλέγονται στη βάση δεδομένων του συστήματος και αποτελούν το βιομετρικό πρότυπο του χρήστη. Κατά τη διαδικασία αυθεντικοποίησης συγκεντρώνονται τα καινούργια βιομετρικά στοιχεία του χρήστη και πραγματοποιείται η εξαγωγή ενός νέου συνόλου χαρακτηριστικών που λέγεται σύνολο δοκιμής. Στη μονάδα σύγκρισης συντελείται η σύγκριση του συνόλου συλλογής και του συνόλου δοκιμής βιομετρικών χαρακτηριστικών. (Campisi, P., 2013). Στο τελικό στάδιο βρίσκεται η μονάδα απόφασης, η οποία είναι αρμόδια για τη λήψη της τελικής απόφασης σε σχέση με την ταυτότητα του άτομου. Αναλόγως με την εφαρμογή η λειτουργία που επιτελούν τα βιομετρικά συστήματα μπορεί να διακριθεί σε δυο κατηγορίες: την αυθεντικοποίηση ή πιστοποίηση και την εξακρίβωση ταυτότητας των χρηστών. Συγκεντρωτικά έχουμε τις εξής βασικές μονάδες σε ένα βιομετρικό σύστημα:

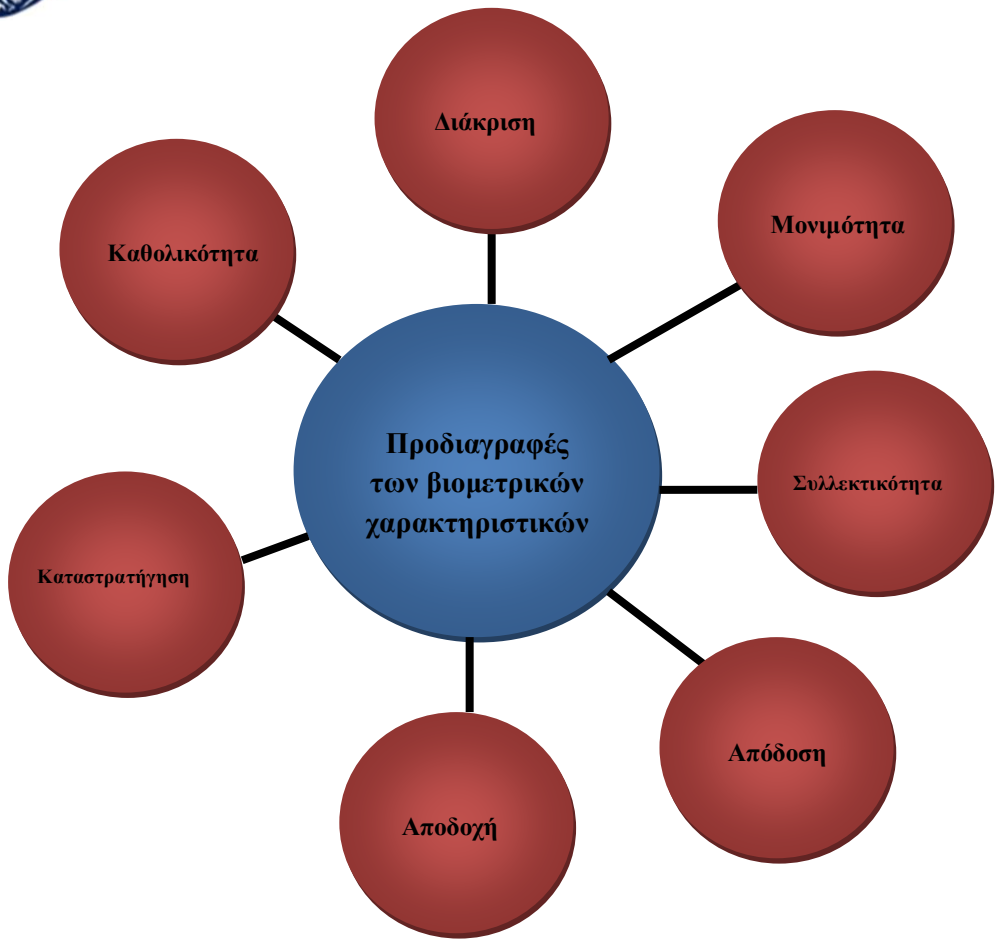
- **Μονάδα αισθητήρα**: Ανάλογα με το δείγμα που θα συλλεχθεί, απαιτείται και ο κατάλληλος βιομετρικός σαρωτής ή αναγνώστης ώστε να ληφθούν ακατέργαστα τα βιομετρικά δεδομένα του ατόμου. Για παράδειγμα για τη λήψη δακτυλικών αποτυπωμάτων χρησιμοποιείται ένας οπτικός αισθητήρας δακτυλικών αποτυπωμάτων που απεικονίζει τη δομή του δακτύλου. (Kenta Takahashi et al., 2011). Η μονάδα αισθητήρα αποτελεί μείζονος σημασίας για την απόδοση του βιομετρικού συστήματος και ως εκ τούτου μια μη επαρκώς σχεδιασμένη μονάδα αισθητήρα έχει μεγάλες πιθανότητες να προκαλέσει αποτυχία στη σωστή λειτουργία του βιομετρικού συστήματος. Πιο συγκεκριμένα, ο ειδικός αισθητήρας (συνήθως σαρωτής ή κάμερα) πραγματοποιεί μετατροπή ενός βιομετρικού χαρακτηριστικού σε κώδικα, τον οποίο αποθηκεύει ως «πρότυπο» και το αντιστοιχεί με ένα συγκεκριμένο φυσικό πρόσωπο. Σε οποιασδήποτε προσπάθεια απόκτησης πρόσβασης αυτού του φυσικού πρόσωπου από εν λόγο σύστημα, πραγματοποιείται έλεγχος της ταυτότητάς του, με σάρωση του βιομετρικού του χαρακτηριστικού, γίνεται ο επαναυπολογισμός του κώδικα και τέλος συγκρίνεται με το ήδη αποθηκευμένο πρότυπο. (Bolle R. M. et al, 2013). Για μεγαλύτερη ασφάλεια, ένα πρότυπο μπορεί να συνδυαστεί με επιπλέον μέτρα ελέγχου πρόσβασης π.χ. κωδικός πρόσβασης (PIN). Αυτό που πρέπει να γίνει κατανοητό είναι ότι το βιομετρικό σύστημα αποθηκεύει το πρότυπο, το οποίο είναι σε ψηφιακή μορφή και όχι την αρχική εικόνα του βιομετρικού χαρακτηριστικού. Ως επί το πλείστον συναντώνται και περιπτώσεις όπου χρησιμοποιούνται και πολλαπλά βιομετρικά συστήματα (multi-biometrics). Ένα πολλαπλό βιομετρικό σύστημα ταυτοποίησης χρησιμοποιεί ένα συνδυασμό δύο ή περισσότερων βιομετρικών μεθόδων, επιτυγχάνοντας έτσι μεγαλύτερη πιστότητα και αξιοπιστία.
- **Μονάδα εξαγωγής χαρακτηριστικών:** Μετά τη συλλογή των βιομετρικών δεδομένων από τον αισθητήρα θα πρέπει να αξιολογηθούν ως προς την ποιότητα τους για να κριθούν εάν είναι κατάλληλα για περαιτέρω επεξεργασία. Στις περισσότερες των περιπτώσεων τα δεδομένα που αποκτήθηκαν εισέρχονται σε αλγόριθμους ενίσχυσης σήματος προκειμένου να βελτιωθεί η ποιότητα τους. Πάραυτα, υπάρχουν περιπτώσεις όπου η ποιότητα των δεδομένων δεν είναι καλή και ο χρήστης πρέπει να ξαναπαρουσιάσει τα βιομετρικά του δεδομένα. Στην συνέχεια, τα βιομετρικά δεδομένα υπόκεινται σε επεξεργασία και γίνεται

εξαγωγή ενός συνόλου χαρακτηριστικών που είναι αντιπροσωπευτικά του υποκείμενου γνωρίσματος. (Breebaart J. Et al.,2009). Για παράδειγμα, σε ένα δακτυλικό αποτύπωμα, η τοποθεσία και η κατεύθυνση των σημείων (κορυφογραμμών και κοιλάδων) εξάγονται από την μονάδα εξαγωγής χαρακτηριστικών σε ένα βιομετρικό σύστημα που έχει σαν βάση τα δακτυλικά αποτυπώματα.

- **Μονάδα σύγκρισης και μονάδα απόφασης:** Εν συνεχεία, πραγματοποιείται σύγκριση ανάμεσα στα εξαγόμενα χαρακτηριστικά και στα αποθηκευμένα πρότυπα και δημιουργούνται βαθμολογίες αντιστοίχησης. Για παράδειγμα, σε ένα βιομετρικό σύστημα βασισμένο σε δακτυλικά αποτυπώματα, γίνεται καθορισμός του αριθμού των αντιστοιχισμένων σημείων μεταξύ του δείγματος εισόδου και των προτύπων και βάση αυτής της σύγκρισης προκύπτει μια βαθμολογία. (Bolle R. M. et al., 2013). Η βαθμολογία μπορεί να επηρεαστεί και από την ποιότητα των βιομετρικών δεδομένων. Επίσης, η μονάδα αυτή ενσωματώνει μία μονάδα απόφασης, στην οποία η βαθμολογία χρησιμοποιείται είτε για να επικυρωθεί μια ταυτότητα, είτε για να καταταχτούν οι εγγεγραμμένες ταυτότητες σε σειρά με σκοπό την εύρεση ενός ατόμου. Όταν λοιπόν ο χρήστης επιχειρήσει να αναγνωριστεί ή να επιβεβαιώσει την ταυτότητα του εκείνη τη δεδομένη στιγμή και αφού ληφθεί το κατάλληλο βιομετρικό χαρακτηριστικό του, γίνεται σύγκριση είτε με όλα τα αποθηκευμένα δείγματα, σε περίπτωση αναγνώρισης, είτε μόνο με το δείγμα της ταυτότητας που διεκδικεί, σε περίπτωση αυθεντικοποίησης. (Joseph Mwema et al., 2015). Η διαδικασία της σύγκρισης των στοιχείων αποτελεί το τελευταίο στάδιο της βιομετρικής αναγνώρισης, στο οποίο λαμβάνεται η απόφαση αν ο χρήστης έχει τα πλήρη δικαιώματα για να προσπελάσει ένα χώρο, υπολογιστικούς πόρους ή οποιαδήποτε άλλη εφαρμογή χρησιμοποιείται μέσω της βιομετρική συσκευής.
- **Μονάδα βάσης δεδομένων συστήματος**: Κατά την διαδικασία της εγγραφής, το σύνολο των χαρακτηριστικών που προκύπτει από την εξαγωγή του ακατέργαστου βιομετρικού δείγματος (δηλαδή του πρότυπου) αποθηκεύεται στην βάση δεδομένων μαζί με κάποιες προσωπικές πληροφορίες (όπως για παράδειγμα όνομα, διεύθυνση, κτλ) που διακρίνουν τον χρήστη.

2.3 Προδιαγραφές βιομετρικών χαρακτηριστικών

Βιομετρικά χαρακτηριστικά θεωρούνται τα χαρακτηριστικά εκείνα που είναι μοναδικά για κάθε άτομο και ως εκ τούτου χρησιμοποιούνται για την ταυτοποίηση του. Τα χαρακτηριστικά αυτά είναι είτε φυσιολογικά χαρακτηριστικά είτε συμπεριφοριστικά γνωρίσματα του ατόμου. Ένα κατάλληλο βιομετρικό δεδομένο θα πρέπει να συμβαδίζει με τις παρακάτω προδιαγραφές:



Εικόνα 2.6: Προδιαγραφές των βιομετρικών χαρακτηριστικών

- **Καθολικότητα:** Αναφέρεται στο κατά πόσο εμφανίζεται το εκάστοτε βιομετρικό χαρακτηριστικό σε κάθε άτομο.
- **Διάκριση:** Αφορά στην ικανότητα του εκάστοτε βιομετρικού χαρακτηριστικού να διακρίνει ένα άτομο από τα υπόλοιπα.
- **Μονιμότητα:** Περιγράφει την δυνατότητα του βιομετρικού χαρακτηριστικού να παραμένει αναλλοίωτο με την πάροδο του χρόνου.
- **Συλλεκτικότητα:**. Αφορά την δυνατότητα απόκτησης και ποσοτικοποίησης του βιομετρικού χαρακτηριστικού.
- **Απόδοση:** Αναφέρεται στη μέτρηση της ακρίβειας, της ταχύτητας και της αξιοπιστίας του συστήματος που συλλέγει τα δεδομένα του βιομετρικού χαρακτηριστικού.
- **Αποδοχή:** Αναφέρεται στο κατά πόσο το ευρύ κοινό αποδέχεται την χρήση ενός συγκεκριμένου βιομετρικού χαρακτηριστικού στην καθημερινότητα τους
- **Καταστρατήγηση:** Περιγράφει το ποσοστό ευκολίας εξαπάτησης του συστήματος αναγνώρισης που χρησιμοποιεί το συγκεκριμένο βιομετρικό χαρακτηριστικό.

Στο παρακάτω πίνακα γίνεται σύγκριση μεταξύ ορισμένων βιομετρικών τεχνολογιών (φυσιολογικών και συμπεριφοριστικών) με βάσει τις παραπάνω προδιαγραφές:

Βιομετρικό σύστημα	Καθολικότητα	Διάκριση	Μονιμότητα	Συλλεκτικότητα	Απόδοση	Αποδοχή	Καταστρατήγηση
Πρόσωπο	Y	X	M	Y	X	Y	Y
Δακτυλικό αποτύπωμα	M	Y	Y	M	Y	M	M
Γεωμετρία χεριού	M	M	M	Y	M	M	M
Μάτι	Y	Y	Y	M	Y	X	X
Υπογραφή	X	X	X	Y	X	Y	Y
Φωνή	M	X	X	M	X	Y	Y

Πίνακας 2.7 : Σύγκριση βιομετρικών τεχνολογιών (Υψηλή, μέτρια και χαμηλή συμβολίζονται με Y, M και X, αντίστοιχα)[50]

Από αυτόν τον πίνακα, μπορούμε να συμπεράνουμε ότι κανένα βιομετρικό σύστημα δεν είναι ιδανικό, καθώς δεν ικανοποιεί ταυτόχρονα όλες αυτές τις ιδιότητες. Πάραυτα, κάθε βιομετρικό σύστημα, σε οποιοδήποτε χαρακτηριστικό και να είναι βασισμένο, έχει τα δικά του δυνατά και αδύνατα σημεία, τα οποία ανάλογα τη περίπτωση το κάνουν εν τέλει αποδεκτό.

2.4 Είδη βιομετρικών συστημάτων

Πλέον, υπάρχει μια πληθώρα βιομετρικών συστημάτων τα όποια χρησιμοποιούνται σε διάφορες εφαρμογές και χώρους για την αυθεντικοποίηση και την ταυτοποίηση των ατόμων. Όπως ήδη προαναφέρθηκε, κανένα βιομετρικό σύστημα δεν είναι ιδανικό όμως το καθένα έχει τα δικά του πλεονεκτήματα και μειονεκτήματα και ανάλογα με αυτά διαφέρει η επιλογή του από εφαρμογή σε εφαρμογή. (Ratha N. K. et. al, 2001)

Εικόνα 2.8: Μέθοδοι βιομετρικής αυθεντικοποίησης-ταυτοποίησης

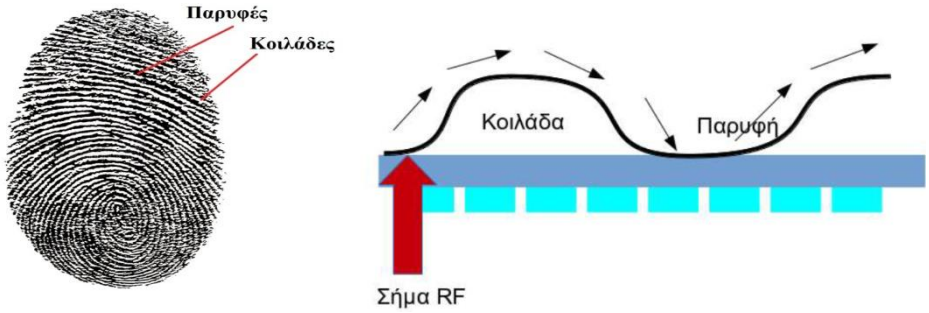
Οι πιο διαδεδομένοι βιομετρικοί τύποι αυθεντικοποίησης είναι οι εξής:

- **Αναγνώριση προσώπου**. Η μέθοδος αυτή εστιάζει στο περίγραμμα του προσώπου και στα μοναδικά χαρακτηριστικά του όπως το σχήμα ματιών, το μέγεθος της μύτης και του στόματος κτλ.
- **Αναγνώριση ίριδας**. Αυτός ο τύπος αυθεντικοποίησης αναγνωρίζει τα μοναδικά μοτίβα της ίριδας του ματιού, και είναι ένας από τους πιο αξιόπιστους τύπους αναγνώρισης.
- **Σάρωση δακτυλικών αποτυπωμάτων**. Αυτή η μέθοδος εστιάζει στις παρυφές και κοιλάδες των δακτυλικών αποτυπωμάτων, τα οποία είναι μοναδικά για κάθε άτομο.
- **Αναγνώριση φωνής**. Σε αυτή την περίπτωση γίνεται εστίαση στα μοναδικά ηχητικά κύματα της φωνής, στον τρόπο που μιλάει το άτομο όπως επίσης και στην έκταση της φωνής.
- **Γεωμετρία χεριών**. Σε αυτή τη μέθοδο λαμβάνεται υπόψη το μήκος, το πλάτος και η επιφάνεια του χεριού καθώς και το ύψος των δακτύλων, η απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων.
- **Χαρακτηριστικά συμπεριφοράς**. Σε αυτό τον τύπο αυθεντικοποίησης λαμβάνονται χαρακτηριστικά όπως ο τρόπος πληκτρολόγησης, υπογραφής, βάδισης, και άλλες παρόμοιες κινήσεις.

Στις επόμενες υποενότητες θα αναλύσουμε κάποιους από τους πιο δημοφιλείς βιομετρικούς τύπους αυθεντικοποίησης.

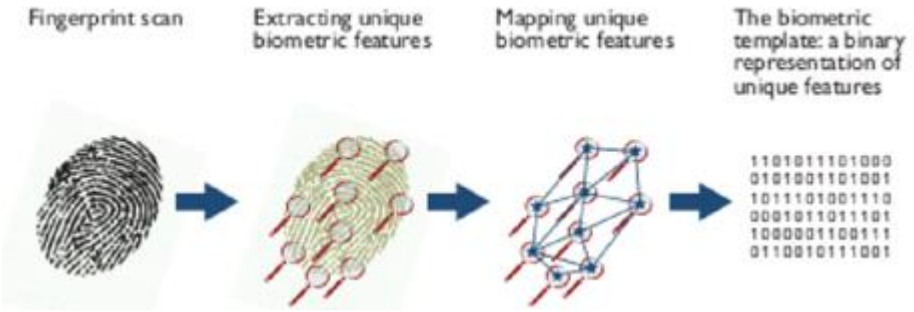
2.4.1 Δακτυλικό αποτύπωμα

Μια από τις πιο γνωστές και αρχαιότερες βιομετρικές μεθόδους ταυτοποίησης είναι το δακτυλικό αποτύπωμα. Ως επί το πλείστον, τα δακτυλικά αποτυπώματα χρησιμοποιούνταν στην εγκληματολογία, όμως λόγο της μεγάλης αποδοχής, της υψηλής ακρίβειας, καθώς και του σχετικά φθηνού κόστους των συστημάτων τους, έγιναν πλέον από τα ευρέως χρησιμοποιούμενα σε πολλές εφαρμογές και τομείς της κοινωνίας. (Manisha et al., 2020).
Αυτό που κάνει αυτή τη μέθοδο ξεχωριστή είναι η μοναδικότητα που χαρακτηρίζει ένα δακτυλικό αποτύπωμα, πιο συγκεκριμένα τα μοτίβα που διέπουν το δακτυλικό αποτύπωμα διαμορφώνονται από γενετικούς και περιβαλλοντικούς παράγοντες και είναι διαφορετικά ακόμη και μεταξύ ομοζυγωτικών διδύμων. (Kamaldeep, 2011). Στη βιομετρική επιστήμη, ένα δακτυλικό αποτύπωμα θεωρείται ως το μοτίβο που σχηματίζεται από τις παρυφές και τις κοιλάδες των δάχτυλων. Όπως φαίνεται στην εικόνα 2.9 οι παρυφές είναι οι μαύρες γραμμές ενώ οι κοιλάδες είναι το άσπρο χώρισμα μεταξύ τους.



Εικόνα 2.9: Δακτυλικό αποτύπωμα [41]

Πριν από περίπου είκοσι χρόνια, τα δακτυλικά αποτυπώματα συλλέγονταν με μελάνι και χαρτί, σήμερα η συλλογή τους πραγματοποιείται μέσω ηλεκτρονικών αισθητήρων τους λεγόμενους σαρωτές δακτυλικών αποτυπωμάτων, οι οποίοι καταγράφουν την ψηφιακή εικόνα του δακτυλικού αποτυπώματος. Οι αισθητήρες αποτελούν το σημαντικότερο μέρος ενός βιομετρικού συστήματος δακτυλικών αποτυπωμάτων, γιατί η ποιότητα του συλλεγόμενου δείγματος καθορίζει σε σημαντικό βαθμό την απόδοση όλου του συστήματος. Οι τεχνολογίες αισθητήρων που εφαρμόζονται στο σαρωτή μπορούν να είναι τεχνολογίες πυριτίου, υπερήχων ή οπτικών οι οποίοι είναι οι περισσότερο χρησιμοποιούμενοι. (Hammad M. et al., 2018). Η ποιότητα της ληφθείσας εικόνας μπορεί να επηρεαστεί από την τεχνολογία του σαρωτή, τις συνθήκες απόκτησης και την κατάσταση του δακτύλου.



Εικόνα 2.10: Διαδικασία δημιουργίας βιομετρικού προτύπου δακτυλικού αποτυπώματος [26]

Όπως διακρίνεται στην εικόνα 2.10, αρχικά, πραγματοποιείται η καταγραφή του δακτυλικού αποτυπώματος από τον σαρωτή ως εικόνα bitmap όπου οι μαύρες περιοχές απεικονίζουν τις παρυφές και οι άσπρες δείχνουν κοιλάδες, και αφού γίνει η βελτιστοποίηση της ποιότητας αυτής της ψηφιοποιημένης εικόνας, γίνεται η προετοιμασία για τη φάση τμηματοποίησης. Η τμηματοποιημένη πλέον εικόνα είναι έτοιμη για τη διαδικασία εξαγωγής χαρακτηριστικών όπου εξάγονται τα εμφανή χαρακτηριστικά που αντιπροσωπεύουν το δείγμα φτάνοντας έτσι στο τελικό στάδιο όπου γίνεται η μετατροπή του σε πρότυπο. Στη διαδικασία εγγραφής, το ληφθέν πρότυπο αποθηκεύεται στη βάση δεδομένων, ενώ στη διαδικασία ταυτοποίησης πραγματοποιείται σύγκριση με κάθε αποθηκευμένο πρότυπο που υπάρχει στη βάση δεδομένων. (Hammad M. et al., 2018). Το αποτέλεσμα της σύγκρισης αυτής είναι μια βαθμολογία που κυμαίνεται μεταξύ 0 και 1, και δείχνει το βαθμό ομοιότητας του δείγματος με το πρότυπο που βρίσκεται στη βάση δεδομένων.

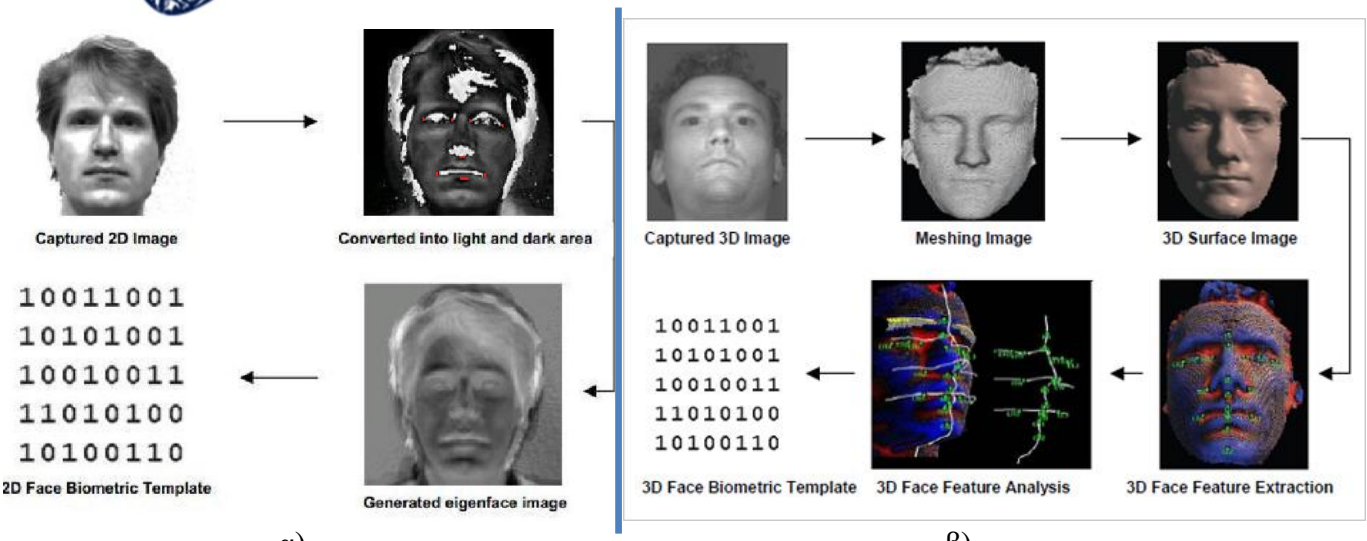
Εικόνα 2.11: Σαρωτής δακτυλικών αποτυπωμάτων (fingerprint scanner) [58]

Κάποια από τα οφέλη των δακτυλικών αποτυπωμάτων περιγράφονται συνοπτικά παρακάτω:

- Είναι αρκετά δύσκολο να πλαστογραφηθεί, εν αντιθέσει με τις αστυνομικές ταυτότητες και τα διαβατήρια.
- Τα δακτυλικά αποτυπώματα είναι φύσει αδύνατο να κλαπούν (σε αντίθεση με τα ψηφιακά τα οποία μπορούν)
- Τα δακτυλικά αποτυπώματα είναι πιο δύσκολο να αντιγραφούν από τις υπόγραφες.

2.4.2 Αναγνώριση προσώπου

Η μέθοδος της αναγνώρισης προσώπου διακρίνεται σε δυο τεχνικές, την δυσδιάστατη αναγνώριση και την τρισδιάστατη. Η τεχνική της δυσδιάστατης αναγνώρισης βασίζεται στη καταγραφή πρόσωπου με βάση το αποχρωματισμό των εικόνων, δηλαδή την εύρεση σκοτεινών και φωτεινών σημείων που επιδεικνύουν τη κοντινή ή μακρινή αντίστοιχα απόσταση από το επίπεδο της κάμερας. Ακολούθως, με τη χρήση ειδικών αλγορίθμων η εικόνα αυτή διαμορφώνεται με βάση τα eigenfaces και δημιουργούνται μοναδικά διανύσματα χαρακτηριστικών γνωρισμάτων του προσώπου (π.χ. η απόσταση μεταξύ ματιών το πλάτος της μύτης, το σχήμα των ματιών, το μήκος του σαγονιού το κτλ), τα οποία υποδεικνύουν την ταυτότητα του ατόμου. (Cavoukian Ann et al.,2016). Η τεχνική αυτή έχει αρκετούς περιορισμούς, καθώς το αποτέλεσμα της ταυτοποίησης επηρεάζεται από τις εκφράσεις του προσώπου τη χρήση καλλυντικών, τον φωτισμό λήψης κτλ. Η τρισδιάστατη αναγνώριση είναι μια παραλλαγή της δισδιάστατης αναγνώρισης, όπου λαμβάνεται η τρισδιάστατη γεωμετρική αναπαράσταση του ανθρώπινου προσώπου. Στην τρισδιάστατη τεχνική, δεν υφίσταται πλέον οι περιορισμοί που υπήρχαν στην δυσδιάστατη τεχνική, καθώς επιτυγχάνονται καλύτερα αποτελέσματα με τη χρήση της γεωμετρίας συμπαγών στοιχείων του προσώπου.



α) β)

Εικόνα 2.12: α) Διαδικασία δημιουργίας βιομετρικού προτύπου αποτυπώματος προσώπου από Δυσδιάστατη εικόνα β) Διαδικασία δημιουργίας βιομετρικού προτύπου αποτυπώματος προσώπου από Τρισδιάστατη εικόνα [26]

Το ψηφιακό πρότυπο που δημιουργείται, χρησιμοποιείται τόσο σε συστήματα ταυτοποίησης, όσο και σε συστήματα αυθεντικοποίησης, και συγκρίνεται σε πραγματικό χρόνο με τα ψηφιακά πρότυπα όλων των χρηστών τα οποία υπάρχουν σε μια βάση δεδομένων που περιέχουν εκατομμύρια πρόσωπα, ώστε να καθοριστεί η ταυτότητά του εκάστοτε χρήστη. (Karthik Nandakumar, 2005). Το λογισμικό που χρησιμοποίει ο εν λόγο βιομετρικός τρόπος αυθεντικοποίησης μπορεί πραγματοποιήσει στιγμιαίους υπολογισμούς των αποτυπωμάτων των προσώπων, είτε μέσω ζωντανού βίντεο είτε μέσω ψηφιακών εικόνων.

Εικόνα 2.13: Ηλεκτρονικός σαρωτής αναγνώρισης προσώπου [59]

Η αναγνώριση προσώπου είναι μια αρκετά ακριβή τεχνολογία, καθώς χρησιμοποιεί μεθοδολογίες και αλγορίθμους νευρολογικών δικτύων και απαιτείται η χρήση κάμερας, η οποία θα λάβει το ηλεκτρονικό αποτύπωμα του προσώπου. (Shinji Hirata et al., 2009). Παρόλα αυτά είναι μια αποδέκτη από το ευρύ κοινό τεχνολογία κερδίζοντας διαρκώς έδαφος σε αρκετούς χώρους που

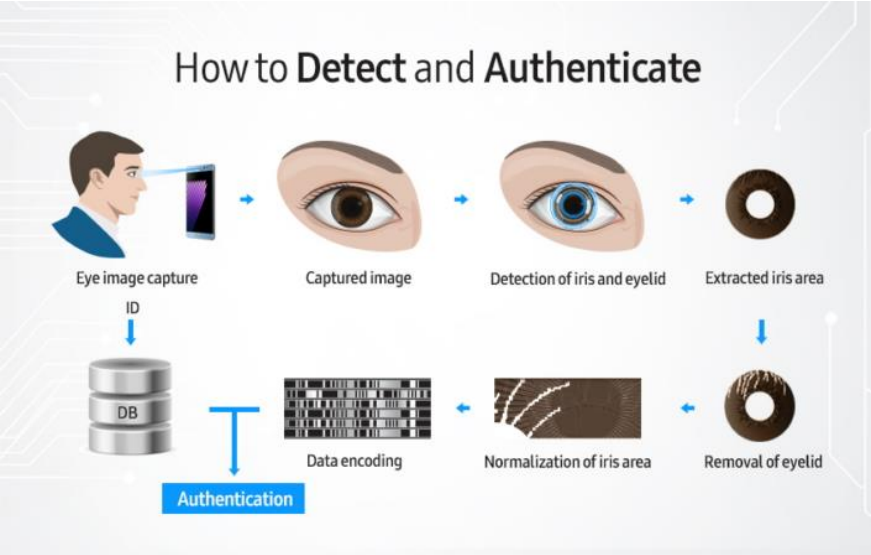
απαιτούν έλεγχο πρόσβασης (όπως τράπεζες, επιχειρήσεις, αεροδρόμια κτλ), έχοντας έτσι μεγάλες μελλοντικές προοπτικές εξέλιξης στο πεδίο της βιομετρικής τεχνολογίας.

2.4.3 Σάρωση ίριδας

Ανάμεσα σε αυτή τη μεγάλη γκάμα βιομετρικών τεχνολογιών, η ίσως πιο διαδεδομένη και ταχέως εξελισσόμενη είναι η αναγνώριση της ίριδας του ματιού. Σύμφωνα με έρευνες που έχουν πραγματοποιηθεί η ανθρώπινη ίριδα διαθέτει περίπου 250 χαρακτηριστικά (όπως νεύρα, ιστούς, κύτταρα κτλ.) όπου καθένα από αυτά είναι μοναδικά σε κάθε άνθρωπο. (Wildes Richard P., 1997). Ο αριθμός αυτών των χαρακτηριστικών είναι δέκα φορές περισσότερος από αυτών που υφίστανται στα δακτυλικά αποτυπώματα. Ως επί το πλείστον, έχει παρατηρηθεί η μοναδικότητα των λεπτομερειών κάθε ίριδας τόσο σε διδύμους όσο και στο ίδιο άτομο, με την ίριδα του δεξιού ματιού να είναι διαφορετική από αυτή του αριστερού ματιού. (Jain K. et al., 2008). Αυτό δείχνει ότι η πιθανότητα το πρότυπο της ίριδας ενός χρήστη να ταιριάζει απόλυτα με το πρότυπο τις ίριδας κάποιου άλλου ατόμου είναι μηδαμινή.

Η ίριδα ως βιομετρικό χαρακτηριστικό διαθέτει αρκετά πλεονεκτήματα σε σχέση με τα υπόλοιπα βιομετρικά χαρακτηριστικά. Κάποια πλεονεκτήματα είναι τα εξής :

- Η δυνατότητα συλλογής δείγματος χωρίς φυσική επαφή
- Η σταθερότητα των χαρακτηριστικών γνωρισμάτων στο πέρας της ζωής του ατόμου
- Το γεγονός ότι δεν μπορεί να γίνει αντιγραφή ούτε κλοπή από κάποιον άλλο χρήστη
- Τα μηχανήματα ανάγνωσης ίριδας δεν μπορούν να εξαπατηθούν από χρήση καλλυντικών στο δέρμα, αλλαγή χτενίσματος ή άλλου είδους μεταμφίεσης



Εικόνα 2.14: Διαδικασία εύρεσης και αυθεντικοποίησης βιομετρικού προτύπου ίριδας [62]

Το όλο σύστημα ονομάζεται Iris Recognition System (IRS) και αναγνωρίζει εάν ένας χρήστης είναι πραγματικά αυτός που ισχυρίζεται, παίρνοντας μια στατική εικόνα από το μάτι του. Το σύστημα

IRS αποτελείται από την μονάδα οπτικής αναγνώρισης, την μονάδα ελέγχου της κάμερας, καθώς και μια βάση δεδομένων. Η διαδικασία οπτικής αναγνώρισης ξεκινάει όταν το μάτι ενός ανθρώπου πλησιάσει κοντά στο φακό της οπτικής κάμερας και ο φακός της κάμερας εστιάσει στην περιοχή της ίριδάς του. Ακολούθως, ο μηχανισμός της κάμερας θα πραγματοποιήσει λήψη μιας φωτογραφία (snapshot) και θα γίνει η επεξεργασία αυτής της εικόνας από τη μονάδα ελέγχου της κάμερας. Εν συνεχεία, το σύστημα θα αναλύσει την εικόνα του μοτίβου της ίριδας και παράξει έναν κώδικα μήκους 512 bytes που ονομάζεται κώδικας ίριδας (IrisCode). (Kamaldeep.,2011). Μόλις ολοκληρωθεί αυτή η διαδικασία, η μονάδα ελέγχου της κάμερας επικοινωνεί με την βάση δεδομένων, η οποία στη πορεία θα συγκρίνει ένα προς ένα τα bit του κωδικού με όλων αυτών που βρίσκονται αποθηκευμένα στη βάση δεδομένων. Αν ο χρήστης εντοπιστεί στην βάση δεδομένων, τότε η αναγνώριση πραγματοποιείται και επιβεβαιώνεται η ταυτότητα του.

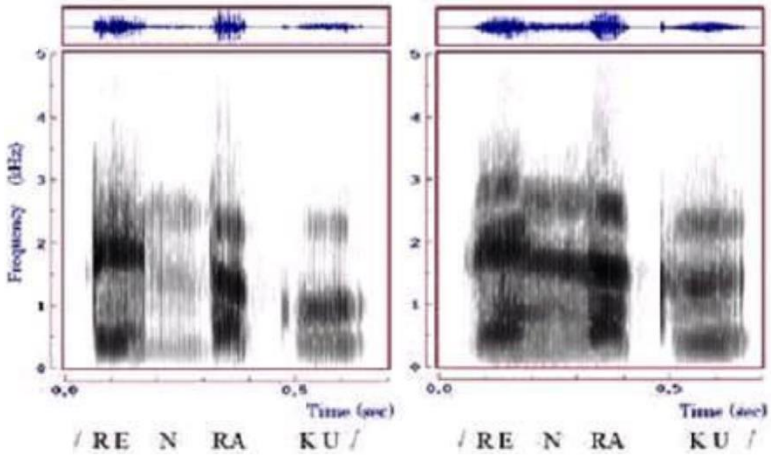
Εικόνα 2.15: Ηλεκτρονικός σαρωτής αναγνώρισης ίριδας [60]

2.4.4 Αναγνώριση φωνής

Η μέθοδος αυτή αναγνωρίζει τα ηχητικά σήματα που παράγουν οι χρήστες με τη φωνή τους. Το αρχικό στάδιο για την αναγνώριση φωνής είναι να γίνει παραγωγή ενός δείγματος φωνής το οποίο σε περίπτωση εγγραφής του χρήστη θα είναι η αναφορά ταυτότητας ενώ σε περίπτωση ταυτοποίησης θα γίνει έλεγχος με τα δείγματα που είναι ήδη κατοχυρωμένα στη βάση δεδομένων. (Padma Polash Paul et. al., 2012). Βέβαια υπάρχον δυο τρόποι που μπορεί να πραγματοποιηθεί η αναγνώριση της φωνής, η εξαρτώμενη σε κάποια λέξη-φράση, και η ανεξάρτητη λέξεων ή φράσεων. Στο πρώτο τρόπο ζητείται από τον χρήστη να επαναλάβει κάποια συγκεκριμένη λέξη ή φράση ή μια σειρά αριθμών, η οποία θα είναι ίδια με αυτή που έδωσε κατά την εγγραφή. Στο δεύτερο τρόπο ζητείται από το χρήστη να αρθρώσει οποιαδήποτε λέξη ή φράση ή μια σειρά αριθμών κατά βούληση ώστε να ληφθούν τα ηχητικά σήματα που θα παράξει η φωνή του. Το δείγμα αυτό, είτε του πρώτου είτε του δεύτερου τρόπου αποτελεί τη βιομετρική αναφορά, η οποία θα μετατραπεί σε ψηφιακή μορφή και στη συνέχεια αφού επεξεργαστεί θα δημιουργηθεί το πρότυπο. Τέλος, με βάση ένα κατώφλι που έχει οριστεί από το σύστημα προκύπτει το αποτέλεσμα της βαθμολογίας σύγκρισης και ανάλογα με αυτό πραγματοποιείται η πιστοποίηση ή όχι του ατόμου. (Kenta Takahashi et al., 2011).

Εικόνα 2.16: Ηχητικά σήματα της φωνής [61]

Για τον καταγραφή των σημάτων της φωνής θα πρέπει να εντοπίζονται κάποια μοναδικά στοιχεία που τη χαρακτηρίζουν όπως ο τόνος, η ένταση της και άλλοι παράγοντες όπως το μέγεθος στόματος, του λάρυγγα, της μύτης κτλ. Ως αποτέλεσμα δημιουργείται ένα φωνητικό πρότυπο που αναλύεται με ένα φασματογράφημα, το οποίο εμφανίζει τη χρονική διάρκεια, τη συχνότητα των δονήσεων των χορδών της φωνής και το εύρος έντασης της. Τα πλεονεκτήματα του βιομετρικού αυτού χαρακτηριστικού είναι η ευρεία αποδοχή από τους χρήστες, το μικρό μέγεθος της κάθε εγγραφής στη βάση δεδομένων, η υψηλή ταχύτητα του συστήματος και η δυνατότητα για πιστοποίηση από απόσταση. (Georgios Goudelis et al., 2008). Φυσικά υπάρχουν και αρκετά μειονεκτήματα αυτού του βιομετρικού χαρακτηριστικού, τα οποία το κατατάσσουν χαμηλά σε προτίμηση σε σχέση με άλλες μεθόδους. Ένα βασικό μειονέκτημα είναι ότι λόγο εξωτερικών παραγόντων όπως θόρυβος, αλλοιωμένη φωνή λόγο ασθένειας, ηλικίας κτλ. υπάρχει δυσκολία στη σωστή λήψη του δείγματος Το πρόβλημα αυτό δημιουργεί αλλοίωση του δείγματος και κατά συνέπεια μη ακρίβεια του αποτελέσματος. (Campisi, P., 2013). Ως επί το πλείστον, το σύστημα είναι επιρρεπή σε εισβολείς που επιχειρούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση προκαλώντας απομιμήσεις ή κλωνοποίηση της φωνής μέσω αναπαραγωγής κάποιου ηχογραφημένου μηνύματος του εξουσιοδοτημένου χρηστή. Αυτός είναι και ο βασικός λόγος που δεν χρησιμοποιούνται αποκλειστικά και μόνο τα χαρακτηριστικά φωνής σε ένα σύστημα ταυτοποίησης, αλλά σε συνδυασμό της με κάποια άλλη βιομετρική μέθοδο όπως η αναγνώριση μέσω ίριδας, πρόσωπου κλπ.



Εικόνα 2.17: Αναπαράσταση αποτυπωμάτων φωνής της ίδιας φράσης από δυο άτομα [26]

2.5 Παραδείγματα χρήσης βιομετρικών συστημάτων

Ο βασικός σκοπός που χρησιμοποιούνται τα βιομετρικά χαρακτηριστικά είναι για τη δημιουργία ενός επίπεδου ασφάλειας και προστασίας εναντίων πλαστών και ψεύτικων εγγράφων. (Kresimir Delac et al., 2004). Τα βιομετρικά συστήματα πλέον χρησιμοποιούνται αρκετά, ακόμη και στην καθημερινότητα μας, με τη χρήση τους να εφαρμόζεται σε κινητά υπολογιστές, τράπεζες, δίκτυα κτλ. Οι κύριες περιοχές όπου χρησιμοποιούνται τα βιομετρικά συστήματα για την ταυτοποίηση και την αυθεντικοποίηση των ατόμων είναι οι παρακάτω:

- Στην εγκληματολογία για τον εντοπισμό δραστών
- Στον τουρισμό και τον συνοριακό έλεγχο (βιομετρικά διαβατήρια-ταυτότητες)
- Στον έλεγχο πρόσβασης σε φυσικούς χώρους
- Σε συστήματα παρακολούθησης
- Στη προστασία προσωπικών δεδομένων
- Σε ηλεκτρονικές τραπεζικές συναλλαγές

Παρακάτω θα αναλυθούν κάποια παραδείγματα βιομετρικών μέσων και συστημάτων που χρησιμοποιούνται στη καθημερινή μας ζωή.

- Το βιομετρικό διαβατήριο όπως και η βιομετρική ταυτότητα είναι ένα ηλεκτρονικό έγγραφο, το οποίο χρησιμοποιεί τα βιομετρικά χαρακτηριστικά προκειμένου να πιστοποιήσει την ταυτότητα των κατόχων του. Τα στοιχεία αποθηκεύονται σε ένα μικροσκοπικό τσιπ, προκειμένου να εξασφαλιστεί η ακεραιότητα του διαβατηρίου καθώς και των βιομετρικών δεδομένων του.
- Το AFIS (Automated Fingerprint Identification System) είναι ένα αυτοματοποιημένο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων που χρησιμοποιούν οι αστυνομικές αρχές παγκοσμίως για να εντοπίζουν εγκληματίες μέσω των δακτυλικών τους αποτυπωμάτων.
- Οι τράπεζες πλέον έχουν θεσπίσει τη χρήση βιομετρικών συστημάτων στα ATM, το internet banking κτλ για την έγκυρη πιστοποίηση των χρηστών.
- Τα υπολογιστικά συστήματα είναι αρκετά ευάλωτα σε επιθέσεις, έτσι κρίνεται απαραίτητη η διαφύλαξη ευαίσθητων προσωπικών δεδομένων όπως ο αριθμός πιστωτικής κάρτας, τα ιατρικά δεδομένα, τραπεζικά δεδομένα κ.ά.
- Το σύστηνα IRIS βρίσκει εφαρμογή σε χώρους όπως τα αεροδρόμια και γενικά σε κτήρια υψίστης ασφαλείας όπου είναι απαραίτητος ο έλεγχος πρόσβασης των ατόμων.

Εικόνα 2.18: Μέρη που εφαρμόζονται τα βιομετρικά συστήματα

2.6 Απόδοση των βιομετρικών συστημάτων

Ένα σημαντικό κριτήριο με το οποίο αξιολογείται εάν ένα βιομετρικό σύστημα είναι κατάλληλο και αξιόπιστο είναι η απόδοση αυτού του συστήματος. Για τον υπολογισμό της απόδοσης ενός βιομετρικού συστήματος πιστοποίησης έχουν δημιουργηθεί κάποιοι δείκτες με τους όποιους μετράται η επίδοση του με ποσοστά.

Οι κατά κόρον χρησιμοποιούμενοι δείκτες της απόδοσης των βιομετρικών μεθόδων είναι:

• **Το ποσοστό των λανθασμένων απορρίψεων, FRR (False Rejection Rate)**, δηλαδή ο αριθμός των περιπτώσεων όπου δεν παραχωρήθηκε πρόσβαση σε εξουσιοδοτημένους χρήστες ενώ το βιομετρικό τους χαρακτηριστικό υπήρχε καταχωρημένο στη βάση δεδομένων.

• **Το ποσοστό των λανθασμένων αποδοχών, FAR (False Acceptance Rate)**, δηλαδή ο αριθμός των περιπτώσεων όπου παραχωρήθηκε πρόσβαση σε μη εξουσιοδοτημένους χρήστες ενώ τα βιομετρικά τους στοιχεία δεν είναι καταχωρημένα στη βάση δεδομένων.

Αυτοί οι δύο δείκτες είναι αλληλοεξαρτώμενοι, καθώς όταν αυξάνεται ο ένας, υπάρχει μείωση του άλλου. (Rodwell P. et. al., 2007). Φυσικά, στην περίπτωση που το σύστημα γίνει αρκετά τυπικό ώστε να έχει μηδαμινό ποσοστό των λανθασμένων αποδοχών, τότε ακόμη και οι πραγματικοί χρήστες θα δυσκολεύονται να αποκτήσουν πρόσβαση σε αυτό με αποτέλεσμα να υπάρξει αύξηση του ποσοστού των λανθασμένων απορρίψεων. Από την άλλη βέβαια, εάν το σύστημα γίνει πολύ φιλικό θα μπορούσε ο καθένας να αποκτήσει εύκολα πρόσβαση σε πόρους του. Ανάλογα το είδος και το σκοπό της εκάστοτε εφαρμογής, δίνεται μεγαλύτερη ή μικρότερη έμφαση στον κάθε δείκτη απόδοσης και με βάση αυτούς τους δείκτες σχεδιάζονται αντίστοιχα βιομετρικά συστήματα.

	Αποδοχή	Άρνηση
Νόμιμη προσπάθεια	True Positive (TP)	False Negative (FN)
Παράνομη προσπάθεια	False Positive (FP)	True Negative (TN)

Πίνακας 2.19: Συμβολισμοί νόμιμης και παράνομης προσπάθειας πρόσβασης σε ένα σύστημα

FRR: Ποσοστό νόμιμων προσπαθειών που απορρίπτονται

$$FRR=\frac{FN}{TP+FN}$$

FAR: Ποσοστό παράνομων προσπαθειών που γίνονται αποδεκτές

$$FAR=\frac{FP}{FP+TN}$$

Επίσης εξίσου σημαντικοί δείκτες μέτρησης της απόδοσης είναι οι εξής ακόλουθοι:

Equal error rate (EER): Ο δείκτης αυτός εμφανίζεται όταν τα ποσοστά FAR και FRR είναι ίσα. Κατά κύριο λόγο, χρησιμοποιείται ως αναφορά σύγκρισης μεταξύ διαφορετικών συστημάτων βιομετρίας. Ως εκ τούτου, το βιομετρικό σύστημα που έχει μικρό δείκτη EER έχει πιο ακριβή και αξιόπιστα αποτελέσματα.

Failure to capture rate (FTC): Ο δείκτης αυτός δείχνει το βαθμό αδυναμίας ενός συστήματος να εντοπίσει ένα βιομετρικό χαρακτηριστικό, ακόμα κι αν αυτό είναι σωστό. Σε περιπτώσεις λάθους απόρριψης ο χρήστης θα πρέπει να ξαναδοκιμάσει να αποκτήσει πρόσβαση στο σύστημα. Επομένως, ένας μεγάλος αριθμός λάθος απορρίψεων, έχει ως αποτέλεσμα απώλεια χρόνου και κατά συνεπεία την πρόκληση εκνευρισμού στο χρήστη.

Failure to enroll rate (FTE): Ο δείκτης αποτυχίας εγγραφής δείχνει το ποσοστό αδυναμίας του βιομετρικού συστήματος να εξάγει χαρακτηριστικά από το δείγμα κατά τη διάρκεια της διαδικασίας εγγραφής του χρήστη σε αυτό. Εν ολίγης, προσδιορίζει το βαθμό ανικανότητας του συστήματος να προβεί σε δημιουργία πρότυπου εγγραφής για έναν νέο χρήστη. Οι βασικοί λόγοι για τους οποίους το σύστημα συνήθως αποτυγχάνει να εντοπίσει το αποκτηθέν βιομετρικό δείγμα είναι λόγο κακής ποιότητας του βιομετρικού χαρακτηριστικού (όπως για παράδειγμα ασθενών γνωρισμάτων λόγω της ένδυσης, απότομης κίνησης των χρηστών κτλ).

Failure to acquire rate (FTA): Ο δείκτης αποτυχίας απόκτησης δείχνει το ποσοστό αδυναμίας του βιομετρικού συστήματος να προβεί στην καταγραφή ή τον εντοπισμό ενός δείγματος ικανοποιητικής ποιότητας. Ο κύριος λόγος που συμβαίνει αυτό είναι το γεγονός ότι το απαιτούμενο βιομετρικό χαρακτηριστικό δεν δύναται να συλλεχθεί λόγω λόγο βλάβης του συστήματος εντοπισμού ή προσωρινού τραυματισμού του χρήστη.

Εικόνα 2.20: Τυπική πορεία FAR και FRR ενός βιομετρικού συστήματος [66]

2.7 Πλεονεκτήματα και μειονεκτήματα των βιομετρικών συστημάτων

Αφού έχουμε αναλύσει στις προηγούμενες ενότητες, τον τρόπο λειτουργίας της βιομετρικής τεχνολογίας μπορούμε πλέον να κάνουμε μια καταγραφή των θετικών και των αρνητικών στοιχείων που προκύπτουν από τη χρήσης της. Παρακάτω θα ακολουθήσουν ενδεικτικά πλεονεκτήματα και μειονεκτήματα διάφορων βιομετρικών συστημάτων ασφαλείας.

2.7.1 Πλεονεκτήματα βιομετρικών συστημάτων

Παρατηρούνται αρκετά πλεονεκτήματα από τη χρήση των βιομετρικών μεθόδων πρόσβασης, κάποια από αυτά είναι η μεγάλη ασφάλεια, η διευκόλυνση των χρηστών, ο περιορισμός της εξαπάτησης, κτλ. Η βιομετρία επίσης, έχει τη δυνατότητα να προσφέρει αυξημένη βεβαιότητα για την ταυτότητα ενός ατόμου, πράγμα που σημαίνει εγγύηση, αξιοπιστία, και ακρίβεια. Ένα άλλο σημαντικό όφελος, αποτελεί το γεγονός ότι τα βιομετρικά χαρακτηριστικά είναι μόνιμα, δε μπορούν να χαθούν ή να ξεχαστούν και είναι πολύ δύσκολη η αντιγραφή τους. (Goudelis et al., 2008). Ακόμη ένα βασικό πλεονέκτημα της χρήσης των βιομετρικών χαρακτηριστικών, που τους κάνει να υπερτερούν σε σχέση με τους παραδοσιακούς κωδικούς αποτελεί η ευκολία στη χρήσης τους καθώς δεν απαιτούν την απομνημόνευση κωδικών πρόσβασης. Συγκεντρωτικά έχουμε τα έξης πλεονεκτήματα:

- Η αναγνώριση πραγματοποιείται με φυσικά ή συμπεριφοριστικά χαρακτηριστικά με αποτέλεσμα να μην είναι απαραίτητη η ύπαρξη ελεγκτή-διαχειριστή για να ενημερώνει το σύστημα.
- Δεν υπάρχει απαίτηση για χρήση κάρτας, ή συνθηματικού πρόσβασης
- Δεν υπάρχει πιθανότητα να χαθούν ή να κλαπούν
- Είναι μόνιμα και δεν αλλάζουν με τη πάροδο του χρόνου
- Είναι μονίμως διαθέσιμα προς χρήση
- Προσφέρουν μεγάλο βαθμό εγκυρότητας ως προς την ταυτότητα του χρήστη
- Χαμηλό κόστος προμήθειας και συντήρησης.
- Χαμηλοί χρόνοι απόκρισης.

2.7.2 Μειονεκτήματα βιομετρικών συστημάτων

Τα συστήματα βιομετρίας παρά την υψηλή ασφάλεια, δεν είναι τέλεια, παρουσιάζουν ορισμένα μειονεκτήματα όπως η διατήρηση μεγάλων βάσεων δεδομένων, οι υψηλές απαιτήσεις συντήρησης, η χρονοβόρα καταχώρηση, οι διάφορες κοινωνικές αντιλήψεις κτλ. Αρκετές βιομετρικές τεχνολογίες, με εξαίρεση την ταυτοποίηση DNA, αποκλείουν ορισμένους ανθρώπους λόγω κάποιων χαρακτηριστικών τους, να χρησιμοποιήσουν τα βιομετρικά συστήματα. (Karthik Nandakumar, 2005). Για παράδειγμα, αρκετοί τυφλοί είναι φύσει αδύνατον να χρησιμοποιήσουν τον σαρωτή ίριδας. Λόγο παρόμοιων περιορισμών τα συστήματα βιομετρίας που χρησιμοποιούνται από μεγάλη μερίδα πληθυσμού οφείλουν να εγκαθιστούν και επιπλέον εφεδρικούς τρόπους αναγνώρισης. Ένα ακόμη αρνητικό στοιχείο αφορά στο γεγονός ότι τα δείγματα των βιομετρικών χαρακτηριστικών που σαρώνονται πρέπει να είναι ευδιάκριτα, ειδάλλως υπάρχει η πιθανότητα λάθους από το σύστημα, μειώνοντας έτσι την αξιοπιστία του. Επιπλέον, οι εκτενείς διαδικασίες καταχώρησης και το μεγάλο ποσοστό απόρριψης ενδέχεται να προκαλέσουν την έντονη δυσαρέσκεια του χρήστη. Εν τέλει, στα μειονέκτημα πρέπει να αναφερθεί η εφεκτικότητα πολλών ανθρώπων να κάνουν χρήση των εν λόγο τεχνολογιών, εξαιτίας διαφόρων κοινωνικών πεποιθήσεων που επικρατούν, όπως ότι η εκπεμπόμενη ακτινοβολία αυτών των μεθόδων έχει αρνητικό αντίκτυπο στην υγεία.

Συγκεντρωτικά έχουμε τα έξης μειονεκτήματα:

- Η αντίληψη των χρηστών ότι η λήψη δακτυλικού αποτυπώματος συνάδει και με διάπραξη εγκληματικής ενέργειας.
- Η αντίληψη των χρηστών ότι η εκπεμπόμενη ακτινοβολία μεθόδων έχει αρνητικό αντίκτυπο στην υγεία.
- Η αντίληψη άρσης της ιδιωτικότητας
- Η αξιοπιστία και η ακρίβεια επιδέχεται βελτίωσης
- Η διατήρηση μεγάλων βάσεων δεδομένων
- Οι υψηλές απαιτήσεις συντήρησης και η χρονοβόρα καταχώρηση
- Τα βιομετρικά συστήματα αποκλείουν ορισμένους ανθρώπους λόγω κάποιων χαρακτηριστικών τους

2.8 Νομικό πλαίσιο

Όσον αφόρα το νομικό πλαίσιο που διέπει τη χρήση βιομετρικών μεθόδων κατά την είσοδο σε εργασιακούς χώρους, η αρχή προστασίας προσωπικών δεδομένων έχει εκδώσει επίσημη απόφαση ότι, ειδικά κάποιες μέθοδοι από αυτές, προσβάλουν ολοφάνερα την ανθρώπινη προσωπικότητα. Από την αρχή της αναλογικότητας, όπως αυτή προβλέπεται στο άρθρο 4 του ν.2472/97, η χρήση βιομετρικών τεχνολογιών για τη επαλήθευση της ταυτότητας των εργαζομένων κατά την εισχώρηση τους σε διάφορους χώρους εργασίας επιτρέπεται αποκλειστικά σε περιπτώσεις που είναι απαραίτητη η προστασία των χώρων εργασίας (όπως σε εγκαταστάσεις του στρατού, σε εργαστήρια υγειονομικού ενδιαφέροντος κτλ) και εφόσον δεν υφίσταται άλλος τρόπος για την εκπλήρωση του σκοπού αυτού. Ως εκ τούτου, ο υπεύθυνος επεξεργασίας αφενός πρέπει να έχει επίγνωση των υπαρχόντων κινδύνων, καθώς και των διαφορετικών δυνατοτήτων αντιμετώπισής τους και αφετέρου, των προσβολών της ιδιωτικότητας και της ανθρώπινης προσωπικότητας από τη χρήση τέτοιων τεχνολογιών. Το είδος των πληροφοριών, ο σκοπός, ο τρόπος συλλογής και

αποθήκευσης, τα μέτρα ασφάλειας αποτελούν στοιχεία τα οποία ελέγχονται πριν αποφανθεί η Αρχή Προστασίας Προσωπικών Δεδομένων για τη νομιμότητα της εν λόγο επεξεργασίας. Επίσης, σε κάθε νόμιμη εφαρμογή ο υπεύθυνος της επεξεργασίας σύμφωνα με το άρθρο 11 του ν.2472/1997 οφείλει να ενημερώνει το υποκείμενο των δεδομένων για το συγκεκριμένο σύστημα, τον σκοπό, τους αποδέκτες και το μέγεθος της επεξεργασίας. Η επεξεργασία βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου απαγορεύεται, εξαιρουμένων ειδικών περιπτώσεων (π.χ. όταν έχετε δοθεί η πλήρη συγκατάθεσή του υποκειμένου ή όταν η επεξεργασία απαιτείται για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει της νομοθεσίας της ΕΕ ή της εθνικής νομοθεσίας) (άρθρο 9 § 1 του ΓΚΠΔ). Επιπλέον, δεν πρέπει να γίνεται συλλογή περισσοτέρων πληροφοριών από όσες είναι απαραίτητες για τη ταυτοποίηση των ατόμων. Τέλος, είναι πολύ σημαντικό ο υπεύθυνος της επεξεργασίας να έχει πάρει τα αντίστοιχα μέτρα ασφάλειας, σύμφωνα με το άρθρο 10 του ν.2472/1997, ώστε να μην υπάρχει δυνατότητα τα δεδομένα να χρησιμοποιηθούν από τρίτους για άλλο σκοπό. Εν ολίγοις επειδή η χρήση των βιομετρικών συστημάτων ικανοποιεί υψηλές απαιτήσεις ασφάλειας στον έλεγχο πρόσβασης (ταυτοποίηση/ αυθεντικοποίηση) σε φυσικούς χώρους ή υπολογιστικά συστήματα υφίστανται περιπτώσεις όπου, υπάρχει δυνατότητα να ξεπερνιούνται οι ενδεχόμενοι κίνδυνοι από πλευράς προστασίας προσωπικών δεδομένων σύμφωνα με την αρχή της αναλογικότητας.

3. Ασφάλεια βιομετρικών συστημάτων

3.1 Απαιτήσεις ασφάλειας

Η ασφάλεια των βιομετρικών συστημάτων σχετίζεται με τα τεχνικά χαρακτηριστικά του συστήματος και τη συνολική ανθεκτικότητά του έναντι των τρωτών σημείων. Ο σχεδιασμός των τεχνικών ασφάλειας ενός βιομετρικού συστήματος περιστρέφεται γύρω από πολλές θεμελιώδεις απαιτήσεις που παρουσιάζονται παρακάτω.

- **Διαθεσιμότητα:** Η απαίτηση αναφέρεται στους μηχανισμούς και τους ελέγχους ασφαλείας που πρέπει να καθοριστούν προκειμένου να διασφαλιστεί ότι κάθε τμήμα του συστήματος θα λειτουργεί σωστά και θα είναι διαθέσιμο όταν αυτό είναι απαραίτητο με αποτέλεσμα την προστασία του συστήματος από τυχαίες βλάβες και φυσικές ή δικτυακές επιθέσεις.
- **Αυθεντικότητα οντότητας:** Αυτή η απαίτηση διασφαλίζει ότι όλες οι οντότητες που εμπλέκονται στην επεξεργασία είναι αυτές που ισχυρίζονται ότι είναι.
- **Αυθεντικότητα δεδομένων:** Αυτή η απαίτηση περιλαμβάνει την αυθεντικότητα της προέλευσης των δεδομένων και την ακεραιότητα των δεδομένων. Η προέλευση των δεδομένων διασφαλίζει τη γνησιότητα και την πρωτοτυπία των βιομετρικών στοιχείων. Η ακεραιότητα των δεδομένων είναι η προϋπόθεση που εγγυάται ότι τα δεδομένα είναι συνεπή, ακριβή και σωστά. Τα μέτρα ασφαλείας που προσφέρουν ακεραιότητα μπορούν επίσης να διασφαλίσουν ότι οι τροποποιήσεις είναι ανιχνεύσιμες σε όλα τα στοιχεία λογισμικού και υλικού που περιλαμβάνονται στο βιομετρικό σύστημα.
- **Εμπιστευτικότητα:** Η εμπιστευτικότητα διασφαλίζει ότι δεν θα αποκαλυφθούν πληροφορίες σχετικά με τα αποθηκευμένα και μεταδιδόμενα δεδομένα του συστήματος. Για ένα βιομετρικό σύστημα, αυτό σημαίνει ότι τα αποθηκευμένα πρότυπα και η μετάδοση τους μεταξύ των σταδίων του συστήματος θα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και τροποποίηση. Αυτό μπορεί να επιτευχθεί μέσω μηχανισμών ελέγχου πρόσβασης και διαφόρων τεχνικών κρυπτογράφησης.

- **Μη αποποίηση:** Αυτή η απαίτηση εγγυάται ότι τα εμπλεκόμενα μέρη σε ένα βιομετρικό σύστημα, συμπεριλαμβανομένου του χρήστη, δεν μπορούν να αρνηθούν ότι έχουν πραγματοποιήσει μια συγκεκριμένη ενέργεια. Επίσης, παρέχει στοιχεία για τις οντότητες και τα στοιχεία που έλαβαν χώρα σε μια ενέργεια και για τα μηνύματα που έχουν σταλεί. Όπως περιγράφεται παρακάτω, σχετίζεται με πολλές αρχές απορρήτου προκειμένου να διασφαλιστεί η αξιοπιστία της διαδικασίας αναγνώρισης και της βιομετρικής αρχιτεκτονικής.
- **Μη αντιστρεψιμότητα:** Η ιδιότητα αναφέρεται στην εφαρμογή μονόδρομων λειτουργιών για τη δημιουργία ενός ασφαλούς προτύπου με τις βιομετρικές αναφορές του χρήστη, έτσι ώστε η γνώση των μετασχηματισμένων βιομετρικών στοιχείων να μην μπορεί να χρησιμοποιηθεί για τη λήψη πληροφοριών σχετικά με την αρχική βιομετρική είσοδο.
- **Δυνατότητα Αποσύνδεσης:** Αυτή η ιδιότητα υποδεικνύει ότι πολλές βιομετρικές αναφορές (μετασχηματισμένα πρότυπα) από τον ίδιο χρήστη δεν μπορούν να συνδεθούν μεταξύ τους ή με τον χρήστη από τον οποίο προήλθαν. Επίσης σχετίζεται με τις οντότητες που εμπλέκονται στη διαδικασία αντιστοίχισης. Αυτό σημαίνει ότι σε ένα μη αποσυνδεόμενο βιομετρικό σύστημα, δεν θα πρέπει να είναι δυνατόν να αντληθούν περαιτέρω πληροφορίες σχετικά με τη σχέση μεταξύ των μερών.
- **Μονιμότητα:** Προσδιορίζει την περίοδο ισχύος που αντιστοιχεί σε ένα σύνολο αποθηκευμένων προτύπων και προστατευμένων αναφορών ταυτότητας.
- **Δυνατότητα ακύρωσης:** Σε περίπτωση που τα μέτρα ασφαλείας εντοπίσουν επιθέσεις στο βιομετρικό σύστημα, ο κίνδυνος παραβίασης προτύπων μπορεί να μετριαστεί με την παροχή μεθόδων για την ακύρωση ενός βιομετρικού προτύπου προκειμένου να αποφευχθεί η μελλοντική επιτυχή επαλήθευση μιας συγκεκριμένης βιομετρικής αναφοράς για την ταυτότητα ενός δεδομένου χρήστη.
- **Ανανεωσιμότητα:** Είναι η δυνατότητα ένα βιομετρικό πρότυπο να μπορεί να ανακληθεί και να αντικατασταθεί με ένα νέο σε περίπτωση διακινδύνευσης του ήδη υπάρχοντος. Αυτό είναι αρκετά δύσκολο να επιτευχθεί με ένα πρότυπο, καθώς τα βιομετρικά χαρακτηριστικά είναι μόνιμα και δεν μπορούν να αλλάξουν. Ως εκ τούτου, ένα εγγεγραμμένο πρότυπο πρέπει να μπορεί να μετατραπεί με έναν εναλλακτικό τρόπο χρησιμοποιώντας διάφορες τεχνικές.

3.2 Ευπάθειες βιομετρικών συστημάτων

Παρόλο που τα βιομετρικά συστήματα παρέχουν πολλαπλά οφέλη σε σχέση με τα παραδοσιακά συστήματα ελέγχου ταυτότητας, παραμένουν ευάλωτα σε επιθέσεις. Ένα βιομετρικό σύστημα δύναται να είναι ευάλωτο λόγω επιθέσεων προς αυτό, όπως επίσης και λόγω κακού σχεδιασμού. (Abdulmonam et. al., 2014). Η διαδικασία της αναζήτησης πιθανών ευάλωτων σημείων έχει δύο στάδια, ένα εκ των οποίων είναι η εύρεση αδυναμιών και η άλλη η αξιολόγηση πιθανών επιθέσεων. Οι ευπάθειες στα βιομετρικά συστήματα πηγάζουν κατά κύριο λόγο από τη δομή του συστήματος, τα βιομετρικά χαρακτηριστικά και την πολιτική διαχείρισης. Ο Διεθνής Οργανισμός Τυποποίησης ISO / IEC FCD 19792 παρουσιάζει μια λίστα με διάφορες απειλές και τρωτά σημεία των βιομετρικών συστημάτων που αναλύονται παρακάτω:

1. Παρουσίαση ψεύτικου βιομετρικού δείγματος στον αισθητήρα: περιλαμβάνει την παρουσίαση ενός ψεύτικου βιομετρικού δείγματος (π.χ. δακτύλου από σιλικόνη, μάσκα προσώπου, ηχογραφημένο δείγμα φωνής) στον αισθητήρα.

2. Επανάληψη αποθηκευμένων ψηφιακών βιομετρικών σημάτων: Ένα αποθηκευμένο σήμα αναπαράγεται στο σύστημα αγνοώντας τον αισθητήρα. Για παράδειγμα, επανάληψη ενός παλιού αντιγράφου μιας εικόνας δακτυλικών αποτυπωμάτων ή ενός ηχογραφημένου ηχητικού σήματος.

3. Άρνηση εξαγωγής χαρακτηριστικών: Το πρόγραμμα εξαγωγής χαρακτηριστικών μπορεί να αντικατασταθεί από ένα πρόγραμμα Trojan horse που παράγει προκαθορισμένα σύνολα χαρακτηριστικών.

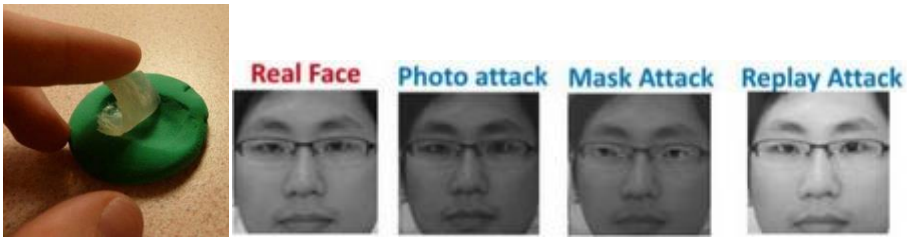
4. Πλαστογράφηση βιομετρικών χαρακτηριστικών: Τα χαρακτηριστικά που εξάγονται από το σύστημα εισόδου αντικαθίστανται από ένα ψεύτικο σύνολο χαρακτηριστικών.

5. Επίθεση στην μονάδα αντιστοίχισης: Σε αυτή την επίθεση, οι γνήσιες τιμές χαρακτηριστικών που προκύπτουν από το στάδιο της αντιστοίχισης αντικαθιστώνται από τιμές που επιλέγονται από τον εισβολέα.

6. Παραποίηση των στοιχείων της βάσης δεδομένων: Η βάση δεδομένων των αποθηκευμένων προτύπων μπορεί να είναι τοπική ή απομακρυσμένη. (Manisha et al., 2020). Ο εισβολέας προσπαθεί να παραποιήσει ένα ή περισσότερα βιομετρικά πρότυπα στη βάση δεδομένων (π.χ. προσθήκη, τροποποίηση ή κατάργηση προτύπων). Ως αποτέλεσμα, είτε μια ψεύτικη ταυτότητα μπορεί να εγκριθεί, είτε ένας νόμιμος χρήστης μπορεί να έρθει αντιμέτωπος με άρνηση υπηρεσίας.

7. Επίθεση καναλιού: Τα αποθηκευμένα πρότυπα μεταδίδονται μέσω ενός καναλιού επικοινωνίας που υπάρχει μεταξύ της βάσης δεδομένων προτύπων και της μονάδας αντιστοίχισης. Τα δεδομένα στο κανάλι μπορούν να κλαπούν, αντικατασταθούν ή να τροποποιηθούν από τον εισβολέα.

8. Επίθεση στη διαδικασία τελικής απόφασης: Εάν το αποτέλεσμα της αντιστοίχισης (αποδοχή ή απόρριψη) μπορεί να μπλοκαριστεί από κάποιο επιτήδειο, τότε η λειτουργία συστήματος ελέγχου ταυτότητας θα παρακαμφθεί.



Εικόνα 3.1 Δημιουργία ψεύτικων βιομετρικών χαρακτηριστικών (δακτυλικού αποτυπώματος και προσώπου αντίστοιχα)

Συνολικά, εντοπίζονται 20 πιθανά σημεία επίθεσης και 22 ευπάθειες σε διάφορα μέρη ενός βιομετρικού συστήματος τα οποία παρουσιάζονται συγκεντρωτικά στην εικόνα 3.2. Πιο αναλυτικά, παρακάτω αναφέρονται οι επιθέσεις ανάλογα το σημείο στο οποίο μπορούν να εφαρμοστούν:

- Στον αισθητήρα μπορούν να εφαρμοστούν αρκετές επιθέσεις όπως:
  - Επίθεση αντίγραφου (Spoofing attack) ή επίθεση μίμησης (mimicry attack): σε περίπτωση που το βιομετρικό χαρακτηριστικό είναι φυσικό ή βασίζεται στη συμπεριφορά ενός ατόμου αντίστοιχα. Αυτές οι επιθέσεις αντιγράφουν με διάφορα μέσα και μεθόδους, το βιομετρικό

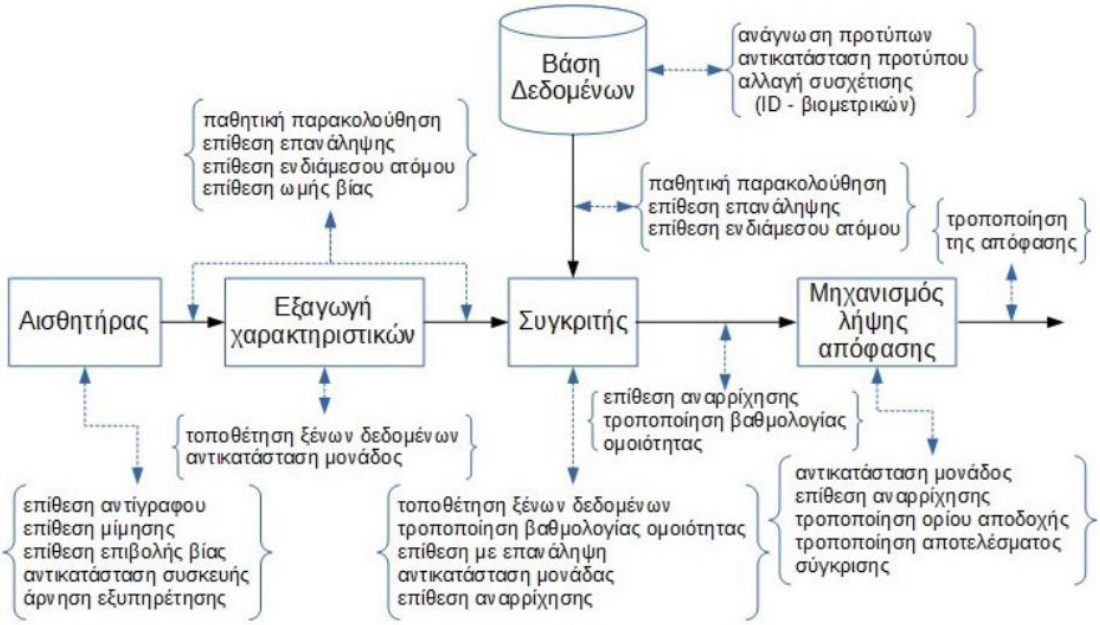
στοιχείο του εγγεγραμμένου χρήστη και το χρησιμοποιούν ώστε να κοροϊδέψουν το σύστημα. (Hadid A.,2014)

- Επίθεση επιβολής βίας: το ορθό βιομετρικό χαρακτηριστικό παρουσιάζεται παρά τη θέληση του χρήστη, για παράδειγμα ένας επιτήδειος αναγκάζει ένα νόμιμο χρήστη υπό κάποιου είδους απειλή, να του δώσει πρόσβαση στο σύστημα.
- Αντικατάσταση συσκευής: αλλαγή της γνήσιας συσκευής καταγραφής με μία άλλη τροποποιημένη συσκευή.
- Άρνηση εξυπηρέτησης (Denial of service): ο κατακλυσμός ενός τεράστιου αριθμού αιτημάτων πρόσβασης στο βιομετρικό σύστημα θα οδηγούσε σε μη διαθεσιμότητα των υπηρεσιών του ακόμη και σε εγκύρους χρήστες.

- Η μονάδα του εξαγωγέα χαρακτηριστικών μπορεί να βρεθεί υπό τον έλεγχο κάποιου επιτήδειου ο όποιος έχει τη δυνατότητα να παράξει συγκεκριμένα χαρακτηριστικά που ο ίδιος επιλέγει, με σκοπό να αποκτήσει τον πλήρη έλεγχο του συστήματος και κατά συνέπεια την πρόσβαση σε αυτό.
- Η μονάδα του συγκριτή κινδυνεύει από την δημιουργία ψευδών βαθμολογιών που παράγει, από τις οποίες κρίνεται το αποτέλεσμα για την τελική αποδοχή ή απόρριψη του χρήστη. Αυτό δύναται να πραγματοποιηθεί με ποικίλους τρόπους όπως:
  - Τροποποίηση των βαθμολογιών ομοιότητας: ο επιτιθέμενος έχοντας στην κατοχή του την τιμή μίας βαθμολογίας ομοιότητας την αλλάζει προτού διαμορφωθεί η τελική απόφαση.
  - Επίθεση επανάληψης: καταγεγραμμένα ορθά δεδομένα ενθέτονται στη μονάδα.
  - Αντικατάσταση κάποιου μέρους: αλλαγή ενός από τα υλικά ή λογισμικά μέρη της μονάδας του συγκριτή με σκοπό τον έλεγχο της συμπεριφοράς του.
  - Επίθεση αναρρίχησης (Hill climbing attack): κλιμακούμενη επαναλαμβανόμενη επίθεση που πραγματοποιεί μικρές τροποποιήσεις κάθε φόρα σε ένα δείγμα μέχρις ότου κάποια στιγμή η βαθμολόγια ομοιότητας να ξεπεράσει το ορισμένο όριο αποδοχής.
- Κανάλια επικοινωνίας: τα κανάλια ενώνουν τις διάφορες μονάδες ενός βιομετρικού συστήματος, όπως το κανάλι μεταξύ του αισθητήρα με τη μονάδα του εξαγωγέα χαρακτηριστικών, της μονάδας του εξαγωγέα χαρακτηριστικών με τη μονάδα του συγκριτή, της βάσης δεδομένων με τη μονάδα του συγκριτή, και της μονάδας του συγκριτή με την εφαρμογή, μπορεί να ελέγχονται και να παρακολουθούνται από μη εξουσιοδοτημένα άτομα. (Natgunanathan I. et.al.,2018). Ανάμεσα στις ενδεχόμενες επιθέσεις είναι:
  - παθητική παρακολούθηση (Eavesdropping attack): η κρυφή παρακολούθηση που συμβαίνει κατά την μετάδοση βιομετρικών δεδομένων.
  - επίθεση ενδιάμεσου ατόμου (Man-in-the-middle attack): η ικανότητα ενός εισβολέα να παραποιεί τα μηνύματα που ανταλλάσσονται μεταξύ δύο σημείων χωρίς να ξέρουν οι επικοινωνούντες ότι το κανάλι έχει παραβιαστεί.
- Βάση δεδομένων: ένας επιτιθέμενος μπορεί να αναγνώσει, να τροποποιήσει ή να αντικαταστήσει τα πρότυπα των εγγεγραμμένων χρηστών, που βρίσκονται στη βάση δεδομένων. Αυτό θα μπορούσε να προκαλέσει την αποδοχή ενός μη εξουσιοδοτημένου ατόμου ή την άρνηση της υπηρεσίας σε εγγεγραμμένα άτομα που σχετίζονται με τα κατεστραμμένα πρότυπα. Επιπλέον, μια τέτοια επίθεση θα επέτρεπε στον εισβολέα την πρόσβαση σε ευαίσθητα προσωπικά δεδομένα των χρηστών που είναι κατοχυρωμένα στη βάση δεδομένων μαζί με τα πρότυπα. (Karthik Nandakumar,2005). Κατά συνέπεια, οι επιθέσεις αυτές θεωρούνται πολύ σοβαρές, καθώς σχετίζονται με το απόρρητο των χρηστών.
- Μηχανισμός λήψης απόφασης: Η παράκαμψη της τελικής απόφασης μπορεί να πραγματοποιηθεί από έναν επιτιθέμενο, ο οποίος δύναται να τροποποιήσει τη λήψη της απόφασης στο τελικό στάδιο

της βιομετρικής αυθεντικοποίησης. Ακόμα κι αν το βιομετρικό σύστημα παρουσιάζει εξαιρετικό επίπεδο ακρίβειας και απόδοσης, μπορεί να καταστεί μη λειτουργικό από αυτόν τον τύπο επιθέσεων.

Στο παρακάτω σχήμα παρουσιάζονται τα στάδια λειτουργίας ενός βιομετρικού συστήματος και αναγράφονται οι πιθανές επιθέσεις που μπορούν να συμβούν σε αυτό, ανάλογα με την τοποθεσία.

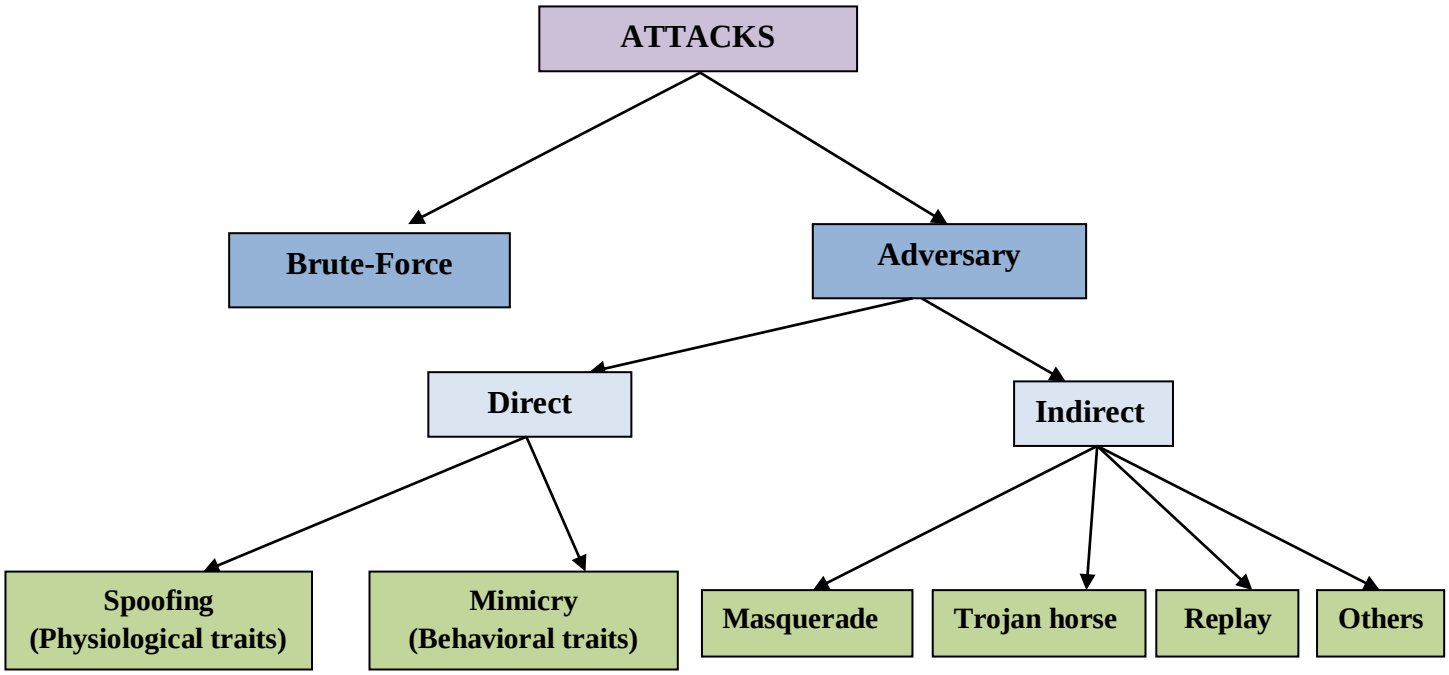


Εικόνα 3.2 Πιθανές επιθέσεις σε ένα βιομετρικό σύστημα ανάλογα με την τοποθεσία

3.3 Επιθέσεις σε βιομετρικά συστήματα

Σε αυτή την ενότητα θα παρουσιαστεί συγκεντρωτικά το σύνολο των επιθέσεων που αναφέρθηκαν παραπάνω με σκοπό να γίνει μια πιο αναλυτική προσέγγιση αυτού του θέματος. Το βιομετρικό σύστημα υφίσταται πολλές κακόβουλες επιθέσεις που μπορούν να εκτελεστούν λόγο διαφόρων ευπαθειών του, όπως είδαμε και στην προηγούμενη υποενότητα. Κακόβουλες επιθέσεις σε ένα βιομετρικό μηχάνημα αποτελούν πρόβλημα ασφάλειας και υποβαθμίζουν τις επιδόσεις του συστήματος. (Kaur H. et al.,2020). Όπως φαίνεται και από το σχήμα 3.3 οι επιθέσεις που συναντώνται συχνά στα βιομετρικά συστήματα διακρίνονται σε:

- Brute-Force attacks: Μια τέτοια επίθεση περιλαμβάνει την υποβολή μεγάλου αριθμού βιομετρικών χαρακτηριστικών από τον επιτήδειο στο σύστημα μέχρι τελικά να καταφέρει να το ξεκλειδώσει έχει πρόσβαση στους πόρους του. Για να εκτελεστεί αποτελεσματικά αυτού του είδους οι επιθέσεις ο εισβολέας πρέπει να διατηρεί μια βάση δεδομένων μεγάλου αριθμού καταχωρήσεων των προτύπων των βιομετρικών χαρακτηριστικών. Αυτή η απειλή, παρουσιάζεται σε όλα τα βιομετρικά συστήματα και είναι αρκετά δύσκολο να αποφευχθεί. Αυτό εξαρτάται κυρίως από την ακρίβεια του συστήματος και από το βιομετρικό χαρακτηριστικό που χρησιμοποιείται.
- Adversary attacks: Μια τέτοια επίθεση αναφέρεται στην προσπάθεια ενός εισβολέα, εγγεγραμμένου ή μη, να ξεγελάσει το σύστημα, με τέτοιο τρόπο ώστε να το παρακάμψει και τελικά να έχει πρόσβαση στους πόρους του.



Εικόνα 3.3: Ταξινόμηση των επιθέσεων σε ένα βιομετρικό σύστημα

Δεδομένου ότι τα ευάλωτα σημεία της Brute-Force επίθεσης είναι εγγενή με τη στατιστική φύση των βιομετρικών συστημάτων, η βιομετρική κοινότητα έχει επικεντρωθεί στη μελέτη των adversary επιθέσεων. (Abdulmonam et. al., 2014). Αυτές οι επιθέσεις μπορούν να διακριθούν σε άμεσες και έμμεσες επιθέσεις όπως περιγράφεται παρακάτω:

Άμεσες επιθέσεις. Σε αυτές τις επιθέσεις δεν απαιτούνται συγκεκριμένες γνώσεις σχετικά με τη λειτουργία του συστήματος, όπως για παράδειγμα, ο αλγόριθμος αντιστοίχισης που χρησιμοποιείται, η διανυσματική μορφή χαρακτηριστικών, κ.λπ. Ο επιτιθέμενος έχει ως στόχο τη μονάδα του αισθητήρα προσπαθώντας μέσω πλαστοπροσωπίας να έχει πρόσβαση στο σύστημα. (Latha U. et al., 2013). Η αντικατάσταση του σετ χαρακτηριστικών με πλαστά ή αλλοιωμένα χαρακτηριστικά ονομάζεται πλαστογράφηση δεδομένων. Αυτοί οι τύποι επιθέσεων πλαστογράφησης βρίσκουν εφαρμογή σε φυσικά χαρακτηριστικά, όπως είναι το δακτυλικό αποτύπωμα ή το πρόσωπο ονομάζονται Spoofing επιθέσεις, ενώ αυτοί που βασίζονται σε συμπεριφοριστικά χαρακτηριστικά, όπως η φωνή ή η υπογραφή ονομάζονται επιθέσεις μίμησης. (Hadid A.,2014)

Έμμεσες επιθέσεις. Εν αντιθέσει με τις άμεσες επιθέσεις, σε αυτές ο εισβολέας πρέπει να γνωρίζει κάποιες πρόσθετες πληροφορίες σχετικά με την εσωτερική λειτουργία του συστήματος και στις περισσότερες περιπτώσεις, απαιτείται φυσική πρόσβαση σε ορισμένα από τα στοιχεία της εφαρμογής (εξαγωγέας χαρακτηριστικών, μονάδα αντιστοίχισης, βάση δεδομένων κ.λπ.). Κάποιες από τις επιθέσεις αυτής της κατηγορίας είναι οι παρακάτω:

- Masquerade attack: Η επίθεση μεταμφιέσεων είναι ένας γενικός όρος που δίνεται σε οποιαδήποτε απόπειρα του εχθρού να προσποιείται ότι είναι νόμιμος χρήστης για να έχει πρόσβαση είτε στο σύστημα είτε στις πληροφορίες και τις υπηρεσίες ενός εγγεγραμμένου χρήστη.

- Trojan horse attacks: Ορισμένα μέρη του συστήματος, μπορούν να αντικατασταθούν από ένα πρόγραμμα Δούρειου ίππου με σκοπό την απόκτηση του πλήρη έλεγχου του συστήματος. Για παράδειγμα, ο εισβολέας μπορεί να επιτεθεί στον εξαγωγέα χαρακτηριστικών με τέτοιο τρόπο ώστε να παράγει επιθυμητά χαρακτηριστικά και να τα προσθέτει στην υπάρχουσα βάση δεδομένων ή να αντικαταστήσει το πρότυπο του νόμιμου χρήστη με το δικό του κλέβοντας με αυτό τον τρόπο την ταυτότητά του.
- Replay attacks: Σε μια επίθεση επανάληψης αρχικά ο επιτιθέμενος αντιγράφει το δείγμα που καταγράφει ο αισθητήρας, και σε ύστερο χρόνο αναπαράγει τα δεδομένα αυτά.
- Άρνηση υπηρεσίας (DoS): ο εισβολέας βλάπτει το σύστημα κατακλύζοντας το με πολλά ψευδή αιτήματα πρόσβασης έτσι ώστε οι υπολογιστικοί πόροι να σπαταλούνται και οι γνήσιοι χρήστες να μην μπορούν να το χρησιμοποιήσουν.
- Tampering Attack: Η δυνατότητα ενός εισβολέα να μπορεί να τροποποιήσει τις βαθμολογίες στην μονάδα αντιστοίχησης, μπορεί να έχει ως αποτέλεσμα το σύστημα να κάνει δέκτη την αίτηση πρόσβασης σε ένα μη εξουσιοδοτημένο χρήστη ενώ ταυτόχρονα να απορρίπτει την πρόσβαση σε νόμιμους χρήστες.
- Zero-effort attack: Σε αρκετές περιπτώσεις ένα υψηλό FRR προκαλεί ενόχληση στους νόμιμους χρήστες οι οποίοι ζητούν από τον διαχειριστή του συστήματος να μειώσει το κατώφλι επαλήθευσης. Αυτό αναπόφευκτα προκαλεί υψηλό FAR, το οποίο, με τη σειρά του, μειώνει το επίπεδο ασφάλειας του συστήματος. Ένα σύστημα που χαρακτηρίζεται από υψηλό δείκτη λανθασμένων αποδοχών (False Acceptance Rate) είναι πιθανό να παραβιαστεί έπειτα από έναν αριθμό βιομετρικών χαρακτηριστικών που θα παρουσιαστούν τυχαία στο σύστημα, καθώς θα βρεθεί κάποιο που να ταιριάζει. (Pagnin E. et. al., 2017). Αυτό μπορεί να συμβεί ακόμα και αν δεν υπάρχει κάποιος που να επιθυμεί να επιτεθεί στο σύστημα, αυτή η περίπτωση ονομάζεται επίθεση μηδενικής-προσπάθειας (zero-effort attack).

Εν κατακλείδι, δυο περιστατικά επιθέσεων που πραγματοποιηθήκαν πρόσφατα και αναστάτωσαν την κοινή γνώμη αναφέρονται ενδεικτικά στις παρακάτω παραγράφους.

Τον Αύγουστο του 2019, οι ερευνητές ασφαλείας Noam Rotem και Ran Locar ανακοίνωσαν την ανακάλυψη ενός κενού ασφαλείας στο δίκτυο της Suprema. Η Suprema, με έδρα τη Νότια Κορέα, χρησιμοποιείται παγκοσμίως από χιλιάδες εταιρείες ως πάροχος βιομετρικού ελέγχου ταυτότητας και ασφάλειας ταυτότητας, για τον έλεγχο της πρόσβασης σε φυσικούς χώρους και εγκαταστάσεις. Το κενό ασφαλείας επέτρεψε στους ερευνητές να έχουν πρόσβαση στα δεδομένα ελέγχου ταυτότητας περισσότερων από 1 εκατομμυρίου χρηστών. Αυτές οι πληροφορίες περιλάμβαναν δεδομένα αναγνώρισης προσώπου, δακτυλικά αποτυπώματα, μη κρυπτογραφημένα ονόματα χρήστη και κωδικούς πρόσβασης και άλλα ευαίσθητα δεδομένα. Επιπλέον, οι ερευνητές ανακάλυψαν τα εκτεθειμένα αρχεία προσωπικών δεδομένων 27,8 εκατομμυρίων χρηστών στη βάση δεδομένων Suprema Biostar 2 και κατάφεραν να εντοπίσουν κωδικούς πρόσβασης του διαχειριστή του συστήματος, καθώς και να αντικαταστήσουν τα δακτυλικά αποτυπώματα των χρηστών. Οι πληροφορίες στη βάση δεδομένων του συστήματος δεν είχαν προστασία στον κυβερνοχώρο καθώς η αποθήκευση των κωδίκων πρόσβασης των χρηστών και του διαχειριστή στη ήταν σε απλό κείμενο (plaintext) και όχι κρυπτογραφημένο (ciphertext). Ως επί το πλείστον, εκπρόσωπος της εταιρείας δήλωσε στο Guardian ότι εάν υπήρχε συγκεκριμένη απειλή για τα προϊόντα ή / και τις υπηρεσίες της, θα λάμβανε άμεσα μέτρα. Ωστόσο, παραμένει άγνωστο εάν

κάποιος κακόβουλος χρήστης ανακάλυψε και εκμεταλλεύτηκε την ευπάθεια αυτή πριν γίνει γνωστή από τους ερευνητές.

Τον Μάρτιο του 2020, μια ομάδα ερευνητών ασφαλείας, οι SafetyDetectives, αποκάλυψε παραβίαση στα δεδομένα της Antheus Tecnologia, μιας εταιρείας βιομετρικών λύσεων που εδρεύει στη Βραζιλία. Η εταιρεία είχε αφήσει εκτεθειμένες ευαίσθητες πληροφορίες σε μη ασφαλή διακομιστή, συμπεριλαμβανομένων 76.000 δακτυλικών αποτυπωμάτων. Όπως αναφέραμε, η εταιρεία παραμέλησε να προστατεύσει με κωδικό πρόσβασης τη βάση δεδομένων στο cloud και να κρυπτογραφήσει τις πληροφορίες που ήταν αποθηκευμένες σε αυτήν. Ως εκ τούτου, ο ευάλωτος διακομιστής περιείχε περίπου 16 gigabyte δεδομένων, με 81,5 εκατομμύρια αρχεία, συμπεριλαμβανομένων πληροφοριών σύνδεσης του διαχειριστή, τηλεφωνικών αριθμών των υπαλλήλων, προσωπικών και εταιρικών διευθύνσεων ηλεκτρονικού ταχυδρομείου τα οποία ήταν εκτεθειμένα και χωρίς ιδιαίτερη προστασία. Οι εκπρόσωποι της Antheus Tecnologia, ισχυρίστηκαν ότι τα δεδομένα είχαν κατακερματιστεί, κάτι που τελικά δεν ίσχυε. Μια ενδεχόμενη επίθεση εάν κάποιος επιτήδειος εκμεταλλεύονταν αυτή την ευπάθεια θα ήταν να τροποποιήσουν, το δυαδικό κώδικα που υπήρχε αποθηκευμένο στη βάση δεδομένων με σκοπό να αναδημιουργήσουν τα βιομετρικά δεδομένα, κάτι που θα είχε καταστροφικές συνέπειες για τους νόμιμους χρήστες.

3.4 Τεχνικές αντιμετώπισης ευπαθειών

Υπάρχουν ορισμένα αντίμετρα που μπορούν να ληφθούν για την ελαχιστοποίηση του κινδύνου, των φορέων απειλής και των τρωτών σημείων που περιγράφονται παραπάνω. Είναι σημαντικό να σημειωθεί ότι η ασφάλεια δεν πρέπει να βασίζεται σε μία μόνο μέθοδο προστασίας, αλλά σε ένα συνδυασμό τεχνικών ώστε να υπάρξει μια πιο αποτελεσματική προστασία ολόκληρου του συστήματος. (Abdulmonam et. al., 2014). Τα βασικά αντίμετρα που εφαρμόζονται κατά κόρο για την προστασία των βιομετρικών προτύπων και θα αναφερθούν παρακάτω επιγραμματικά χωρίζονται σε:

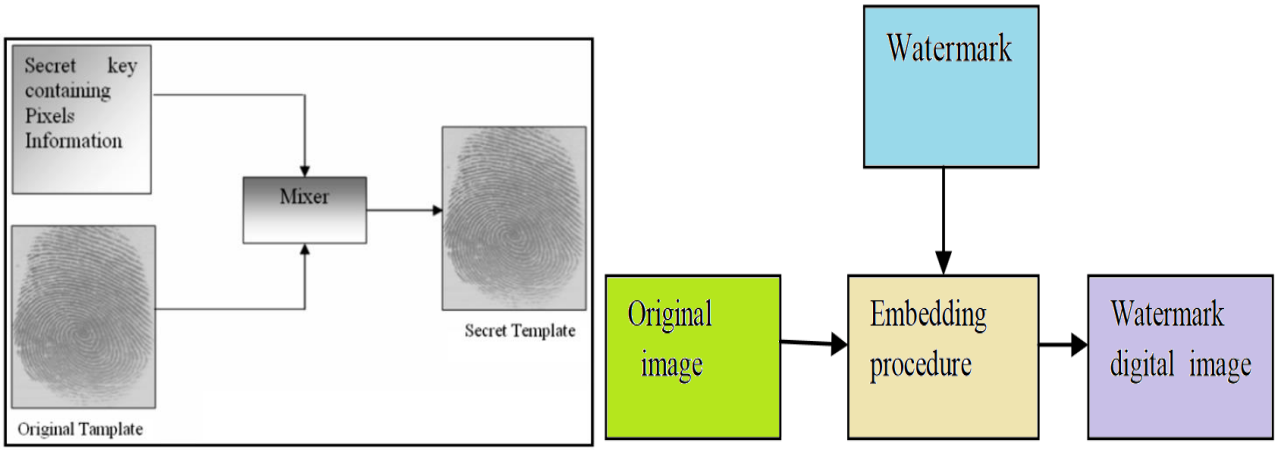
(α) τεχνικές που βασίζονται σε υλικό (Hardware based) και (β) τεχνικές που βασίζονται σε λογισμικό (Software based).

Η προστασία προτύπων με βάση το υλικό μπορεί να εκτελεστεί παραδείγματος χάριν από μια έξυπνη κάρτα, γνωστή και ως τεχνική match-on-card. Η βιομετρική έξυπνη κάρτα δακτυλικών αποτυπωμάτων είναι μια πλαστική κάρτα εξοπλισμένη με μικροελεγκτή, η οποία μπορεί να αποθηκεύει και να επεξεργάζεται τα δεδομένα του χρήστη. Ο μικροελεγκτής μπορεί να λαμβάνει αιτήματα από αναγνώστες έξυπνων καρτών και να επαληθεύει την ταυτότητα του χρήστη. Όταν ένας χρήστης παρουσιάζει την έξυπνη κάρτα δακτυλικών αποτυπωμάτων του σε έναν αναγνώστη έξυπνων καρτών (για την αναγνώριση / έλεγχο ταυτότητας), ο αναγνώστης επικοινωνεί με την κάρτα και ζητά από τον χρήστη να σαρώσει το δάχτυλό του. Ο χρήστης σαρώνει το δάχτυλό του (αυτό που είναι καταχωρημένο στην έξυπνη κάρτα δακτυλικών αποτυπωμάτων) και ο αναγνώστης καρτών καταγράφει δείγμα δακτυλικών αποτυπωμάτων. (Latha U. et al., 2013). Έπειτα, εξάγει τις σχετικές πληροφορίες από το δείγμα και τις στέλνει στην κάρτα. Ακολούθως, το τσιπ δακτυλικών αποτυπωμάτων του μικροελεγκτή της έξυπνης κάρτας εκτελεί μια βιομετρική σύγκριση μεταξύ της νέας σάρωσης και των ήδη αποθηκευμένων βιομετρικών δεδομένων σύμφωνα με τον αλγόριθμο που χρησιμοποιείται και λαμβάνει μια απόφαση (match ή non-match), η οποία αποστέλλεται στον αναγνώστη καρτών.

Εικόνα 3.4: Βιομετρική έξυπνη κάρτα δακτυλικών αποτυπωμάτων [70]

Η ασφάλεια βιομετρικών προτύπων βάσει λογισμικού μπορεί να επιτευχθεί με:

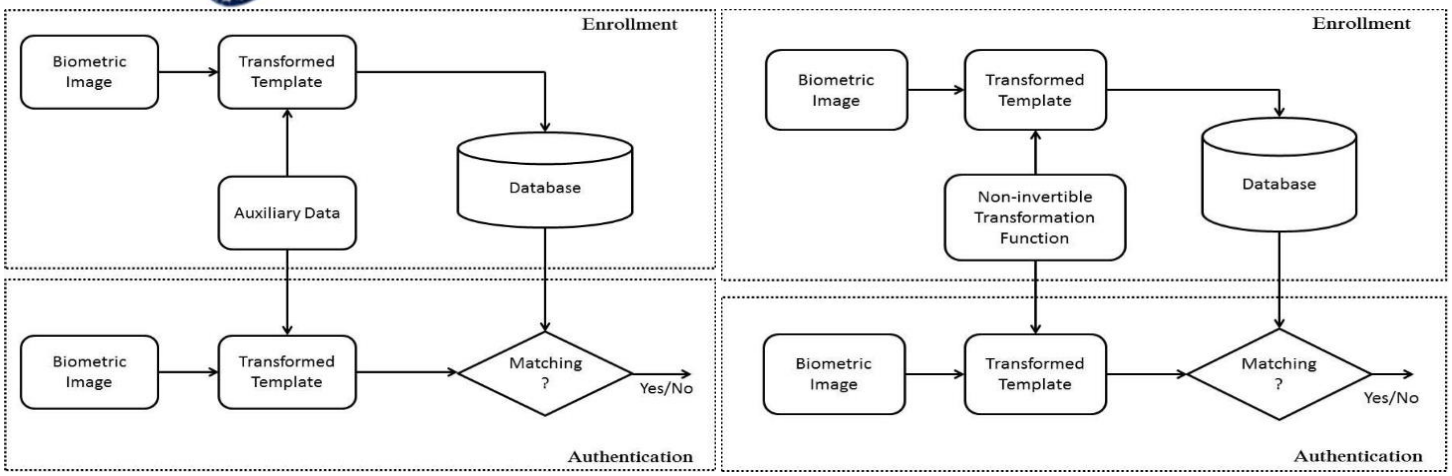
1.Τεχνικές βασισμένες στον μετασχηματισμό εικόνας όπως η τεχνική της **υδατογράφησης** στην οποία οι ιδιωτικές πληροφορίες ενσωματώνονται στα δεδομένα κεντρικού υπολογιστή για την προστασία των δικαιωμάτων πνευματικής ιδιοκτησίας αυτών των δεδομένων, παρέχοντας με αυτό τον τρόπο προστασία από την παράνομη χρήση βιομετρικών δεδομένων. (Abdulmonam et. al., 2014). Υπάρχουν δύο τύποι υδατογραφήματος που βασίζονται στον τομέα εφαρμογής: ο χωρικός τομέας, όπου αλλάζουν οι τιμές pixel στην εικόνα και ο φασματικός τομέας, όπου προστίθεται ένα σήμα υδατογραφήματος στην κεντρική εικόνα. Άλλη μια τεχνική μετασχηματισμού της εικόνας είναι η τεχνική της **στεγανογραφίας** η οποία κρύβει σημαντικά δεδομένα σε μια ανυποψίαστη εικόνα φορέα. Λεπτομέρειες δακτυλικών αποτυπωμάτων εξάγονται και κρύβονται σε pixel μιας εικόνας «κάλυψης» ή καλύτερα εξωφύλλου, όπως μια εικόνα προσώπου, μια εικόνα ίριδας ή μια άσχετη εικόνα. Η εικόνα εξωφύλλου μεταδίδεται μέσω ενός μη ασφαλούς καναλιού επικοινωνίας. Ακόμα κι αν ο εισβολέας παρεμποδίσει την εικόνα εξωφύλλου, δεν θα γνωρίζει ότι οι λεπτομέρειες δακτυλικών αποτυπωμάτων είναι κρυμμένες στην εικόνα εξωφύλλου.(Lim M et. al., 2015). Η στεγανογραφία και το υδατογράφημα χρησιμοποιούνται για την αποτροπή επιθέσεων στο κανάλι μεταξύ αισθητήρα και εξαγωγέα χαρακτηριστικών και στο κανάλι μεταξύ μονάδας αντιστοίχισης και συσκευής εφαρμογής. Το υδατογράφημα χρησιμοποιείται για έλεγχο ταυτότητας και απόδειξη της ιδιοκτησίας του εκάστοτε προτύπου, ενώ η στεγανογραφία μπορεί να χρησιμοποιηθεί για τη μεταφορά κρίσιμων βιομετρικών πληροφοριών από έναν client σε έναν server. Ο συνδυασμός αυτών των δύο τεχνικών παρέχει περισσότερη ασφάλεια σε σύγκριση με τη μεμονωμένη χρήση μιας τεχνικής.



α) **β)**

Εικόνα 3.5: α) Διαδικασία βιομετρικής στεγανογραφίας β) Διαδικασία βιομετρικού υδατογραφήματος [5]

2.Τεχνικές βασισμένες στον μετασχηματισμό χαρακτηριστικών: Μια συνάρτηση μετασχηματισμού εφαρμόζεται στο βιομετρικό πρότυπο και δίνει ως αποτέλεσμα ένα μετασχηματισμένο πρότυπο, το οποίο αποθηκεύεται στη βάση δεδομένων. Η συνάρτηση μετασχηματισμού λαμβάνει παραμέτρους που προέρχονται από ένα τυχαίο κλειδί ή από ένα κωδικό. Η ίδια συνάρτηση εφαρμόζεται και στο βιομετρικό χαρακτηριστικό που προσφέρει ο χρήστης για την επαλήθευση και πρόσβαση του στο σύστημα. Ως επί το πλείστον, το αποτέλεσμα που προκύπτει, συγκρίνεται με το μετασχηματισμένο αποθηκευμένο πρότυπο. Ανάλογα με τα χαρακτηριστικά της συνάρτησης μετασχηματισμού, το μετασχηματισμένο χαρακτηριστικό που προκύπτει μπορεί να κατηγοριοποιηθεί περαιτέρω ως salting ή ως μη αναστρέψιμου μετασχηματισμού. (Pagnin E. et. al., 2017). Ως εκ τούτου, η εφαρμοζόμενη συνάρτηση μπορεί να είναι αντιστρέψιμη, έχοντας ως αποτέλεσμα μία προσέγγιση (salting), όπου η ασφάλεια είναι βασισμένη στην προστασία των παραμέτρων της συνάρτησης, ή να είναι μη-αντιστρέψιμη, οπότε εφαρμόζεται μία μονόδρομη συνάρτηση στο πρότυπο και είναι υπολογιστικά αδύνατο να αντιστραφεί η συνάρτηση ακόμα και αν οι παράμετροι του μετασχηματισμού φανερωθούν. (Kaur H. et al.,2020). Η χρήση μεθόδων της πρώτης κατηγορίας συνήθως έχουν ως αποτέλεσμα χαμηλούς δείκτες λανθασμένης αποδοχής (FAR), όμως σε περίπτωση που το κλειδί ενός χρήστη παραβιαστεί, το πρότυπο του χρήστη παύει να είναι ασφαλές καθώς, υπάρχει δυνατότητα αντιστροφής του μετασχηματισμού. Αντίθετα, όταν γίνεται χρήση μη-αντιστρέψιμων μετασχηματισμών, ακόμα και αν το κλειδί διαρρεύσει, δεν υπάρχει δυνατότητα απόκτησης κάποιας σημαντικής πληροφορίας για το πρότυπο, παρέχοντας έτσι καλύτερη ασφάλεια από αυτή που υφίσταται με την προσέγγιση (salting). Πιο αναλυτικά, η επιλογή της ασφάλειας προτύπων που είναι βασισμένη σε μη-αντιστρέψιμους μετασχηματισμούς, εκμεταλλεύεται το γεγονός ότι υπάρχει δυσκολία αντιστροφής του μετασχηματισμού ώστε να αποκτηθούν τα αρχικά βιομετρικά δεδομένα. (Padma Polash Paul et. al., 2012). Είναι σημαντικό να αναφερθεί ότι, όταν γίνεται χρήση των τεχνικών παραμόρφωσης προτύπων, είτε με αντιστρέψιμους είτε με μη-αντιστρέψιμους μετασχηματισμούς, μόνο τα παραμορφωμένα δεδομένα αποθηκεύονται στην βάση δεδομένων. Αυτό συνεπάγεται ότι ακόμα και σε περίπτωση παραβίασης της βάσης δεδομένων, θεωρητικά, αν δεν υπάρχει πρόσβαση στα κλειδιά και ο μετασχηματισμός είναι μη αντιστρέψιμος, δεν υπάρχει δυνατότητα εξαγωγής των βιομετρικών δεδομένων.



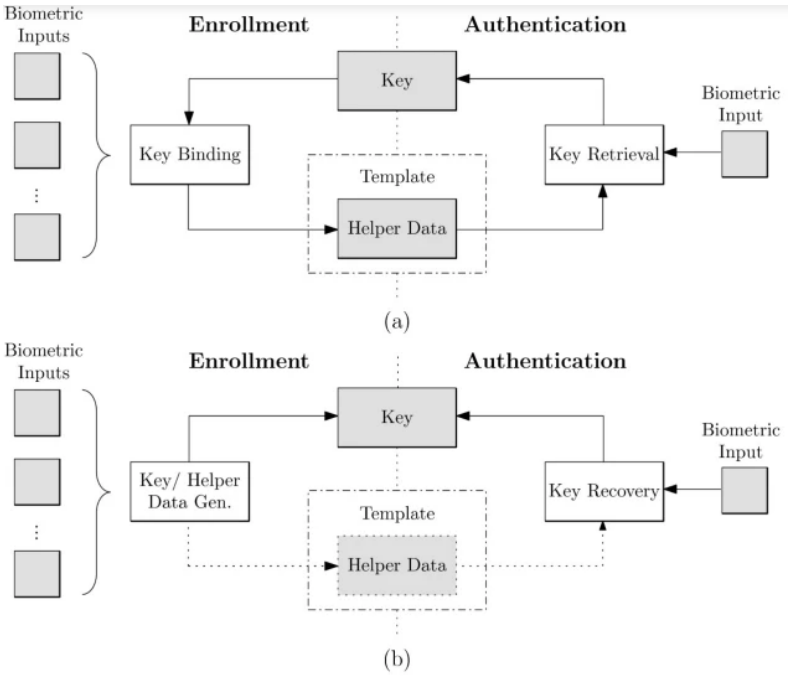
α) β)

Εικόνα 3.6: α) Μπλοκ διάγραμμα της προσέγγισης salting για επαλήθευση β) Μπλοκ διάγραμμα της μη αναστρέψιμης συνάρτησης μετασχηματισμού για επαλήθευση [67]

3.Τεχνικές βασισμένες σε βιομετρική κρυπτογραφία: Η τρίτη βασική κατηγορία έχει ως κύριο χαρακτηριστικό τα βιομετρικά κρυπτοσυστήματα, τα οποία μπορούν να εισχωρήσουν σε ένα βιομετρικό σύστημα. Λόγω της ενδοατομικής μεταβλητότητας που παρουσιάζουν τα περισσότερα βιομετρικά χαρακτηριστικά, είναι αδύνατη η απευθείας εξαγωγή κλειδιών. (Eliza Yingzi Du et al., 2011).Τα βιομετρικά κρυπτοσυστήματα έχουν σχεδιαστεί για να εντάξουν με ασφάλεια ένα κλειδί στα βιομετρικά δεδομένα ή να παράξουν ένα κλειδί από βιομετρικά δεδομένα. Η πλειονότητα των βιομετρικών κρυπτοσυστημάτων απαιτεί την ύπαρξη ορισμένων δημόσιων πληροφοριών ή αλλιώς βοηθητικών δεδομένων, τα οποία χρησιμοποιούνται για την απόκτηση ή την παραγωγή κλειδιών. (Christian Rathgeb et al.,2011). Ως εκ τούτου, τα βοηθητικά δεδομένα, δεν θα πρέπει να αποκαλύπτουν σημαντικές πληροφορίες σχετικά με τα αρχικά βιομετρικά πρότυπα, καθώς συμμετέχουν στην ανακατασκευή των κλειδιών. Ανάλογα με τη διαδικασία που δημιουργούνται τα βοηθητικά δεδομένα, τα βιομετρικά κρυπτοσυστήματα διακρίνονται σε δύο κατηγορίες:

1) παραγωγής κλειδιού (key-generating), όπου δυαδικά κλειδιά δημιουργούνται από τα βιομετρικά χαρακτηριστικά.

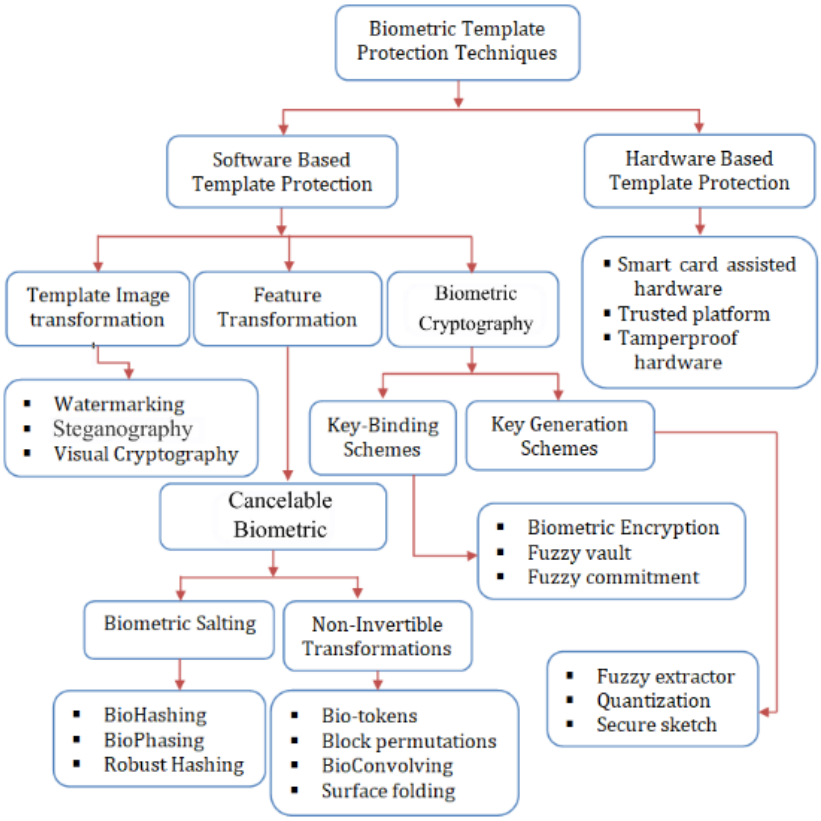
2) ενσωμάτωσης κλειδιού (key-binding), όπου ένα τυχαίο κλειδί ενσωματώνεται με ασφάλεια στα βιομετρικά δεδομένα.



Εικόνα 3.7: Η βασική αρχιτεκτονική προστασίας ενός βιομετρικού συστήματος μέσω (α) ενσωμάτωσης κλειδιών και (β) της δημιουργίας κλειδιών [68]

Ένα σύστημα ενσωμάτωσης κλειδιού δύναται να χρησιμοποιηθεί για να προστατεύσει ένα βιομετρικό πρότυπο με την αρωγή ενός δυαδικού κλειδιού, ασφαλίζοντας έτσι ένα σύστημα βιομετρικής αναγνώρισης, ή για να απελευθερώσει ένα κρυπτογραφικό κλειδί μόνο όταν ο κάτοχος του επιδείξει ένα συγκεκριμένο βιομετρικό χαρακτηριστικό. (Jin Z. et al, 2016). Και στις δύο αυτές περιπτώσεις ένα μυστικό κλειδί, ενσωματώνεται κατά την διάρκεια της εγγραφής με ένα πρότυπο αναφοράς ώστε να γίνει η παραγωγή των βοηθητικών δεδομένων. (Abdellatef E., et al., 2019). Από αυτά τα δεδομένα θα πρέπει να είναι αδύνατον να πραγματοποιηθεί εξαγωγή πληροφοριών σχετικών με τα αρχικά βιομετρικά δείγματα ή το κλειδί. Τα βοηθητικά δεδομένα στην πορεία χρησιμοποιούνται μαζί με τα βιομετρικά χαρακτηριστικά του χρήστη κατά την φάση της ταυτοποίησης.

Σε ένα σύστημα παραγωγής κλειδιού, τα βοηθητικά δεδομένα προέρχονται αποκλειστικά από το βιομετρικό πρότυπο. (Christian Rathgeb et al.,2011). Ακολούθως τα κλειδιά παράγονται απευθείας από τα βοηθητικά δεδομένα και ένα βιομετρικό χαρακτηριστικό. Αν το σύστημα παραγωγής κλειδιού εξάγει κλειδιά χωρίς την χρήση βοηθητικών δεδομένων, τότε αυτά δεν μπορούν να ανανεωθούν σε περίπτωση παραβίασης.



Εικόνα 3.8: Τεχνικές προστασίας βιομετρικών προτύπων

Η λεπτομερής ταξινόμηση αυτών των συστημάτων προστασίας βιομετρικών προτύπων φαίνεται στο σχήμα 3.8 και επεκτείνονται περαιτέρω σε άλλες υποκατηγορίες τεχνικών προστασίας προτύπων όπως:

- Liveness detection: Είναι η ικανότητα διάκρισης μεταξύ ενός πραγματικού βιομετρικού δείγματος που λαμβάνεται από ένα ζωντανό άνθρωπο και ενός ψεύτικου βιομετρικού δείγματος που λαμβάνεται από ένα αντικείμενο. Η ανίχνευση της «ζωντάνιας» χρησιμοποιείται για την αποτροπή επιθέσεων στον αισθητήρα και αποτελεί τη βασική άμυνα ενάντια της πλαστογράφησης. Στην ουσία διασφαλίζει ότι το βιομετρικό δείγμα που παρουσιάζεται στον αναγνώστη προέρχεται από ένα ζωντανό άτομο και δεν είναι τεχνητό ή από πτώμα.(Jin Z. et al, 2016). Ορισμένες δοκιμές ζωτικότητας βασίζονται σε αυτόνομες αποκρίσεις και άλλες μπορούν να χρησιμοποιήσουν μια δομή πρόκλησης / απόκρισης, όπως το ανοιγοκλείσιμο των βλέφαρων όταν αυτό ζητηθεί. Οι μέθοδοι ανίχνευσης ζωτικότητας μπορούν να ενσωματωθούν στον βιομετρικό αναγνώστη ή μπορούν να δημιουργηθούν από μια ξεχωριστή συσκευή που θα εντοπίζει τη ύπαρξη σημείων ζωής μέσω μετρήσεων όπως ανίχνευση παλμών, αρτηριακή πίεση, θερμοκρασία κτλ.
- Multiple biometrics: Τα πολλαπλά βιομετρικά στοιχεία αυξάνουν το χρόνο επεξεργασίας και προσθέτουν ένα επίπεδο πολυπλοκότητας, καθώς απαιτούνται περισσότερα από ένα βιομετρικά, για παράδειγμα, δακτυλικό αποτύπωμα και σάρωση ίριδας. Είναι σαφές ότι είναι πολύ πιο δύσκολο να πλαστογραφηθούν πολλαπλά και διαφορετικά βιομετρικά χαρακτηριστικά αποτελώντας έτσι, ισχυρό αποτρεπτικό στοιχείο για την πλαστογράφηση.
- Ακεραιότητα σήματος και δεδομένων: Ένα σημαντικό στοιχείο της ακεραιότητας του συστήματος είναι τα δεδομένα που παράγονται στον αισθητήρα να είναι αξιόπιστα και να

παραμένουν ασφαλή μετά το πέρασμα από διάφορα στάδια σύγκρισης και επεξεργασίας. Ως επί το πλείστον, οι αμυντικές τεχνικές κατά της επανάληψης και των επιθέσεων Man in the Middle περιλαμβάνουν:

- ✓ Χρονική σήμανση του σήματος μεταξύ του αισθητήρα και του υπόλοιπου συστήματος. Η χρονική σήμανση, σε σύγκριση με τα ρολόγια συστήματος ή την τρέχουσα ώρα, μπορεί να υποδεικνύει τη χρήση παλαιών ή επαναλαμβανόμενων δεδομένων.
- ✓ Χρήση ψηφιακών υπογραφών.
- ✓ Αποκλεισμός προσπαθειών αντιστοίχισης σε περίπτωση υπέρβασης του ορίου ψευδούς αντιστοίχισης ή χρονικών περιόδων. Ο καθορισμός ορίων σχετικά με τον αριθμό των προσπαθειών αγώνων ή τον αριθμό των αποτυχημένων προσπαθειών σε μια δεδομένη χρονική περίοδο, είναι μια αποτελεσματική τεχνική άμυνας. Είναι επίσης σημαντικό να λαμβάνονται υπόψη τα σχετικά αμυντικά μέτρα, όπως η ακεραιότητα του υλικού και η κρυπτογράφηση.

- Cancellable biometrics: Ένα χαρακτηριστικό της βιομετρίας είναι ότι είναι αναντικατάστατα και μόλις τεθούν σε κίνδυνο, γενικά δεν μπορούν να επαναχρησιμοποιηθούν. Μια τεχνική που επιτρέπει την επαναχρησιμοποίηση των αρχικών βιομετρικών περιγράφεται ως ακυρώσιμη βιομετρική. (Abdellatef E. et al., 2019). Ουσιαστικά είναι ένας μηχανισμός προστασίας προτύπων, όπου το αρχικό βιομετρικό σχέδιο παραμορφώνεται σκόπιμα για να εγγραφεί στο σύστημα ελέγχου ταυτότητας. Όταν εφαρμόζεται το ακυρώσιμο βιομετρικό σχήμα, αντί για το αρχικό βιομετρικό σχέδιο, αποθηκεύεται μια παραμορφωμένη έκδοση του προτύπου. Μόνο τα μετασχηματισμένα δεδομένα αποθηκεύονται και εάν αυτά τα δεδομένα έχουν παραβιαστεί, μπορεί να εφαρμοστεί ένας νέος μετασχηματισμός, αντικαθιστώντας έτσι το αρχικό πρότυπο. (Kaur H. et al.,2020). Τα επιλέξιμα βιομετρικά δεν προστατεύουν τα βιομετρικά συστήματα ενάντια στην επίθεση, αλλά θα βοηθήσουν στην ανάκτηση όπου έχουν παραβιαστεί πρότυπα ή άλλα βιομετρικά δεδομένα. Τα ακυρώσιμα βιομετρικά, ωστόσο, είναι ελάχιστα χρήσιμα όταν η αρχική βιομετρική ή η εικόνα έχει παραβιαστεί. (Eliza Yingzi Du et al., 2011). Η ακυρώσιμη βιομετρική χρησιμοποιείται κατά κύριο λόγο για την αποτροπή επιθέσεων στη βάση δεδομένων συστήματος.

Σημείο επίθεσης	**Επίθεση**	**Αντίμετρο**
Συλλογή μετρήσεων	Spoofing	Έλεγχος φυσικής παρουσίας Έλεγχος ζωντάνιας
	Παράκαμψη συσκευής	Αυθεντικοποίηση συσκευής
	Υπερφόρτωση (Denial of Service)	Αυστηρές προδιαγραφές συσκευών
Μετάδοση μετρήσεων	Υποκλοπή	Ασφαλές κανάλι (κρυπτογράφηση)
	Επανάληψη/εμφύτευση	•Ψηφιακή υπογραφή •Χρονοσήμανση •Χρόνος ζωής
	Brute force	•Κλείδωμα •Time out
Εξαγωγή προτύπων	Παράκαμψη συσκευής	Αυθεντικοποίηση συσκευής
	Πλαστά δεδομένα	Ισχυροί αλγόριθμοι

Μετάδοση προτύπων	Υποκλοπή	Χρήση ασφαλούς καναλιού
	Επανάληψη/έγχυση	•Ψηφιακή υπογραφή •Χρονοσήμανση •Χρόνος ζωής
	Brute force	•Κλείδωμα •Time out
Σύγκριση προτύπων	Πλαστά δεδομένα	Ισχυροί αλγόριθμοι
	Παράκαμψη συσκευής	Αυθεντικοποίηση συσκευής
	Παράκαμψη απόφασης	Ασφαλές κανάλι
	Hill climbing	Κβάντιση σκορ
Αποθήκευση προτύπων	Εισβολή	•Access control •Κρυπτογράφηση δεδομένων •Αποκεντρωμένη βάση
	Υποκλοπή	Ασφαλές κανάλι

Πίνακας 3.8: Συγκεντρωτικός πίνακας επιθέσεων και αντιμέτρων ανάλογα το σημείο επίθεσης

4. Προστασία βιομετρικών προτύπων μέσω βιομετρικής κρυπτογράφησης

4.1 Βιομετρία και κρυπτογραφία

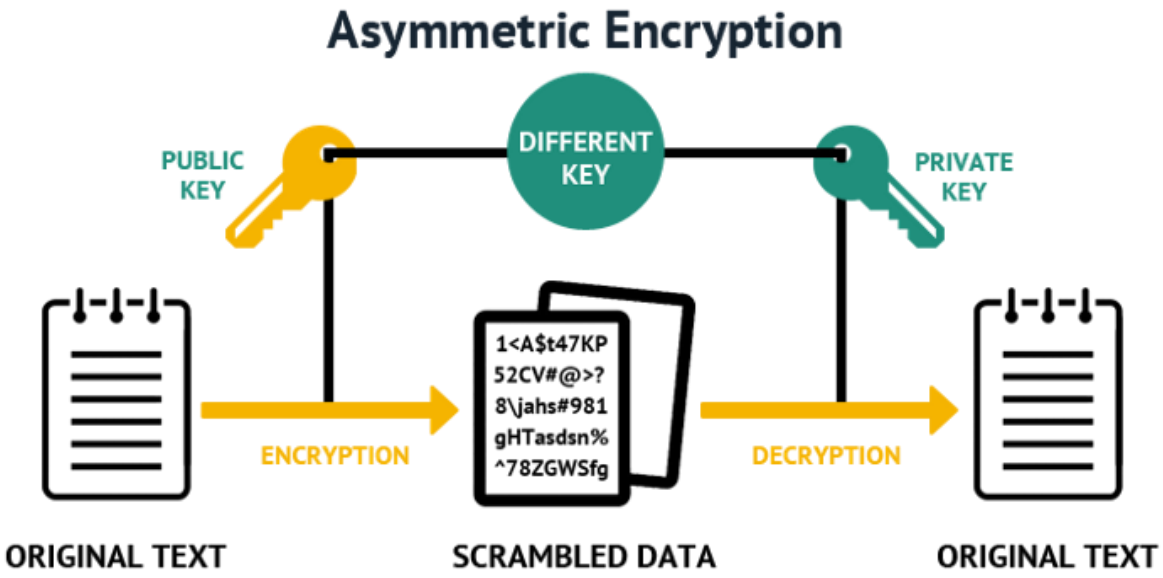
Με την εκθετική αύξηση της ανταλλαγής πληροφοριών τα τελευταία χρόνια, η αξιόπιστη μετάδοση και αποθήκευση ευαίσθητων δεδομένων έχει καταστεί ζωτική πτυχή της ασφάλειας του δικτύου. Η ασφάλεια των πληροφοριών και η ασφαλής μετάδοση δεδομένων καθίστανται πολύ σημαντικά ζητούμενα στην επιστήμη της ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων, καθώς τα δεδομένα διασχίζοντας ένα δίκτυο είναι ένας πολύ εύκολος στόχος για κάθε εισβολέα που υπάρχει στο δίκτυο. Για να αποφευχθεί αυτό, συνιστάται η κρυπτογράφηση των μηνυμάτων για την παροχή ασφάλειας των πληροφοριών. Ως επί το πλείστον, για την ασφαλή μετάδοση δεδομένων μέσω ενός μη ασφαλούς καναλιού, η κρυπτογραφία θεωρείται ως η πιο αποτελεσματική μέθοδος. Η κρυπτογραφία είναι η διαδικασία μετατροπής ενός απλού κειμένου, σε κρυπτογραφημένο κείμενο, δηλαδή μη αναγνώσιμου, με σκοπό να αποκρύβει το περιεχόμενο των μηνυμάτων από ακούσιους και μη εξουσιοδοτημένους χρήστες. (Lim M et. al., 2015). Ουσιαστικά, οι πληροφορίες που αποστέλλονται μέσω ενός δικτύου πρέπει να είναι κρυπτογραφημένες προκειμένου να καταστούν μη κατανοητές για όλους τους άλλους εκτός από τον προβλεπόμενο δέκτη. Σε αυτό το κεφάλαιο θα εστιάσουμε στη τεχνική της βιομετρικής κρυπτογράφησης που είναι υποκατηγορία της μεθόδου ενσωμάτωσης κλειδιού, αφού πρωτίστως γίνει μια σύντομη σύγκριση της με αυτή της παραδοσιακής κρυπτογράφησης.

Οι κρυπτογραφικές τεχνικές χρησιμοποιούν αλγόριθμους κρυπτογράφησης για την κρυπτογράφηση δεδομένων, τραπεζικών συναλλαγών, διαδικτυακών συναλλαγών, ασύρματων επικοινωνιών κ.λπ. Ως επί το πλείστον, η κρυπτογράφηση είναι μια διαδικασία ανακατανομής δεδομένων χρησιμοποιώντας μια μαθηματική συνάρτηση που ονομάζεται αλγόριθμος κρυπτογράφησης και ένα κλειδί που επηρεάζει τα αποτελέσματα αυτής της μαθηματικής συνάρτησης. Τα δεδομένα, πριν γίνουν κρυπτογραφημένα, λέγονται "καθαρό κείμενο", ενώ τα κρυπτογραφημένα δεδομένα λέγονται "κείμενο κρυπτογράφησης". Η ισχύς των κρυπτογραφημένων δεδομένων εξαρτάται γενικά από τον αλγόριθμο κρυπτογράφησης και το μέγεθος του κλειδιού κρυπτογράφησης. Πιο αναλυτικά, στην κρυπτογράφηση, ένα κλειδί (K1) χρησιμοποιείται για την κρυπτογράφηση ενός

μηνύματος (plaintext P) με τον αλγόριθμο κρυπτογράφησης (E) και έχει ως αποτέλεσμα το ciphertext (C). Κατά την αποκρυπτογράφηση, το ciphertext μετατρέπεται σε plaintext χρησιμοποιώντας ένα κλειδί (K2) και έναν αλγόριθμο αποκρυπτογράφησης (D). Υπάρχουν δύο τύποι κρυπτογράφησης: η συμμετρική κρυπτογράφηση και η ασύμμετρη κρυπτογράφηση. Η πιο γνωστή τεχνική που χρησιμοποιείται στην κρυπτογραφία είναι η τεχνική της συμμετρικής κρυπτογράφησης. Στη συμμετρική κρυπτογράφηση (π.χ., DES, AES), το ίδιο κλειδί (δηλαδή, K1 = K2 = K) χρησιμοποιείται στην διαδικασία της κρυπτογράφησης (C = EK (P)) και στην διαδικασία της αποκρυπτογράφησης (P = DK (C)). Ο αποστολέας κρυπτογραφεί το μήνυμα που θέλει να στείλει με ένα μυστικό κλειδί και ο παραλήπτης που έχει ένα αντίγραφο του ίδιου κλειδιού, αποκρυπτογραφεί το μήνυμα. Εάν ο αποστολέας θέλει να κρυπτογραφήσει ένα διαφορετικό μήνυμα και να το στείλει σε άλλο δέκτη, πρέπει να χρησιμοποιηθεί ένα διαφορετικό μυστικό κλειδί. Υπάρχουν δύο τύποι συμμετρικών αλγορίθμων που χρησιμοποιούνται αυτήν τη στιγμή, οι Stream ciphers και οι block ciphers.

Εικόνα 4.1: Συμμετρική κρυπτογράφηση και αποκρυπτογράφηση [69]

Παρόλο που η συμμετρική κρυπτογράφηση προσφέρει υψηλό επίπεδο ασφάλειας, δεν παρέχει ασφαλή μέσα ανταλλαγής κλειδιών, καθώς ενέχει ο κίνδυνος sniff των δεδομένων κατά τη μεταφορά. Μια λύση σε αυτό το πρόβλημα είναι η ασύμμετρη κρυπτογράφηση. Στην ασύμμετρη κρυπτογράφηση (π.χ. αλγόριθμος RSA, Diffie-Hellman), χρησιμοποιούνται δύο διαφορετικά κλειδιά (K1 και K2), το δημόσιο κλειδί χρησιμοποιείται για την κρυπτογράφηση ενός μηνύματος (C = EK1(P)), και το ιδιωτικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση του κειμένου κρυπτογράφησης σε απλό κείμενο (P = DK2(C)). Η προσέγγιση της ασύμμετρης κρυπτογράφησης χρησιμοποιεί ένα δημόσιο κλειδί, γνωστό σε όλους, για την κρυπτογράφηση του μηνύματος και ένα ιδιωτικό κλειδί, γνωστό μόνο στον προοριζόμενο δέκτη, για την αποκρυπτογράφηση του μηνύματος. Η κρυπτογράφηση δημόσιου κλειδιού που γίνεται σε ένα μήνυμα ή δεδομένα απλού κειμένου με τη χρήση ενός αλγορίθμου μπορεί να αποκρυπτογραφηθεί μόνο από το συζευγμένο ιδιωτικό κλειδί που είναι γνωστό μόνο στον δέκτη, εφαρμόζοντας τον ίδιο αλγόριθμο.



Εικόνα 4.2: Ασύμμετρη κρυπτογράφηση και αποκρυπτογράφηση [69]

Αν και η κρυπτογραφία είναι αποτελεσματική για την ασφαλή μετάδοση δεδομένων μέσω ενός μη ασφαλούς καναλιού, έχει αρκετά μειονεκτήματα. Ένα σημαντικό μειονέκτημα αποτελεί το γεγονός ότι το κρυπτογραφημένο μήνυμα βασίζεται στη κατοχή του κλειδιού και όχι στην αυθεντικότητα του χρήστη (οποιοσδήποτε μπορεί να αποκτήσει το κλειδί και να παριστάνει το νόμιμο χρήστη). (Stylios I. et al., 2016). Επιπρόσθετα, για να υπάρξει μια ισχυρή κρυπτογράφηση, το μήκος των κλειδιών που χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση πρέπει να είναι αρκετά μεγάλο. Ως εκ τούτου, η συντήρηση και η κοινή χρήση τέτοιων μεγάλων και τυχαίων κλειδιών γίνεται κρίσιμο πρόβλημα στα συστήματα κρυπτογράφησης. Επιπλέον, υπάρχει η πιθανότητα τα κλειδιά αυτά να μαντευτούν ή να σπάσουν από απλές επιθέσεις dictionary.

Αυτά τα προβλήματα αντιμετωπίζονται, χρησιμοποιώντας τα βιομετρικά κρυπτοσυστήματα. Καταρχάς, ο συνδυασμός κρυπτογραφίας και βιομετρικών στοιχείων είναι γνωστός ως βιομετρική κρυπτογραφία. Η ενσωμάτωση της βιομετρίας με τους κρυπτογραφικούς αλγόριθμους αποδίδουν ένα πολύ ισχυρό σύστημα γνωστό βιομετρικό κρυπτοσύστημα. Τέτοια συστήματα εκμεταλλεύονται το κρυπτογραφικό επίπεδο ασφάλειας μαζί με τη μοναδικότητα των βιομετρικών χαρακτηριστικών του χρήστη. Η ενσωμάτωση της βιομετρικής τεχνολογίας με την κρυπτογραφία καταργεί το πρόβλημα της απομνημόνευσης του κρυπτογραφικού κλειδιού και επιβεβαιώνει τη μη αποποίηση των χρηστών, καθώς τα βιομετρικά χαρακτηριστικά συνδέονται άμεσα με τον κάτοχο. (Kresimir Delac et al., 2004). Σε ένα τέτοιο σύστημα, η διαδικασία δημιουργίας κλειδιών περιλαμβάνει τη χρήση ενός βιομετρικού χαρακτηριστικού του χρήστη (π.χ. δακτυλικών αποτυπωμάτων, ίριδας, κτλ) που αποθηκεύεται σε μια βάση δεδομένων προσβάσιμη τόσο στον αποστολέα όσο και στον παραλήπτη. Όπως ήδη έχουμε αναφέρει, υπάρχουν διάφοροι τύποι κρυπτοσυστημάτων που διατίθενται για εφαρμογές βιομετρίας, όπως κρυπτοσυστήματα δέσμευσης κλειδιών, κρυπτοσυστήματα δημιουργίας κλειδιών, κτλ. Ωστόσο, το βιομετρικό κρυπτοσύστημα, αντιμετωπίζει και αυτό με την σειρά του μερικά προβλήματα. Οποιοδήποτε βιομετρικό σύστημα πρέπει να παρέχει προστασία βιομετρικών προτύπων που επιβεβαιώνει το απόρρητο και την ασφάλεια των βιομετρικών δεδομένων. Τα βιομετρικά δεδομένα που χρησιμοποιούνται σε ένα βιομετρικό σύστημα δεν πρέπει να διαρρέουν πληροφορίες σχετικά με τα βιομετρικά

χαρακτηριστικά. Απαιτείται επίσης να παρέχεται δυνατότητα ανάκλησης στα αμετάκλητα βιομετρικά δεδομένα.

Όπως σημειώθηκε στο προηγούμενο κεφάλαιο, ένα βιομετρικό σύστημα παράγει πάντα μια απάντηση Ναι / Όχι, η οποία είναι ουσιαστικά ένα κομμάτι πληροφοριών. Επομένως, ένας προφανής ρόλος των βιομετρικών στοιχείων στο συμβατικό κρυπτοσύστημα είναι απλώς η διαχείριση κωδικού πρόσβασης. Μόλις λάβει απάντηση Ναι, το σύστημα ξεκλειδώνει έναν κωδικό πρόσβασης ή ένα κλειδί και αυτό το κλειδί πρέπει να αποθηκευτεί σε ασφαλή τοποθεσία. Τα βιομετρικά πρότυπα που είναι αποθηκευμένα σε μια βάση δεδομένων μπορούν να κρυπτογραφηθούν με συμβατικά κρυπτογραφικά μέσα. Αυτό θα βελτιώσει το επίπεδο ασφάλειας του συστήματος, αφού ένας εισβολέας πρέπει πρώτα να αποκτήσει πρόσβαση στα κλειδιά κρυπτογράφησης.

4.2 Βιομετρική κρυπτογράφηση

Η βιομετρική κρυπτογράφηση είναι μια διαδικασία που δεσμεύει με ασφάλεια ένα κρυπτογραφικό κλειδί σε ένα βιομετρικό δείγμα, έτσι ώστε ούτε το κλειδί ούτε το βιομετρικό δείγμα να μπορούν να ανακτηθούν από το αποθηκευμένο πρότυπο. Το κλειδί δημιουργείται εκ νέου μόνο εάν το σωστό βιομετρικό δείγμα παρουσιαστεί κατά την επαλήθευση. Το ψηφιακό κλειδί δημιουργείται τυχαία κατά την εγγραφή, είναι εντελώς ανεξάρτητο από τα βιομετρικά στοιχεία και, ως εκ τούτου, μπορεί πάντα να αλλάξει ή να ενημερωθεί. Μετά την απόκτηση ενός βιομετρικού δείγματος, ο αλγόριθμος που χρησιμοποιείται κατά την βιομετρική κρυπτογράφηση δεσμεύει με ασφάλεια το κλειδί με το βιομετρικό χαρακτηριστικό και δημιουργεί ένα προστατευμένο πρότυπο. (Ngo D. C. L. Et. al., 2015). Το πρότυπο αυτό μπορεί να αποθηκευτεί, είτε σε μια βάση δεδομένων, είτε τοπικά (σε μια έξυπνη κάρτα, έναν υπολογιστή, ένα κινητό τηλέφωνο ή οποιαδήποτε άλλη συσκευή). Στο τέλος της εγγραφής, το κλειδί και το βιομετρικό δείγμα απορρίπτονται. Κατά την επαλήθευση, ο χρήστης παρουσιάζει το νέο βιομετρικό δείγμα, το οποίο, όταν εφαρμόζεται στο νόμιμο πρότυπο, θα επιτρέψει στον αλγόριθμο βιομετρικής κρυπτογράφησης να ανακτήσει το ίδιο κλειδί / κωδικό πρόσβασης. Έτσι, το βιομετρικό χαρακτηριστικό χρησιμεύει ως κλειδί αποκρυπτογράφησης. Στο τέλος της επαλήθευσης, το βιομετρικό δείγμα απορρίπτεται και πάλι. Ο αλγόριθμος βιομετρικής κρυπτογράφησης έχει σχεδιαστεί για να λαμβάνει υπόψη αποδεκτές παραλλαγές κατά την είσοδο του βιομετρικού χαρακτηριστικού. Ωστόσο, ένας εισβολέας του οποίου το βιομετρικό δείγμα είναι αρκετά διαφορετικό δεν θα μπορεί να ανακτήσει τον κωδικό πρόσβασης. Μετά την ανάκτηση του ψηφιακού κλειδιού, επιτρέπεται στον χρήστη η πρόσβαση στους πόρους του εκάστοτε πληροφοριακού συστήματος ή της εκάστοτε εφαρμογής. (Tiwalade O. Majekodunmi et. al., 2011). Συνολικά, η λειτουργία της βιομετρικής κρυπτογράφησης είναι ένα αποτελεσματικό, ασφαλές και φιλικό ως προς το απόρρητο εργαλείο για τη διαχείριση βιομετρικών κωδικών πρόσβασης.

Οι μέθοδοι βιομετρικής κρυπτογράφησης αναπτύχτηκαν αρχικά με σκοπό να προστατέψουν ένα κρυπτογραφημένο κλειδί χρησιμοποιώντας βιομετρικά δεδομένα ή για να παράγουν ένα κρυπτογραφημένο κλειδί από αυτά. Ωστόσο, μπορούν να χρησιμοποιηθούν και ως μηχανισμοί προστασίας βιομετρικών προτύπων. Σε ένα τέτοιο σύστημα αυτό που αποθηκεύεται είναι κάποια πληροφορία σχετικά με το βιομετρικό πρότυπο που είναι γνωστή ως βοηθητική πληροφορία. Παρόλο που η βοηθητική πληροφορία δεν αποκαλύπτει σημαντικά στοιχειά για το αποθηκευμένο βιομετρικό πρότυπο, είναι απαραίτητη για τη προσπέλαση του συστήματος και για την εξαγωγή ενός κρυπτογραφημένου κλειδιού από τα βιομετρικά χαρακτηριστικά. Η αντιστοίχιση γίνεται έμμεσα πιστοποιώντας την εγκυρότητα του εξαγόμενου κλειδιού. Συνήθως, οι μέθοδοι αυτές στηρίζονται σε κώδικες διόρθωσης λαθών για να διαχειριστούν τις ενδοατομικές παραλλαγές. Τα συστήματα βιομετρικής κρυπτογράφησης, ανάλογα με το πώς εξάγονται τα βοηθητικά δεδομένα, μπορούν να

διαχωριστούν περαιτέρω σε δυο γενικές κατηγορίες όπως αναφέραμε συνοπτικά στο προηγούμενο κεφάλαιο: τα συστήματα συσχέτισης κλειδιού **key binding cryptosystems** και τα συστήματα παραγωγής κλειδιού **key generation cryptosystems**. Όταν τα βοηθητικά δεδομένα εξάγονται από την τη διασύνδεση ενός κλειδιού (που είναι ανεξάρτητο από τα βιομετρικά χαρακτηριστικά) με το βιομετρικό πρότυπο τότε το σύστημα αναφέρεται ως σύστημα συσχέτισης κλειδιού. Αξίζει να σημειωθεί ότι εάν είναι γνωστά μόνο τα βοηθητικά δεδομένα είναι υπολογιστικά αδύνατο να ανακτηθεί είτε το κλειδί είτε το βιομετρικό πρότυπο. Η αντιστοίχηση σε ένα τέτοιο σύστημα περιλαμβάνει ανάκτηση του κλειδιού από τα βοηθητικά δεδομένα χρησιμοποιώντας τα βιομετρικά χαρακτηριστικά που εξάγονται κατά την προσπέλαση του συστήματος. Αντίθετα, στα συστήματα παραγωγής κλειδιού τα βοηθητικά δεδομένα εξάγονται κατευθείαν από το βιομετρικό πρότυπο και το κρυπτογραφικό κλειδί παράγεται από τα βοηθητικά δεδομένα και τα νέα βιομετρικά χαρακτηριστικά. Στις επόμενες παραγράφους θα αναλύσουμε αυτές τις δυο μεθόδους, ώστε να υπάρξει μια σαφής και ολοκληρωμένη εικόνα γύρω από αυτά τα κρυπτοσυστήματα.

Τεχνική	Τρόπος λειτουργίας	Δυνατά σημεία	Αδυναμίες
Key binding	Ένα τυχαίο κλειδί ενσωματώνεται με ασφάλεια στα βιομετρικά δεδομένα.	i) Δεν είναι δυνατή η ανάκτηση των δεδομένων χωρίς τη γνώση του μυστικού κλειδιού. ii) Εγγυάται το απόρρητο του χρήστη καθώς τα κρυπτογραφικά κλειδιά είναι ανεξάρτητα από τα βιομετρικά δεδομένα.	Ενας εισβολέας που γνωρίζει το μυστικό κλειδί μπορεί να ανακτήσει τα βιομετρικά δεδομένα από προστατευμένο πρότυπο.
Key generation	Δημιουργεί ένα κλειδί απευθείας από βιομετρικά χαρακτηριστικά που έχουν εξαχθεί.	i) Παρέχει ασφάλεια και απόρρητο εξαλείφοντας την άμεση αποθήκευση βιομετρικών δεδομένων. ii) Είναι δύσκολο για τους εισβολείς να ανακατασκευάσουν πρωτότυπα βιομετρικά δεδομένα από βασική συμβολοσειρά, καθώς τα βιομετρικά δεδομένα δεν διατηρούνται μετά την εγγραφή.	Αφού δεν αποθηκεύονται τα βοηθητικά δεδομένα δεν μπορούν να ενημερωθούν τα κλειδιά.

Πίνακας 4.3: Σύγκριση μεθόδων παραγωγής κλειδιού και συσχέτισης κλειδιού

Η μέθοδος παραγωγής κλειδιού

Η απευθείας παραγωγή κρυπτογραφικών κλειδιών από τα βιομετρικά δεδομένα είναι μια πολύ ελκυστική προσέγγιση αλλά παραμένει ένα δύσκολο πρόβλημα λόγο των ενδοατομικών παραλλαγών. Δυο τεχνικές που χρησιμοποιούν τη μέθοδο της παραγωγής κλειδιού είναι το secure sketch και το fuzzy extractor. Το secure sketch μπορεί να θεωρηθεί ως βοηθητικό δεδομένο που διαρρέει μόνο περιορισμένη πληροφορία σχετικά με το πρότυπο αλλά διευκολύνει την ακριβή ανακατασκευή του προτύπου όταν τα βιομετρικά δεδομένα κατά την διάρκεια της προσπέλασης του συστήματος είναι παρόμοια με αυτά που χρησιμοποιήθηκαν για την παραγωγή του προτύπου. Το fuzzy extractor είναι μια κρυπτογραφική συνάρτηση που παράγει το κρυπτογραφικό κλειδί από τα βιομετρικά χαρακτηριστικά. (Yogendra Narain Singh et al.,2013). Τα βιομετρικά συστήματα που βασίζονται στη μέθοδο της παραγωγής κλειδιού έχουν εν γένει το μειονέκτημα της χαμηλής ικανότητας διαχωρισμού που μπορεί να εκτιμηθεί με την σταθερότητα του κλειδιού και την εντροπία του κλειδιού. Η σταθερότητα του κλειδιού αναφέρεται στο κατά πόσο το κλειδί που παράγεται από τα βιομετρικά δεδομένα επαναλαμβάνεται, ενώ η εντροπία κλειδιού αναφέρεται στον αριθμό των δυνατών κλειδιών που μπορεί να παραχθούν. Για παράδειγμα, εάν το σύστημα παράγει το ίδιο κλειδί ανεξάρτητα από το βιομετρικό πρότυπο που δέχεται ως είσοδο τότε έχει μεγάλη σταθερότητα αλλά μηδενική εντροπία και αυτό θα έχει ως αποτέλεσμα μεγάλο ρυθμό εσφαλμένης αποδοχής. Αντίθετα, αν το σύστημα

παράγει διαφορετικά κλειδιά για βιομετρικά πρότυπα που διαφέρουν ελάχιστα τότε το σύστημα θα έχει μεγάλη εντροπία αλλά πολύ χαμηλή σταθερότητα με αποτέλεσμα τον υψηλό ρυθμό εσφαλμένης απόρριψης. Ωστόσο, το κύριο μειονέκτημα αυτής της μεθόδου είναι η δυσκολία να σχεδιαστεί ένα σύστημα που να έχει ταυτόχρονα υψηλή σταθερότητα και εντροπία.

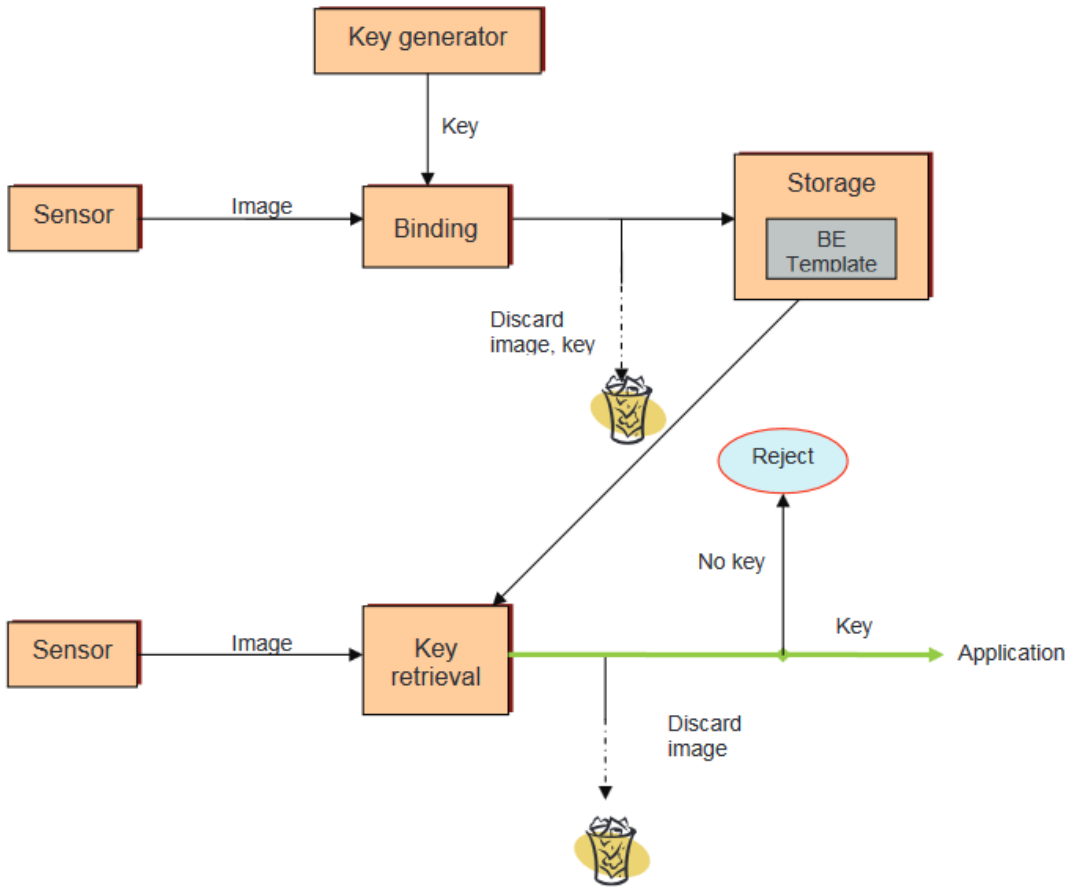
Η μέθοδος συσχέτισης κλειδιού

Στα συστήματα συσχέτισης κλειδιού το βιομετρικό πρότυπο προστατεύεται με το να συσχετίζεται με κάποιο κρυπτογραφημένο κλειδί. Μια μοναδική οντότητα που εμπεριέχει και το κλειδί και το βιομετρικό πρότυπο αποθηκεύεται στη βάση δεδομένων του συστήματος και αποτελεί τα βοηθητικά δεδομένα. Η οντότητα αυτή δεν αποκαλύπτει σημαντική πληροφορία για το αρχικό βιομετρικό πρότυπο και είναι υπολογιστικά ανέφικτο να αποκρυπτογραφηθεί χωρίς να είναι γνωστά τα βιομετρικά δεδομένα του χρήστη. Συνήθως, τα βοηθητικά δεδομένα είναι ένας συνδυασμός ενός κώδικα διόρθωσης λαθών και του βιομετρικού προτύπου. Όταν τα βιομετρικά δεδομένα κατά τη διάρκεια της προσπέλασης του συστήματος διαφέρουν από το βιομετρικό πρότυπο μέσα σε κάποια όρια ανοχής σφάλματος, η κωδικοποιημένη λέξη που αντιστοιχεί στα δεδομένα αυτά αποκωδικοποιείται και μπορεί να χρησιμοποιηθεί για την ανάκτηση του κλειδιού. Το κύριο πλεονέκτημα αυτής της μεθόδου είναι η ανθεκτικότητα σε ενδοατομικές παραλλαγές και το ότι η ανεκτικότητα σε σφάλματα μπορεί να καθοριστεί εύκολα από την ικανότητα διόρθωσης λαθών του κώδικα που χρησιμοποιείται. (Supriya V. G. et al., 2014). Το μειονέκτημα είναι ότι η πιστοποίηση γίνεται μόνο χρησιμοποιώντας μεθόδους διόρθωσης λαθών, κάτι που αποκλείει τη χρήση εξεζητημένων μεθόδων για την αντιστοίχηση των βιομετρικών δεδομένων. Το πιο γνωστό σχήμα συσχέτισης κλειδιού ονομάζεται fuzzy commitment. Κατά την εγγραφή, δεσμεύεται μια κωδικοποιημένη λέξη c ενός κώδικα διόρθωσης λαθών χρησιμοποιώντας ως παράμετρο το διάνυσμα χαρακτηριστικών b. Τα βοηθητικά δεδομένα αποτελούνται από το h(c) και το b-c όπου h() είναι μια συνάρτηση hash function. Κατά την αυθεντικοποίηση αφαιρείται η ποσότητα b-c από το νέο διάνυσμα χαρακτηριστικών b’ του χρήστη και προκύπτει η ποσότητα c’= b’ –b+c=δ+c όπου δ= b’-b είναι η διαφορά στην αναπαράσταση των βιομετρικών χαρακτηριστικών. Εάν η διαφορά αυτή είναι αρκετά μικρή τότε το c’ διαφέρει πολύ λίγο από το c και θα μπορεί να αποκωδικοποιηθεί με τον κώδικα διόρθωσης λαθών. Μια παρόμοια μέθοδος που χρησιμοποιεί κώδικες διόρθωσης λαθών για να διαχειριστούν τη διαφορά στην αναπαράσταση των βιομετρικών δεδομένων ονομάζεται fuzzy vault.

Μέθοδος	Τρόπος λειτουργίας	Δυνατά σημεία	Αδυναμίες
Βιομετρική κρυπτογράφηση	Εφαρμόζει έναν αλγόριθμο κρυπτογράφησης για τη δημιουργία ασφαλούς βιομετρικού προτύπου	Αποτρέπει έναν εισβολέα από την αποκρυπτογράφηση προστατευμένων προτύπων χωρίς τη γνώση του αλγορίθμου και του κρυπτογραφικού κλειδιού	Ευπαθή σε επίθεση masquerade attack
Fuzzy commitment	Χρησιμοποιεί τεχνικές κρυπτογράφησης και διόρθωσης σφαλμάτων για τη σύνδεση μυστικών πληροφοριών σε βιομετρικά δεδομένα.	Αποθηκεύεται μόνο η τιμή κατακερματισμού προστατεύοντας έτσι το μυστικό κλειδί.	Ευπαθή σε επιθέσεις στους κώδικες διόρθωσης λαθών (ECC)
	Χρησιμοποιεί ένα μη οργανωμένο σύνολο	Το μέρος όπου αποθηκεύεται το κλειδί	Ευπαθή σε επιθέσεις πολλαπλών εγγραφών

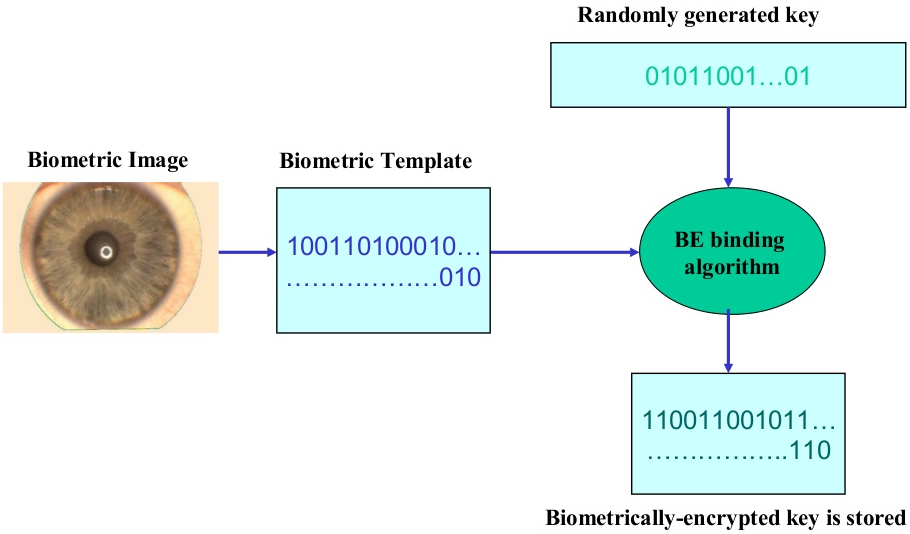
Fuzzy vault	βιομετρικών δεδομένων για να κλειδώσει ένα μυστικό κλειδί	δεν μπορεί να αποκωδικοποιηθεί χωρίς τα έγκυρα βιομετρικά δεδομένα.	(ARM)

Πίνακας 4.4 Σύγκριση των τεχνικών βιομετρικής κρυπτογράφησης, fuzzy commitment και fuzzy vault



Εικόνα 4.4. Διαδικασία βιομετρικής κρυπτογράφησης [9]

Σε αυτή την εργασία θα ασχοληθούμε περισσότερο με τη μέθοδο συσχέτισης κλειδιού καθώς με αυτή τη μέθοδο γίνεται η τεχνική της βιομετρικής κρυπτογράφησης. Η Mytec Technologies Inc., με έδρα το Τορόντο του Καναδά το 1994, ανέπτυξε αυτή τη καινοτόμο τεχνική για την προστασία ενός κλειδιού με τη χρήση βιομετρίας. Σε αυτή την τεχνική το κλειδί συνδέεται με τη βιομετρικό χαρακτηριστικό σε θεμελιώδες επίπεδο, κατά την εγγραφή, και ανακτάται αργότερα χρησιμοποιώντας το ίδιο βιομετρικό χαρακτηριστικό κατά τη διάρκεια της επαλήθευσης. (NaliniK. Ratha et. Al., 2001). Επιπλέον, το κλειδί έχει μέγεθος συνήθως 128 bit και είναι εντελώς ανεξάρτητο από τα βιομετρικά δεδομένα, πράγμα που σημαίνει ότι, πρώτον, εάν το κλειδί παραβιαστεί, η χρήση του συγκεκριμένου βιομετρικού χαρακτηριστικού θα συνεχίσει να υφίσταται, και δεύτερον, το κλειδί μπορεί εύκολα να τροποποιηθεί ή να ενημερωθεί αργότερα. Η διαδικασία που αναπτύχθηκε από την Mytec Technologies ονομάζεται **βιομετρική κρυπτογράφηση**. Κατά τη διάρκεια της εγγραφής, η διαδικασία βιομετρικής κρυπτογράφησης συνδυάζει τη βιομετρική εικόνα με ένα ψηφιακό κλειδί για να δημιουργήσει ένα ασφαλές μπλοκ δεδομένων, γνωστό ως Bioscrypt (βοηθητικά δεδομένα). Το Bioscrypt είναι ασφαλές, καθώς ούτε το βιομετρικό χαρακτηριστικό, ούτε το κλειδί μπορούν να ληφθούν ανεξάρτητα από αυτό. (Prabhakar S. et. Al., 2003)



Εικόνα 4.5: Διαδικασία της εγγραφή ενός βιομετρικού δείγματος με τη μεθόδου της βιομετρικής κρυπτογράφησης [65]

Κατά τη διάρκεια της επαλήθευσης, ο αλγόριθμος της βιομετρικής κρυπτογράφησης ανακτά το κρυπτογραφικό κλειδί συνδυάζοντας τη βιομετρική εικόνα με το Bioscrypt. Έτσι, η βιομετρική κρυπτογράφηση δεν παρέχει απλώς μια απάντηση ναι ή όχι στον έλεγχο ταυτότητας χρήστη για να διευκολύνει την απελευθέρωση ενός κλειδιού, αλλά αντ 'αυτού ανακτά ένα κλειδί που μπορεί να αναδημιουργηθεί μόνο εάν συνδυαστεί η βιομετρική εικόνα με το Bioscrypt.

Για παράδειγμα έστω ότι η Αλίκη, ένας νόμιμος χρήστης, επιθυμεί να αποκτήσει πρόσβαση σε συγκεκριμένο ψηφιακό περιεχόμενο και προσφέρει το βιομετρικό της δείγμα στο σύστημα. Εάν ο η μονάδα αντιστοίχησης του συστήματος ταιριάξει με επιτυχία το βιομετρικό δείγμα εισόδου της Αλίκης με το εγγεγραμμένο βιομετρικό πρότυπο της, τότε απελευθερώνεται ένα κρυπτογραφικό κλειδί. Το κρυπτογραφικό κλειδί χρησιμοποιείται για την αποκρυπτογράφηση του περιεχομένου και, συνεπώς, επιτρέπεται στην Αλίκη η πρόσβαση στο περιεχόμενο. Από την άλλη πλευρά, εάν ο Βίκτωρ, ένας παράνομος χρήστης προσπαθήσει να αποκτήσει πρόσβαση στο ψηφιακό περιεχόμενο της Αλίκης, η βιομετρική αντιστοιχία του με το βιομετρικό πρότυπο της Αλίκης θα αποτύχει και το κρυπτογραφικό κλειδί της Αλίκης δεν θα απελευθερωθεί από το σύστημα. Ας περιγράψουμε εν συντομία τα βήματα που πραγματοποιούνται κατά την διαδικασία της βιομετρικής κρυπτογράφησης σύμφωνα με το παραπάνω παράδειγμα.

1. Η Αλίκη δημιουργεί ένα πρότυπο βιομετρικής κρυπτογράφησης από το βιομετρικό χαρακτηριστικό της και ένα τυχαία επιλεγμένο κωδικό. Ούτε το βιομετρικό χαρακτηριστικό ούτε ο κωδικός μπορούν να ανακτηθούν από το πρότυπο.

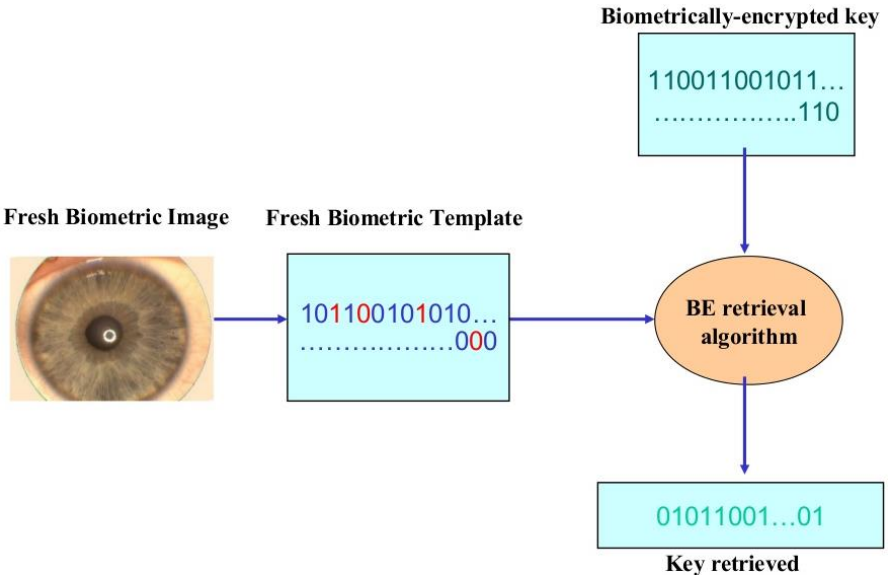
2. Ο κωδικός χρησιμοποιείται για τη δημιουργία ενός ζεύγους κλειδιών (δημόσιο και ιδιωτικό).

3. Το βιομετρικό χαρακτηριστικό, ο κωδικός και το ιδιωτικό κλειδί απορρίπτονται.

4.Το πρότυπο της βιομετρικής κρυπτογράφησης μπορεί να αποθηκευτεί σε μια έξυπνη κάρτα ή σε φορητό υπολογιστή της Αλίκης που διαθέτει επίσης βιομετρικό αισθητήρα.

Το σημαντικό σημείο είναι ότι το πιο κρίσιμο μέρος οποιουδήποτε κρυπτοσυστήματος, ο κωδικός πρόσβασης, συνδέεται με ασφάλεια με τα βιομετρικά στοιχεία. Ούτε το βιομετρικό της Αλίκης

ούτε ο κωδικός της αποθηκεύονται και συνεπώς ούτε αποκαλύπτονται. Ως αποτέλεσμα, το σύστημα είναι εξαιρετικά ασφαλές και διαφυλάσσει το απόρρητο των προσωπικών δεδομένων.



Εικόνα 4.6: Διαδικασία της αυθεντικοποίησης ενός νέου βιομετρικού δείγματος με τη μεθόδου της βιομετρικής κρυπτογράφησης [65]

Όπως επισημάνθηκε, η δημιουργία κλειδιών παραμένει ένας σημαντικός παράγοντας σε οποιαδήποτε λύση κρυπτογραφικής ασφάλειας. Η δημιουργία κλειδιών από βιομετρικά δείγματα ζητά την εξαγωγή σχετικών χαρακτηριστικών από τα φυσιολογικά σήματα και τη μετατροπή τους σε τυχαία δυαδική ακολουθία (μέσω συναρτήσεων κατακερματισμού ή τεχνικών κωδικοποίησης, δημιουργείται η δυαδική ακολουθία). (Natgunanathan I. et.al.,2018). Η εφαρμογή συναρτήσεων κρυπτογραφικού κατακερματισμού είναι μια υπολογιστικά αποδοτική λειτουργία που χαρτογραφεί δυαδικές συμβολοσειρές αυθαίρετου μήκους σε δυαδικές συμβολοσειρές ορισμένου μήκους, που αναφέρονται ως τιμές κατακερματισμού. Στα σχήματα δέσμευσης κλειδιών, ένα κρυπτογραφικό κλειδί δημιουργείται τυχαία κατά τη διάρκεια του σταδίου εγγραφής αλλά είναι ανεξάρτητο από τα βιομετρικά πρότυπα και μπορεί να αλλάξει όταν χρειάζεται. Για τη δέσμευση ενός δυαδικού κλειδιού K, δημιουργείται ένας κωδικός C με βάση το K χρησιμοποιώντας έναν προκαθορισμένο κωδικό διόρθωσης σφαλμάτων. Η τελική δέσμευση θα είναι (h (C), BC), όπου το B είναι ένα βιομετρικό δυαδικό πρότυπο και το h είναι μια συνάρτηση κρυπτογραφικού κατακερματισμού το οποίο και αποθηκεύεται στη βάση δεδομένων. Για να αποδεσμευτεί μια δέσμευση, ένα άτομο πρέπει να παράσχει ένα νέο βιομετρικό δείγμα B0 το οποίο είναι αρκετά κοντά στο B και στη συνέχεια χρησιμοποιείται h (C) για να επαληθευτεί ότι έχει απελευθερωθεί το σωστό κλειδί. Ενώ τα βιομετρικά δεδομένα είναι ασταθή λόγω των ενδοατομικών παραλλαγών, τα κρυπτογραφικά κλειδιά πρέπει να είναι σταθερά και να επαναλαμβάνονται κάθε φορά. Για να γεφυρωθεί αυτό το κενό, τα συστήματα δέσμευσης κλειδιών βασίζονται συνήθως σε τεχνικές διόρθωσης σφαλμάτων, όπως κωδικοί διόρθωσης σφαλμάτων (ECC). Οι τεχνικές διόρθωσης σφαλμάτων που έχουν υιοθετηθεί θα πρέπει να είναι ικανές να διορθώσουν έως και έναν συγκεκριμένο αριθμό δυαδικών ψηφίων που εξαρτάται από το επιδιωκόμενο μέγεθος κλειδιού, το μέγεθος του βιομετρικού προτύπου και την ποσότητα ανεκτής παραμόρφωσης στα βιομετρικά δεδομένα για να ικανοποιήσουν επαρκή παραλλαγή στα δείγματα των χρηστών. (NaliniK. Ratha et. Al., 2001). Το κωδικοποιημένο κρυπτογραφικό κλειδί γίνεται XOR με τη δυαδική αναπαράσταση βιομετρικών

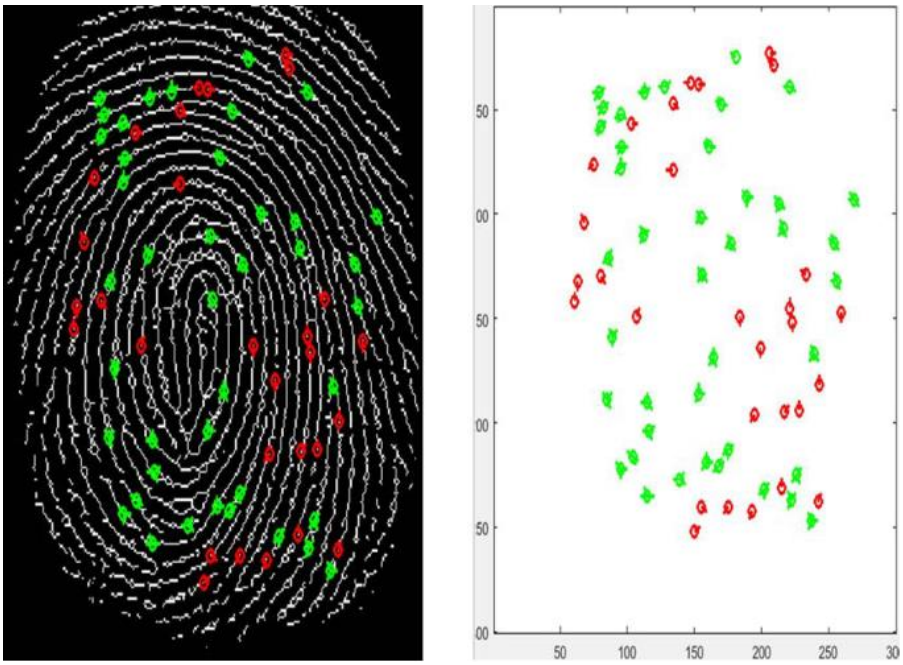
δεδομένων για να αποδώσει αυτό που είναι γνωστό ως βοηθητικά δεδομένα. Το κλειδί απορρίπτεται και τα βοηθητικά δεδομένα αποθηκεύονται μαζί με το κατακερματισμό του κλειδιού. Στο στάδιο επαλήθευσης (στάδιο ανάκτησης κλειδιού), η δυαδική αναπαράσταση υπολογίζεται χρησιμοποιώντας ένα νέο βιομετρικό δείγμα με τον ίδιο τρόπο όπως περιγράφεται παραπάνω και στη συνέχεια γίνεται XOR με τα βοηθητικά δεδομένα. Στη συνέχεια, χρησιμοποιείται η τεχνική διόρθωσης σφαλμάτων στη λειτουργία αποκωδικοποίησης. Η διόρθωση επιτυγχάνεται και το αρχικό κρυπτογραφικό κλειδί αναπαράγεται εάν η διαφορά μεταξύ του βιομετρικού δείγματος και του νέου βιομετρικού δείγματος βρίσκεται εντός ενός προκαθορισμένου κατωφλίου, δηλαδή σε περίπτωση που το νέο βιομετρικό δείγμα ανήκει στο ίδιο άτομο. Το προκαθορισμένο κατώφλι προσδιορίζεται με τον ίδιο τρόπο όπως γίνεται κατά τον καθορισμό του ορίου βιομετρικής επαλήθευσης μέσω ενός πρωτοκόλλου εκπαίδευσης, το οποίο εξαρτάται από την εφαρμογή, όπου επιλέγονται κατάλληλα ποσοστά σφάλματος ανοχής σε όρους FAR και FRR. (Roberts C., 2007). Τέτοια κατώτατα όρια εξαρτώνται από την εφαρμογή, όπου σε ορισμένες εφαρμογές ενδέχεται να απαιτείται λιγότερη ανοχή στο FAR από ότι στο FRR και αντίστροφα.

4.3 Δημιουργία κρυπτογραφικών κλειδιών από βιομετρικά δεδομένα

Ενδιαφέρον παρουσιάζει και η διαδικασία δημιουργίας κρυπτογραφικών κλειδιών από τα εξαγόμενα χαρακτηριστικά των βιομετρικών δεδομένων, κάτι που θα αναλύσουμε σε αυτή την υποενότητα. Δεδομένου ότι σήμερα τα δακτυλικά αποτυπώματα είναι η πιο δημοφιλής βιομετρική μέθοδος, θα παρουσιάσουμε την παραπάνω διαδικασία με βάση ότι το βιομετρικό δείγμα που παρουσιάζεται στον αισθητήρα είναι τα δακτυλικά αποτυπώματα.

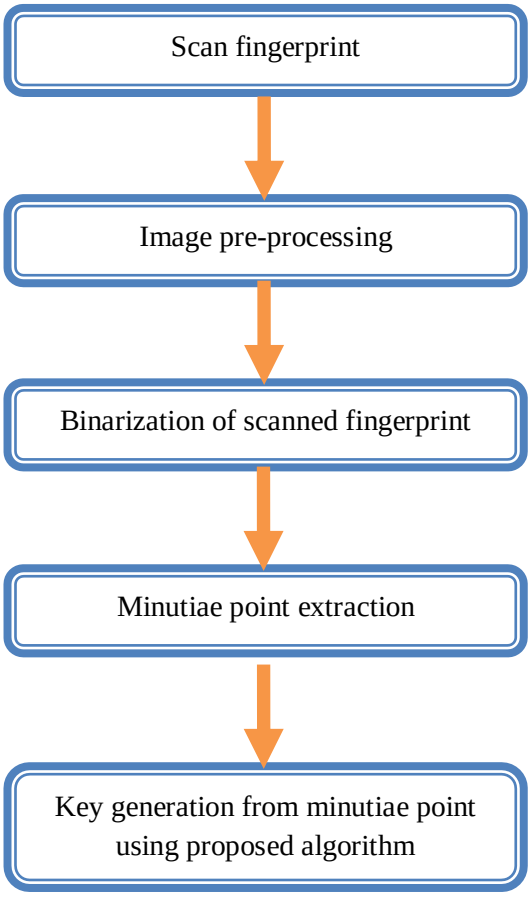
Η αποτελεσματικότητά του αλγόριθμου δημιουργίας κρυπτογραφικών κλειδιών έγκειται στην ικανότητά του να δημιουργεί το κλειδί από τα εξαγόμενα σημεία λεπτομερειών των βιομετρικών δακτυλικών αποτυπωμάτων. (Uludag U. et al., 2004). Όπως φαίνεται παρακάτω, υπάρχουν τρία στάδια που εμπλέκονται σε αυτό το μοντέλο: (i) προ-επεξεργασία, (ii) εξαγωγή λεπτομερειών και (iii) τελική επεξεργασία.

- Προ-επεξεργασία: Αποτελεί το αρχικό στάδιο της όλης διαδικασίας και πραγματοποιείται με τη σάρωσης των δακτυλικών αποτυπωμάτων χρησιμοποιώντας έναν σαρωτή, έτσι ώστε να «ανέβει» ένα ψηφιακό αντίγραφο του στον υπολογιστή για περαιτέρω επεξεργασία. Κατά το στάδιο της προ-επεξεργασίας, η καταγεγραμμένη εικόνα θα βελτιστοποιηθεί χρησιμοποιώντας τεχνικές φιλτραρίσματος εικόνων. Το φιλτράρισμα είναι μια τεχνική βελτίωσης μιας εικόνας για την επισήμανση ή την εξάλειψη ορισμένων χαρακτηριστικών.
- Εξαγωγή λεπτομερειών των χαρακτηριστικών: Το ψηφιακό αντίγραφο του σαρωμένου δακτυλικού αποτυπώματος υποβάλλεται σε επεξεργασία για την εξαγωγή του σημείου λεπτομερειών. Οι κοιλάδες και οι παρυφές των δακτυλικών αποτυπωμάτων χρησιμοποιούνται από το σύστημα λόγω των διακριτών χαρακτηριστικών τους. Η κατεύθυνση (δηλαδή η γωνία) και ο τύπος (δηλαδή η διακλάδωση / τερματισμός) είναι μερικά από τα χαρακτηριστικά που λαμβάνονται υπόψη για τη δημιουργία του πρότυπου. (Ngo D. C. L. Et. al., 2015). Η επιτυχής εξαγωγή των λεπτομερειών απαιτεί στη συνέχεια αποθήκευση σε ένα πρότυπο.
- Τελική επεξεργασία: Η αραίωση παρυφών που απαιτείται για την αναγνώριση λεπτομερειών αποτελεί το τελικό στάδιο.



Εικόνα 4.7: Διαδικασία εξαγωγής λεπτομερειών από ένα δακτυλικό αποτύπωμα [41]

Στη συνεχεία ακολουθεί η δυαδική μετατροπή των εικόνων (Binarization) του σαρωμένου δακτυλικού αποτυπώματος. Μια τέτοια μέθοδος ελέγχει κάθε τιμή pixel και τη συγκρίνει με την τιμή μέσης έντασης φωτεινότητας. Έτσι η εικόνα αυτή θα προβεί σε μετασχηματισμό εικόνας 1-bit για ψηφιακή επεξεργασία όπου το pixel που αντιπροσωπεύει ένα σημείο παρυφών (μαύρο) θα του αποδίδεται η τιμή 0 και στα σημεία κοιλάδων (άσπρο) θα αποδίδεται η τιμή 1. Τέλος δημιουργούνται τα κλειδιά από τον αλγόριθμο δημιουργίας κρυπτογραφικών κλειδιών ο οποίος έχει ως εξής: οι συντεταγμένες και οι γωνίες των λεπτομερειών μετρώνται και οι τιμές δεδομένων εξάγονται. Πιο αναλυτικά όπως φαίνεται και από την εικόνα, το Ridge Ending (RIG) επισημαίνεται με κόκκινο χρώμα και το Bifurcation (BIF) επισημαίνεται με πράσινο χρώμα. Έπειτα, υπολογίζονται οι μέσες τιμές των συντεταγμένων σημείου X και Y και της γωνίας προσανατολισμού θ. Οι έξοδοι που προκύπτουν είναι δεκαδικά για τις συντεταγμένες X και Y και τα ακτίνια για τη γωνία θ. Αυτές οι τιμές εξόδου μετατρέπονται σε δυαδική αναπαράσταση. Συνδυάζοντας αυτές τις τρεις τιμές, θα δημιουργηθεί ένα ιδιωτικό κλειδί για τη δεδομένη εικόνα δακτυλικών αποτυπωμάτων. Στη συνέχεια, τα κρυπτογραφικά κλειδιά δημιουργούνται από τις αντίστοιχες τιμές αυτών των λεπτομερειών.



Εικόνα 4.8: Διαδικασία παραγωγής κλειδιού [41]

Ο χρόνος λειτουργίας σε δευτερόλεπτα για όλη τη διαδικασία κρυπτογράφησης έχει ως εξής: Η εξαγωγή χαρακτηριστικών του βιομετρικού προτύπου χρειάζεται περίπου 0,05 δευτερόλεπτα. Η δημιουργία ενός προτύπου από το εξαγόμενο βιομετρικό χαρακτηριστικό χρειάζεται 0,002 δευτερόλεπτα. Η κωδικοποίηση και η αποκωδικοποίηση του προτύπου σε μια συνάρτηση που χρησιμοποιείται για τη δημιουργία κλειδιών χρειάζεται 0,15 δευτερόλεπτα. Τέλος, η δημιουργία κρυπτογραφικών κλειδιών (δημόσιων / ιδιωτικών) χρειάζεται 0,002 δευτερόλεπτα. Ο συνολικός χρόνος που απαιτείται για ολόκληρη τη λειτουργία είναι 0,204 δευτερόλεπτα.

4.4 Πλεονεκτήματα βιομετρικής κρυπτογράφησης

Οι τεχνολογίες βιομετρικής κρυπτογράφησης παρέχουν τεράστιες δυνατότητες για την ενίσχυση της ιδιωτικής ζωής και της ασφάλειας. Μερικά από τα βασικά πλεονεκτήματα αυτής της τεχνικής αναγράφονται παρακάτω:

- **Αποθηκεύονται μόνο τα βοηθητικά δεδομένα και όχι η βιομετρική εικόνα ή το πρότυπο:** Οι περισσότερες ανησυχίες για την προστασία της ιδιωτικής ζωής και της ασφάλειας προέρχονται από την αποθήκευση και την κακή χρήση των βιομετρικών δεδομένων. (Vincenzo Conti et al, 2017). Οι ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και την ασφάλεια περιλαμβάνουν φόβους για πιθανή αντιστοίχιση δεδομένων, παρακολούθηση προφίλ, παραβίαση ασφάλειας δεδομένων και κλοπή

ταυτότητας από τρίτους. Η βιομετρική κρυπτογράφηση αντιμετωπίζει άμεσα αυτούς τους κινδύνους και οι χρήστες διατηρούν τον πλήρη (τοπικό) έλεγχο των δικών τους βιομετρικών στοιχείων.

- **Υπάρχει δυνατότητα αλλαγής ή ακύρωσης:** Η τεχνική της βιομετρικής κρυπτογραφίας επιτρέπει την αλλαγή ή την ακύρωση του κωδικού που συνδέεται με το βιομετρικό χαρακτηριστικό. Δηλαδή, τα αναγνωριστικά μπορεί να ανακληθούν ή να ακυρωθούν και να αντικατασταθούν από νέα που έχουν υπολογιστεί από το ίδιο βιομετρικό σε περίπτωση που γίνει γνωστός αυτός ο κωδικός. (Patel et. al., 2015)
- **Βελτιωμένη ασφάλεια ελέγχου ταυτότητας:** Στη βιομετρική κρυπτογράφηση, δημιουργούνται πολύ ισχυροί κωδικοί που είναι πιο εκτεταμένοι σε μέγεθος και πιο περίπλοκοι και δεν χρειάζεται να απομνημονευθούν.
- **Δε μπορεί να υπάρξει επίθεση αντικατάστασης προτύπου:** Ένας εισβολέας δεν μπορεί να δημιουργήσει το δικό του πρότυπο αφού αυτός, ή οποιοσδήποτε άλλος, δεν γνωρίζει το ψηφιακό κλειδί και άλλα παροδικά δεδομένα που είχαν χρησιμοποιηθεί για τη δημιουργία του νόμιμου προτύπου. Δεδομένου ότι τα εξαγόμενα χαρακτηριστικά δεν αποθηκεύονται, ο εισβολέας δεν έχει τρόπο να τα τροποποιήσει.
- **Μεγαλύτερη δημόσια αποδοχή, εμπιστοσύνη και μεγαλύτερη συμμόρφωση με τους νόμους περί απορρήτου:** Η ευρεία εμπιστοσύνη είναι κυρίως απαραίτητη για την επιτυχία οποιασδήποτε ανάπτυξης βιομετρικού συστήματος. Τα βιομετρικά δεδομένα διατηρούνται σταθερά υπό τον αποκλειστικό έλεγχο του χρήστη, με τρόπο που ωφελεί τους χρήστες και ελαχιστοποιεί τον κίνδυνο επιτήρησης και κλοπής ταυτότητας. Αυτό αποτελεί ένα βασικό παράγοντα που έχει προχωρήσει τόσο πολύ στην ικανοποίηση των απαιτήσεων της ιδιωτικής ζωής και των νόμων περί προστασίας προσωπικών δεδομένων και έχει προωθήσει την ευρύτερη αποδοχή και χρήση των βιομετρικών στοιχείων**.**

5. Συμπεράσματα-Προτάσεις για μελλοντική έρευνα

5.1 Συμπεράσματα

Ο βιομετρικός έλεγχος ταυτότητας καθίσταται ως ένα πολύ γνωστό και αξιόπιστο σύστημα ελέγχου ταυτότητας, κερδίζοντας διαρκώς έδαφος και κατακτώντας την εμπιστοσύνη των χρηστών. Ως επί το πλείστον, παρουσιάζει αρκετά πλεονεκτήματά, συγκριτικά με τα παραδοσιακά συστήματα έλεγχου, όπως η ασφάλεια, η ακρίβεια, η αξιοπιστία, η άμεση εξυπηρέτηση κτλ. Το βιομετρικό σύστημα χρησιμοποιεί τα φυσιολογικά και συμπεριφοριστικά χαρακτηριστικά όπως το δακτυλικό αποτύπωμα, το πρόσωπο, η φωνή, η ίριδα και μέσω αυτών επιτυγχάνει την εξακρίβωση της ταυτότητας των χρηστών. Αυτά τα συστήματα βρίσκουν εφαρμογή σε χώρους όπως οι τράπεζες, τα αεροδρόμια, οι ηλεκτρονικές συναλλαγές, ο έλεγχος πρόσβασης σε διάφορους φυσικούς χώρους ή πόρους ενός συστήματος κτλ. Παρόλο που η εισαγωγή βιομετρικών στοιχείων σε πληροφοριακά συστήματα μπορεί να οδηγήσει σε σημαντικά οφέλη, μπορεί επίσης να ελλοχεύει πολλούς κινδύνους σχετικά με την ασφάλεια και την προστασία της ιδιωτικής ζωής. Ως εκ τούτου, διαπιστώθηκε ότι οι περισσότερες από τις επιθέσεις στοχεύουν στα βιομετρικά πρότυπα που είναι αποθηκευμένα στη βάση δεδομένων του συστήματος. Αυτό επίσης που παρατηρήθηκε είναι ότι δεν υπάρχει τεχνική ασφάλειας που να μπορεί να ικανοποιήσει όλες τις πτυχές ενός ιδανικού συστήματος προστασίας βιομετρικών προτύπων. Αυτή η εργασία έχει εντρυφήσει στις δυνατότητες και στα οφέλη των βιομετρικών συστημάτων που ενισχύουν την προστασία του απορρήτου και των προσωπικών δεδομένων των χρηστών σε οποιαδήποτε εφαρμογή. Στην εν λόγο διπλωματική επικεντρωθήκαμε στην τεχνική της βιομετρικής κρυπτογράφησης και αναλύσαμε τον τρόπο λειτουργίας, δημιουργίας κλειδιών και εξαγωγής χαρακτηριστικών από ένα βιομετρικό δείγμα. Συμπερασματικά, τα βιομετρικά συστήματα ασφαλείας έχουν αποδειχθεί ακριβή και πολύ αποτελεσματικά σε διάφορες εφαρμογές και σε συνδυασμό με την τεχνική βιομετρικής κρυπτογράφησης παρέχουν μια ολοκληρωμένη προστασία των δεδομένων των χρηστών.

5.2 Μελλοντική εξέλιξη

Με την αυξανόμενη ανάγκη για ασφαλείς μεταδόσεις δεδομένων μέσω μη ασφαλών καναλιών, η εφαρμογή του βιομετρικού κρυπτοσυστήματος σε πρακτικό επίπεδο αποτελεί ένα μείζον θέμα υψίστης σημασίας. Η χρήση ενός τέτοιου συστήματος, που είναι ένας συνδυασμός βιομετρικών χαρακτηριστικών και κρυπτογραφικών αλγορίθμων, παρέχει πολύ καλύτερη ασφάλεια και προστασία της ιδιωτικής ζωής σε σχέση με τα παραδοσιακά συστήματα. Οι μελλοντικές βελτιώσεις ενός τέτοιου βιομετρικού κρυπτοσυστήματος επικεντρώνονται στην οικονομική ανάπτυξη του συστήματος που εξασφαλίζει ασφάλεια σε οποιοδήποτε δίκτυο ή μέσο επικοινωνίας. Η βιομετρική αξιολόγηση της ποιότητας των δειγμάτων κατά τη λήψη τους είναι μια τρέχουσα ερευνητική πρόκληση που έχει αναπτυχθεί τα τελευταία χρόνια. Ωστόσο, απαιτούνται βελτιώσεις στην ακρίβεια (μέσω κρυπτογραφικών αρχιτεκτονικών που έχουν σχεδιαστεί με βιομετρικά δεδομένα) και της ταχύτητας (μέσω τροποποίησης αλγορίθμων). Οι κατευθύνσεις για περαιτέρω έρευνα μπορεί να επικεντρωθούν επίσης σε τεχνικές anti-spoofing, επιδιώκοντας να μειώσουν σε μεγάλο βαθμό την εξαπάτηση του συστήματος από την παρουσίαση ψευδών δειγμάτων, ενισχύοντας παράλληλα την ορθή λειτουργία του συστήματος. Εκτός από ιδέες σχεδιασμού και ερευνητικά ερωτήματα σχετικά με την προστασία της ορθής λειτουργίας του συστήματος, η περαιτέρω έρευνα θα πρέπει να καλύπτει τα κύρια θέματα της ιδιωτικής ζωής και των ανθρωπίνων δικαιωμάτων, αντιμετωπίζοντας τα εμπόδια των κοινωνικών υποψιών για παρακολούθηση των ευαίσθητων προσωπικών δεδομένων και άρση της ιδιωτικότητας.

Εικόνα 5.2: Προτιμήσεις καταναλωτών σχετικά με τη χρήση βιομετρικής τεχνολογίας [63] [64]

Οι επιστήμονες οραματίζονται ατέρμονες δυνατότητες και προοπτικές για το κλάδο της βιομετρικής τεχνολογίας σε μελλοντικό χρόνο. Σύμφωνα με μια πρόσφατη έκθεση προβλέψεων για την αγορά βιομετρικών συστημάτων, η βιομετρική τεχνολογία σημειώνει μια ανοδική πορεία και η προοπτική του κέρδους έχει θετικό πρόσημο, αλλά το ερώτημα στο μυαλό των περισσότερων επαγγελματιών τεχνολογίας είναι αν η τεχνολογία αυτή θα συνεχίσει να βελτιώνεται. Ως εκ τούτου, εκτιμάται ότι το 2022 περισσότερες από 5,5 δισεκατομμύρια συσκευές θα διαθέτουν βιομετρική τεχνολογία και θα δημιουργήσουν μια παγκόσμια πλατφόρμα. Σε σύντομο χρονικό διάστημα είναι προγραμματισμένο από τους κρατικούς φορείς η ένταξη της βιομετρικής ταυτότητας και του βιομετρικού διαβατήριου στη χώρα μας. Σύμφωνα με μια μελέτη του 2017 που διεξήχθη από τη Διεθνή Ένωση Αεροπορικών Μεταφορών (IATA), το 82% των ερωτηθέντων ταξιδιωτών δήλωσαν ότι θα προτιμούσαν να χρησιμοποιήσουν ένα βιομετρικό διαβατήριο για να ταξιδέψουν. Η έρευνα δείχνει επίσης, ότι οι ταξιδιώτες θέλουν ένα πιο ταχύτερο και αυτοματοποιημένο τρόπο ταυτοποίησης στο αεροδρόμιο και είναι πρόθυμοι να χρησιμοποιήσουν τη βιομετρική αναγνώριση για να επιταχύνουν το ταξίδι τους. Ως επί το πλείστον, πάνω από το 63% των αεροπορικών εταιρειών που περιλαμβάνονται στην έρευνα ισχυρίζονται ότι σχεδιάζουν να επενδύσουν στη βιομετρική τεχνολογία πριν από το τέλος του 2020. Εν κατακλείδι, η βιομετρική τεχνολογία έχει ήδη σημειώσει αρκετές επιτυχίες σε πολλούς τομείς όμως έχει ακόμα πολλά να αναδείξει καθώς οι δυνατότητες της είναι απεριόριστες.

Επίλογος

Η εν λόγο διπλωματική παρουσίασε αναλυτικά τα βιομετρικά συστήματα και το επίπεδο ασφάλειας που προσφέρουν, αναλύοντας τα τρωτά σημεία που παρουσιάζονται και τα αντιμέτρα που υφίστανται για την κατάλληλη αντιμετώπιση τους. Η τεχνολογία της βιομετρικής κρυπτογράφησης αποτελεί παράδειγμα των θεμελιωδών αρχών προστασίας της ιδιωτικής ζωής και των δεδομένων συνιστώντας έτσι μια από τις καλύτερες και πιο ισχυρές τεχνικές ασφαλείας των βιομετρικών προτύπων. Εν τέλει, εξίσου σημαντικό είναι να βρεθεί το σημείο εκείνο, στο οποίο ναι μεν θα υφίσταται η ανάγκη για την επιβεβαίωση της ταυτότητας του χρήστη, αλλά φυσικά αυτό θα γίνεται χωρίς να καταπατώνται τα βασικά ανθρώπινα δικαιώματα. Ελπίζω ότι αυτή η επιστημονική εργασία θα προσφέρει πολύτιμη συνεισφορά σε μελλοντικές έρευνες καθώς και σε ακαδημαϊκό επίπεδο να αποτελέσει σημαντικό εγχειρίδιο σε φοιτητές και καθηγητές. Εύχομαι ο κλάδος της βιομετρικής επιστήμης και τεχνολογίας να αναπτυχθεί περαιτέρω, ιδίως σε συστήματα ασφάλειας πληροφοριακών και επικοινωνιακών συστημάτων έτσι ώστε η ταυτοποίηση και αυθεντικοποίηση των χρηστών να αποτελεί πλέον μια γρήγορη και ασφαλή διαδικασία.

Βιβλιογραφία

1. Abdulmonam Omar Alaswad, Ahlal H. Montaser, and Fawzia Elhashmi Mohamad, «Vulnerabilities of Biometric Authentication Threats and Countermeasures», proc. International Journal of Information & Computation Technology, 2014
2. Abdellatef E., Ismail N. A., Elrahman S. E. S. A., Ismail K. N., Rihan M., and El-Samie F. E. A., «Cancelable fusion-based face recognition», Multimedia Tools Appl., vol. 78, no. 22, pp. 31557–31580, 2019
3. Abhishek Nagar, «Biometric Template Security», Michigan State University,pp. 1-6., 2012
4. Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, «Biometric Template Security», EURASIP Advances in Signal Processing, no. Biometrics, 2008.
5. Balwan Singh, «Different protection scheme for biometric templates», available online at www.csjournals.com, 2017
6. Bolle R. M., Connell J., Pankanti S., Ratha N. K., and Senior A. W., «Guide to biometrics», Springer Science & Business Media, 2013
7. Breebaart J., Yang B., Buhan-Dulman I., and Busch C., «Biometric template protection», Datenschutz und Datensicherheit - DuD, 33(5):299–304, 2009
8. Campisi, P., «Security and Privacy in Biometrics»,Springer-Verlag London, 2013, http://doi.org/10.1007/978-1-4471-5230-9
9. Cavoukian Ann and Alex Stoianov, «Biometric Encryption Chapter from the Encyclopedia of Biometrics», [Online]. Available: www.ijcaonline.org., 2016
10. Christian Rathgeb and Andreas Uhl, «A survey on biometric cryptosystems and cancellable biometrics», proc. EURASIP Journal on Information Security, March 2011.
11. Christina-Angeliki Toli, «Secure andPrivacy-PreservingBiometric Systems», KU Leuven – Faculty of Engineering Science, 2018
12. Eliza Yingzi Du, KaiYang, ZhiZhou. 2011, «Key Incorporation Scheme for Cancelable Biometrics. Journal of Information Security», 2(4), 185-194., (2011), DOI:http://dx.doi.org/10.4236/jis.2011
13. Georgios Goudelis, Anastasios Tefas, Ioannis Pitas, «Emerging Biometric Modalities: A Survey», Journal on Multimodal User Interfaces, 2, , 217-235., 2008, doi: http://dx.doi.org/10.1007/s12193-009-0020-x
14. Hadid A. «Face Biometrics Under Spoofing Attacks: Vulnerabilities, Countermeasures», Open Issues, and Research Directions. In IEEE Conference on Computer Vision and Pattern Recognition, CVPR Workshops 2014, Columbus, OH, USA, June 23-28, 2014, pages 113–118, 2014
15. Hammad M., Liu Y., and Wang K., «Multimodal biometric authentication systems using convolution neural network based on different level fusion of ecg and fingerprint», IEEE Access, vol. 7, pp. 26527–26542, 2018
16. ISO/IEC19794-2:2005, Information Technology—Biometric Data Interchange Formats—Part 2: Finger Minutiae Data, (2nd Edition), 2005
17. ISO/IEC2382-37, Information technology — Vocabulary — Part 37: Biometrics. 2012
18. ISO/IEC 24745:2011, Information Technology - Security Techniques -Biometric Information Protection, 2011.
19. ISO/IEC 19795-1:2006, Information Technology - Biometric Performance Testing and Reporting - Part 1: Principles and Framework, 2006.
20. ISO/IEC 19092:2008, Financial Services - Biometrics – Security Framework, 2008.

21. ISO 2017. ISO/IEC 2382-37/2017, Information Technology - Vocabulary -Part 37: Biometrics, 2017.
22. Jain K., Nandakumar K., and Nagar A., «Biometric template security», EUR-ASIP, vol. 8, no. 2, pp. 1–17, 2008
23. Jin Z., Teoh A. B. J., Goi B., and Tay Y. H., «Biometric Cryptosystems: A New Biometric Key Binding and its Implementation for Fingerprint Minutiae-based Representation Pattern Recognition», 56:50–62, 2016.
24. Joseph Mwema, Michael Kimwele, and Stephen Kimani, «A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates», proc. IJCTT, 2015
25. Kamaldeep, «A Review Of Various Attacks On Biometrics System And Their Known Solutions», International Journal of Computer Technology and Application, 2(6),2011
26. Καρατζιώλη Ευαγγελία, «Αυθεντικοποίηση με πολύτροπα βιομετρικά χαρακτηριστικά», Πτυχιακή εργασία, 2012
27. Karthik Nandakumar, «Integration of Multiple Cues in Biometric Systems», pp.1-12, Master of Science,2005
28. Kaur H.and Khanna P., «Privacy preserving remote multi-server biometric authentication using cancelable biometrics and secret sharing», Future Gener. Comput. Syst., vol. 102, pp. 30–41,2020
29. Kenta Takahashi, Shinji Hirata, «Cancelable Biometrics with Provable Security and its Application to Fingerprint Verification», IEICE Transaction on Fundamental Electronic Communication and Computer Science, 94(1), 2011
30. Kresimir Delac, Mislav Grgic, «A Survey Of Biometric Recognition Methods», In: Proceeding of 46th International Symposium Electronics in Marine, Zadar, Croatia, June, 2004
31. Latha U. and Rameshkumar K., «A Study on Attacks and Security Against Fingerprint Template Database», proc. International Journal of Emerging Trends & Technology in Computer Science, 2013
32. Lim M., Teoh A. B. J., and Kim J., «Biometric Feature-Type Transformation: Making Templates Compatible for Secret Protection», IEEE Signal Process. Mag., 32(5):77–87, 2015
33. Manisha and N. Kumar, «Cancelable biometrics: A comprehensive survey», Artif. Intell. Rev., vol. 53, pp. 3403–3446, 2020.
34. NaliniK. Ratha, JonathanH. Connel, and Ruud. Bolle, «Enhancing Security and Privacy in Biometrics-based Authentication Systems», IBM System Journal, 40(3), 614–634, 2001
35. Natgunanathan I., Mehmood A., Xiang Y., Hua G., Li, G.and Bangay S., «An Overview of Protection of Privacy in Multibiometrics», Multimedia Tools Appl., 77(6):6753–6773, 2018
36. Ngo D. C. L., Teoh A. B. J., Hu J., «Biometric Security», Cambridge Scholars Publisher, 2015
37. Padma Polash Paul, Marina Gavrilova. «Multimodal Cancelable Biometrics», In: Proceedings of ICCI*CC, Kyoto, August 22-24, 2012
38. Pagnin E. and Mitrokotsa A., «Privacy-Preserving Biometric Authentication: Challenges and Directions», Security and Communication Networks, 2017:7129505:1–7129505:9, 2017

39. Patel, V. M., Ratha, N. K., & Chellappa, R., «Cancelable Biometrics: A review. Signal Processing Magazine», IEEE, 32(5), 54–65., 2015 http://doi.org/10.1109/MSP.2015.2434151
40. Prabhakar S., Pankanti S., and. Jain A. K, «Biometric Recognition: Security and Privacy Concerns», Biometric recognition: Security and privacy concerns, vol. 1, pp. 33–42,2003
41. Raja Rao B., Dr. E.V.V.Krishna Rao, S.V.Rama Rao and M. Rama mohan rao, «Finger Print Parameter Based Cryptographic Key Generation», International Journal of Engineering Research and Applications, vol. 2, no. 6, pp. 1598-1604, 2012
42. Ratha N. K., Connell J. H., and Bolle R. M., «Enhancing security and privacy in biometrics-based authentication systems», IBM Systems Journal, 40(3):614–634, 2001
43. Roberts C., «Biometric attack vectors and defences», Computers & Security, vol. 26, no. 1, pp. 14–25, 2007
44. Rodwell P., Furnell S. and Reynolds P., «A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head»,Computers & Security, vol. 26, no. 7-8, pp. 468-478, 2007
45. Santiago Gonzalez, Carlos M. Travieso, Jesus B. Alonso, Miguel A. Ferrer, «Automatic Biometric Identification System by Hand Geometry», In: IEEE 37th Annual International Carnahan Conference on Security Technology, 2003, doi: http://dx.doi.org/10.1109/CCST.2003.1297573
46. Shinji Hirata, Kenta Takahashi. «Cancelable Biometrics with Perfect Secrecy for Correlation-based Matching», Lecture Notes in Computer Science, Springer, 5558, 2009
47. Stylios I. and Kokolakis S., «Privacy Enhancing on Mobile Devices: Continuous Authentication with Biometrics and Behavioral Modalities», 2016, [Online]. Available: http://bit.ly/2OlsD94.
48. Supriya V G, S Dr Ramachandra Manjunatha, «Chaos based Cancellable Biometric Template Protection Scheme-A Proposal», proc. International Journal of Engineering Science Invention, 2014
49. Tiwalade O. Majekodunmi, Francis E. Idachaba, «A Review of the Fingerprint, Speaker Recognition, Face Recognition and Iris Recognition Based Biometric Identification Technologies», proc. World Congress On Engineering, 2011
50. Uludag U., Pankanti S., Prabhakar S., and A. K. Jain. «Biometric cryptosystems: issues and challenges» Proceedings of the IEEE, 92(6):948–960, 2004
51. Umut Uludag, Sharath Pankanti Salil Prabhakar, «Biometric Cryptosystems: Issues and Challenges» Proceedings of the IEEE, VOL. 92, NO. 6, 2004
52. Uwe Bubeck, «Biometric Authentication - Technology and Evaluation», Term Project CS5764, 2003
53. Vincenzo Conti, C Militello,S Vitabile, «Biometric authentication overview: a fingerprint recognition sensor description», Volume 2 Issue 1, 2017
54. Wildes Richard P., «Iris Recognition: An Emerging Biometric Technology», 1997.
55. Yogendra Narain Singh, Sanjay Kumar Singh, «A taxonomy of biometric system vulnerabilities and defences», 2013, doi: 10.1504/IJBM.2013.052964
56. https://en.wikipedia.org/wiki/Sir_William_Herschel,_2nd_Baronet
57. https://en.wikipedia.org/wiki/Alphonse_Bertillon
58. https://www.globalspec.com/learnmore/industrial_engineering_software/security_software/biometrics_software

59. https://www.scientificamerican.com/article/can-we-improve-national-security-using-what-we-know-about-face-recognition/
60. https://www.army.mil/article/201384/army_researchers_improving_biometrics_speed_accuracy_for_military_intelligence_security
61. https://www.information-age.com/think-you-speak-voice-recognition-replacing-password-123461752/
62. https://www.pocket-lint.com/phones/news/samsung/138335-samsung-galaxy-note-7-iris-scanner-what-is-it-and-how-does-it-work.amphtml
63. https://www.haptic.ro/future-identity-biometrics-seen-secure-passwords/
64. https://www.cbinsights.com/research/biometrics-transforming-industries/
65. https://www.slideshare.net/DivyaPS/biometric-encryption
66. https://medcraveonline.com/IJBSBE/IJBSBE-02-00011
67. https://www.researchgate.net/publication/322680611_A_Survey_on_Biometrics_and_Cancelable_Biometrics_Systems
68. https://www.researchgate.net/figure/The-basic-concept-of-biometric-a-key-binding-and-b-key-generation_fig17_257879510
69. https://piraveenaparalogarajah.medium.com/understanding-encryption-signing-and-verification-fc256f6b763b
70. https://www.lancashirebusinessview.co.uk/latest-news-and-features/nitecrest-begins-production-of-biometric-payment-cards