Πτυχιακή Εργασία

Αυθεντικοποίηση με πολύτροπα βιομετρικά χαρακτηριστικά

Καρατζιώλη Ευαγγελία
ΑΜ: 06/3099

Επιβλέπων καθηγητής
Ηλιούδης Χρήστος

Θεσσαλονίκη, 2012

Περίληψη

Η εργασία αυτή πραγματεύεται τη χρήση των βιομετρικών συστημάτων και την αυθεντικοποίηση των χρηστών του κατά την είσοδό τους σ’ αυτό. Αρχικά, στο πρώτο κεφάλαιο παρουσιάζονται βασικά στοιχεία και όροι που θα πρέπει να γνωρίζει ο αναγνώστης για να κατανοήσει το περιεχόμενο της εργασίας. Στο δεύτερο κεφάλαιο, αναλύονται όλα εκείνα τα ανθρώπινα χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για την ταυτοποίηση ή πιστοποίηση της ταυτότητας ενός χρήστη. Στη συνέχεια, το τρίτο κεφάλαιο αναλύει το σύστημα από την τεχνική του πλευρά παρουσιάζοντας τα μοντέλα εφαρμογής βιομετρικών συστημάτων καθώς και τους τύπους αρχιτεκτονικής που μπορούν να τα υλοποιήσουν. Στο τέταρτο κεφάλαιο παρουσιάζονται τα βασικά μέρη από τα οποία αποτελείται η διεπαφή προγράμματος της εφαρμογής, κοινή για όλα τα βιομετρικά συστήματα. Στο πέμπτο κεφάλαιο απαριθμούνται οι ευπάθειες ενός βιομετρικού συστήματος καθώς και τα βιομετρικά πρότυπα που δημιουργήθηκαν για την καλύτερη ασφάλεια και μεγαλύτερη ευκολία στη χρήση. Τέλος, στο έκτο κεφάλαιο πραγματοποιείται η μελέτη της υπογραφής, των πεδίων που την αποτελούν και των δυνατοτήτων που μπορεί να προσφέρει σε ένα χρήστη. Δίνεται επίσης ένα παράδειγμα μιας πολύτροπης βιομετρικής υπογραφής. Κλείνοντας, καταγράφονται κάποια συμπεράσματα σχετικά με τη μελέτη που πραγματοποιήθηκε και τους στόχους που τέθηκαν, καθώς επίσης και μελλοντικές έρευνες και υλοποιήσεις που θα μπορούσαν να γίνουν τα επόμενα χρόνια.

Abstract

In this paper is presented the use of biometric authentication systems and user authentication. Firstly, some definitions and terms are impressed, that should be known by the reader for understanding the scope of this work. In second chapter we analyze those human characteristics that can be used to identify or authenticate a user. Thereafter, in third chapter are analyzed the types of application models and architecture in a biometric system. Fourth chapter presents the basic parts of the Biometric Application Programming Interface (Bio API). Subsequently, in fifth chapter is presented a list of vulnerabilities in a biometric system and we record the biometric templates that are created for better security. In sixth chapter we study the biometric signature fields and we also give an example of a multimodal biometric signature. Finally, we make a list of conclusions on the present study and we suggest research and implementations that can be done during the next years.

Πίνακας Περιεχομένων

Ευρετήριο εικόνων και σχημάτων

Κεφάλαιο 4ο

Κεφάλαιο 5ο

Κεφάλαιο 6ο

Κεφάλαιο 7ο

Σχήματα

Ευρετήριο πινάκων

Κεφάλαιο 1^{ο} Εισαγωγή σε βασικές έννοιες

1.1 Στόχοι της πτυχιακής εργασίας

Καθώς η τεχνολογία εξελίσσεται αξιοποιεί ολοένα και περισσότερους επιστημονικούς κλάδους πέρα από αυτή, όπως για παράδειγμα τη Φυσική, τη Γεωμετρία, τη Βιολογία κ.α. και δημιουργεί καινοτόμες επιστήμες και κλάδους. Η παρούσα εργασία κατά κάποιο τρόπο απασχολεί τη Βιολογία μελετώντας την ανατομία του ανθρώπινου σώματος και την Πληροφορική μελετώντας καινοτόμα συστήματα. Η Βιομετρία είναι μια επιστήμη που βρίσκεται στο επίκεντρο του ενδιαφέροντος λόγω της τάσης που υπάρχει στις αρμόδιες αρχές να χρησιμοποιηθεί για τη δημιουργία ηλεκτρονικών διαβατηρίων και στη συνέχεια σε άλλες εφαρμογές, που σχετίζονται με την αυθεντικοποίηση των χρηστών και την ασφάλεια συστημάτων. Αρχικά, θα παρουσιάσουμε τα

ανθρώπινα χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για τη δημιουργία ηλεκτρονικών διαβατηρίων ή άλλων βιομετρικών συστημάτων, βλέποντάς τα από τη βιολογική τους πλευρά. Θα προσπαθήσουμε να περιγράψουμε στον αναγνώστη ένα βιομετρικό σύστημα βλέποντας τη λειτουργικότητά του αλλά και την αρχιτεκτονική του. Θα μελετήσουμε τις αρχιτεκτονικές υλοποίησης που έχουν σχεδιαστεί μέχρι σήμερα και τη διεπαφή χρήστη (interface) που χρησιμοποιείται σε όλα τα αντίστοιχα συστήματα. Βασικός στόχος είναι η μελέτη της βιομετρικής υπογραφής και κατ' επέκταση μιας πολύτροπης βιομετρικής υπογραφής, με μια προγραμματιστική ματιά έτσι ώστε να κατανοήσουμε το βασικότερο κομμάτι της επιστήμης αυτής, και να μπορέσουμε να το χρησιμοποιήσουμε στο μέλλον για τη δημιουργία καινοτόμων συστημάτων και εφαρμογών. Επίσης, θα ερευνήσουμε τους κινδύνους, τις απειλές και τις ευπάθειες ενός συστήματος που αποτελούν εμπόδιο στην ομαλή του λειτουργία. Απώτερος σκοπός της εργασίας αυτής είναι ο χρήστης να γνωρίζει τη δομή μιας πολύτροπης βιομετρικής υπογραφής έτσι ώστε να μπορεί να την αξιοποιήσει και να την εξελίξει για τη δημιουργία νέων εφαρμογών αυθεντικοποίησης και τη δημιουργία νέων προτύπων ασφαλείας.

1.2 Βασικές έννοιες και προδιαγραφές

1.2.1 Βιομετρία και Βιομετρική

*Η **Βιομετρία** είναι μια εξειδικευμένη επιστήμη που το αντικείμενο της έρευνάς της είναι η ανάλυση των βιολογικών στοιχείων μέσω των δικών της στατιστικών και μαθηματικών μεθόδων. Συγκεκριμένα η Βιομετρία αναλύει με δική της μεθοδολογία, χρησιμοποιώντας ειδικά όργανα, τα βιομετρικά χαρακτηριστικά των έμβιων ζωϊκών ειδών και ειδικότερα του ανθρώπου. Έτσι υπό τη γενικότερη έννοια αποτελεί κλάδο της Βιολογίας, ενώ υπό την ειδικότερη επί της Φυσικής ανθρωπολογίας, σε επιμέρους κλάδο, που ονομάζεται **Ανθρωπομετρία.***
Ως κλάδος της Βιομετρίας η ανθρωπομετρία διαιρείται επιμέρους σε

1. *Σωματομετρία*
2. *Σωματοσκοπία*
3. *Μορφολογία*

*Παράλληλα αυτών, η ανθρωπομετρία διακρίνεται και στη **Δικαστική Ανθρωπομετρία**, που αποτελεί και κλάδο της **Εγκληματολογίας**.*
*Νεότερος σύγχρονος κλάδος της Βιομετρίας είναι η **Εργονομική Βιομετρία**, που αποτελεί και ταυτόσημο κλάδο της **Εργονομίας.*** [http://el.wikipedia.org/wiki/Βιομετρία]

*Η **Βιομετρική** είναι η πρακτική της μέτρησης των φυσικών χαρακτηριστικών ή/και της συμπεριφοράς ενός προσώπου για να ελεγχθεί η ταυτότητα του. Η αναγνώριση των φυσικών χαρακτηριστικών γίνεται με τεχνικές επεξεργασίας εικόνας και τεχνολογίες αναγνώρισης προτύπων.*[Χαιρέτη Όλγα, 2009]

1.2.2 Πολύτροπη Βιομετρία

Με σκοπό την βελτίωση των δεικτών βιομετρικής αναγνώρισης, η έρευνα έχει προχωρήσει προς την πολύτροπη βιομετρία. Εδώ η αναγνώριση βασίζεται σε ένα συνδυασμό διαφορετικών βιομετρικών στοιχείων, όπου είναι δυνατόν να χρησιμοποιηθούν πολλοί διαφορετικοί τύποι

μετρήσεων, όπως για παράδειγμα η αναγνώριση δακτυλικών αποτυπωμάτων σε συνδυασμό με την αναγνώριση προσώπου (μέθοδος που ακολουθείται στα βιομετρικά διαβατήρια). [Asker M. Bazen]

1.2.3 Βιομετρικά χαρακτηριστικά

Τα βιομετρικά χαρακτηριστικά διακρίνονται σε δυο κατηγορίες, φυσιολογικά και συμπεριφοριστικά χαρακτηριστικά.
Φυσιολογικά είναι τα χαρακτηριστικά τα οποία σχετίζονται με τη μορφή του σώματος του χρήστη. Τέτοια παραδείγματα είναι το DNA, το πρόσωπο, το δακτυλικό αποτύπωμα, η ίριδα, το αυτί, η γεωμετρία χεριού κ.α.
Συμπεριφοριστικά είναι τα χαρακτηριστικά εκείνα που σχετίζονται με τη συμπεριφορά του χρήστη. Τέτοια παραδείγματα είναι το βάδισμα, η φωνή, η ηλεκτρονική υπογραφή, ο ρυθμός δακτυλογράφησης. Κάποιοι ερευνητές ονομάζουν τη συγκεκριμένη κατηγορία ως behaviometrics.

Οποιαδήποτε ανθρώπινη φυσιολογία ή και κάποιο χαρακτηριστικό συμπεριφοράς μπορεί να χρησιμοποιηθεί ως βιομετρικό χαρακτηριστικό σε ένα σύστημα αρκεί να πληροί, σύμφωνα με τον Anil K. Jain [2004], τις παρακάτω προδιαγραφές.

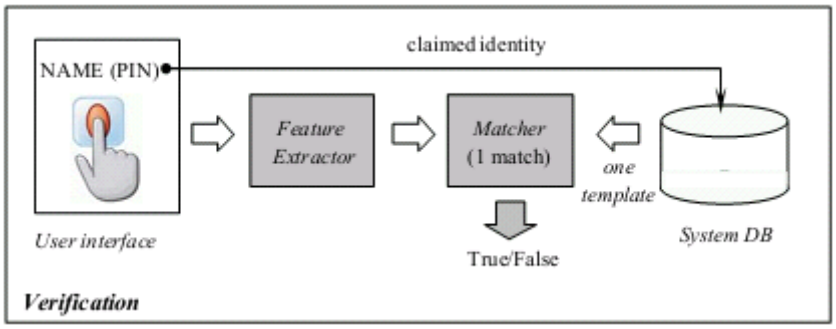
- **Καθολικότητα**: Κάθε άτομο θα πρέπει να έχει το χαρακτηριστικό αυτό.
- **Διάκριση**: Το χαρακτηριστικό αυτό θα πρέπει να διαφέρει ανάμεσα σε δύο ανθρώπους, να είναι δηλαδή διακριτό.
- **Μονιμότητα**: Θα πρέπει να παραμένει αρκετά αναλλοίωτο με την πάροδο του χρόνου.
- **Συλλεκτικότητα**: Θα πρέπει να είναι μετρήσιμο ποσοτικά.

Εκτός από τον έλεγχο καταλληλότητας ενός βιομετρικού χαρακτηριστικού θα πρέπει να πραγματοποιηθεί και ένας έλεγχος στο ίδιο το βιομετρικό σύστημα που θα τα χρησιμοποιήσει. Τα ζητήματα που πρέπει να εξεταστούν είναι τα εξής:

- **Απόδοση**: Αναφέρεται στη δυνατή επίτευξη της ακριβής αναγνώρισης και ταχύτητας του αποτελέσματος. Ποιοι είναι, δηλαδή, οι πόροι που απαιτούνται προκειμένου να επιτευχθεί η επιθυμητή ακρίβεια στην αναγνώριση και η επιθυμητή ταχύτητα, καθώς επίσης και σε όλους τους λειτουργικούς και περιβαλλοντικούς παράγοντες που επηρεάζουν τα δυο αυτά μέτρα.
- **Αποδοχή**: Δείχνει το βαθμό προθυμίας των ανθρώπων να δεχτούν την χρήση ενός συγκεκριμένου βιομετρικού χαρακτηριστικού στην καθημερινότητά τους.
- **Καταστρατήγηση**: Αναφέρεται στην ευκολία του συστήματος να ξεγελαστεί από απάτες και απατεώνες.

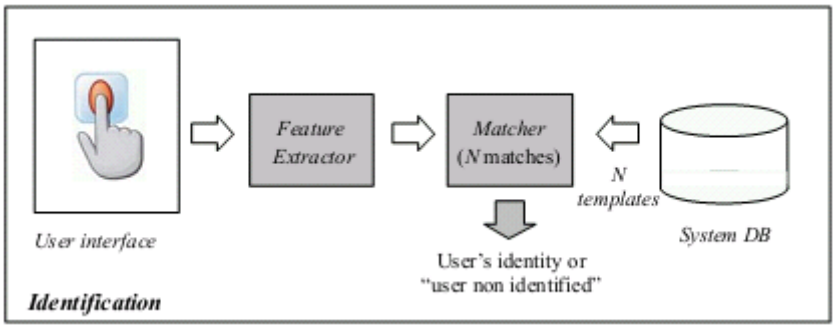
1.2.4 Επαλήθευση – Ταυτοποίηση

Υπάρχει μια σύγχυση ανάμεσα στις έννοιες επαλήθευση και ταυτοποίηση. Γι’ αυτό και σ’ αυτό το σημείο θα δωθούν οι ορισμοί των δυο εννοιών.
Επαλήθευση: Πρόκειται για μια σύγκριση ένα-προς-ένα έτσι ώστε να πραγματοποιηθεί ο έλεγχος αν το άτομο είναι αυτό που ισχυρίζεται πως είναι. Δίνει απαντήσεις σε ρωτήσεις του τύπου “Το συγκεκριμένο δακτυλικό αποτύπωμα ανήκει στον Γιώργο;”



Εικόνα 1.1: Αναπαράσταση συστήματος κατά την επαλήθευση.

Ταυτοποίηση: Είναι γνωστή και ως πιστοποίηση. Πρόκειται για μια σύγκριση ένα-προς-πολλά έτσι ώστε να προσδιοριστεί ένα άγνωστο χαρακτηριστικό και κατ' επέκταση ένα άγνωστο άτομο. Δίνει απαντήσεις σε ερωτήσεις του τύπου "Σε ποιόν ανήκει το συγκεκριμένο δακτυλικό αποτύπωμα;"



Εικόνα 1.2: Αναπαράσταση συστήματος κατά την ταυτοποίηση.

1.2.5 Βασικές μονάδες ενός βιομετρικού συστήματος

Ένα βιομετρικό σύστημα απαρτίζεται από τέσσερις (4) σημαντικές μονάδες:

1. **Αισθητήρας**: Στη μονάδα αυτή πραγματοποιείται η καταγραφή των βιομετρικών χαρακτηριστικών που θα χρησιμοποιηθούν. Για παράδειγμα η μονάδα αυτή μπορεί να είναι ένας αισθητήρας δακτυλικών αποτυπωμάτων, ένας σαρωτής ίριδας κ.α.
2. **Μονάδα εξαγωγής χαρακτηριστικών**: Στη μονάδα αυτή τα δεδομένα που έχουν καταγραφεί από τον αισθητήρα υποβάλλονται σε επεξεργασία προκειμένου να εξάγουν χαρακτηριστικά γνωρίσματα. Για παράδειγμα η θέση και ο προσδιορισμός λεπτομερειών μιας ίριδας, ή ενός δακτυλικού αποτυπώματος κ.α.
3. **Μονάδα αντιστοίχησης**: Στη μονάδα αυτή, κατά την αναγνώριση, συγκρίνονται τα χαρακτηριστικά γνωρίσματα που εξάχθηκαν από τη μονάδα εξαγωγής χαρακτηριστικών με τα πρότυπα που είναι αποθηκευμένα στο σύστημα και παράγουν μια βαθμολογία. Σ' αυτή τη μονάδα επίσης ενσωματώνεται και η μονάδα λήψης αποφάσεων, η οποία σύμφωνα με τη βαθμολογία που έχει δημιουργηθεί παίρνει τις αποφάσεις για τις διαδικασίες επαλήθευσης και ταυτοποίησης.
4. **Βάση δεδομένων**: Στη μονάδα αυτή αποθηκεύονται τα βιομετρικά πρότυπα που δημιουργούνται κατά την εγγραφή ενός χρήστη στο σύστημα.

1.2.6 Δείκτες απόδοσης

Υπάρχουν αρκετοί δείκτες απόδοσης για ένα βιομετρικό σύστημα. Θα αναφέρουμε όμως τους δυο ποιο σημαντικούς.

FRR – False Reject Rate: Είναι το ποσοστό των λανθασμένων απορρίψεων. Αντιστοιχεί στην πιθανότητα όπου το σύστημα έχει αρνηθεί την πρόσβαση σε εξουσιοδοτημένο χρήστη. Είναι γνωστό και ως FMR – False Match Rate.

FAR – False Accept Rate: Είναι το ποσοστό των λανθασμένων αποδοχών. Αντιστοιχεί στην πιθανότητα όπου το σύστημα έχει παραχωρήσει πρόσβαση σε μη εξουσιοδοτημένους χρήστες. Είναι γνωστό και ως FNMR – False Non Match Rate.

Οι δυο αυτοί δείκτες είναι συμπληρωματικοί. Τη στιγμή που αυξάνεται ο ένας, μειώνεται ο άλλος. Πράγμα το οποίο σημαίνει πως αν ένα σύστημα σχεδιαστεί με τέτοιο τρόπο ώστε να μηδενιστεί το ποσοστό των λανθασμένων αποδοχών, τότε θα είναι δύσκολη και η πρόσβαση των εξουσιοδοτημένων χρηστών εξαιτίας των υψηλών μέτρων. Αντίθετα, αν το σύστημα σχεδιαστεί έτσι ώστε να μειωθεί ή μηδενιστεί το ποσοστό των λανθασμένων απορρίψεων, τότε θα είναι πολύ εύκολη η πρόσβαση των μη εξουσιοδοτημένων χρηστών. Θα πρέπει επομένως να έχει προαποφασιστεί από τους σχεδιαστές αν επιθυμούν αυξημένη ασφάλεια του συστήματος ή φιλικότητα προς τους εξουσιοδοτημένους χρήστες.

Κεφάλαιο 2^{ο} Βιομετρικές υπογραφές

Υπάρχει ένας μεγάλος αριθμός βιομετρικών χαρακτηριστικών τα οποία χρησιμοποιούνται σήμερα σε διάφορες εφαρμογές για την αυθεντικοποίηση ενός ατόμου. Κάθε ένα από αυτά έχει κάποια δυνατά και κάποια αδύνατα σημεία και θα πρέπει να ικανοποιεί κάποιες ιδιότητες, όπως μεταξύ άλλων, να είναι παγκόσμιο, διακριτό, μόνιμο. Δεν μπορεί κάθε στοιχείο να ανταποκριθεί στις απαιτήσεις μιας εφαρμογής, δεν είναι δηλαδή αυτό που ονομάζεται βιομετρικά ιδανικό, γι' αυτό και η επιλογή του βιομετρικού στοιχείου διαφέρει από εφαρμογή σε εφαρμογή. Το στοιχείο που πρόκειται να χρησιμοποιηθεί καθορίζεται από τη λειτουργικότητα της κάθε εφαρμογής καθώς και από την ορθότητα των βιομετρικών χαρακτηριστικών.
Στο κεφάλαιο αυτό θα παρουσιάσουμε κάποια χαρακτηριστικά τα οποία θα μπορούσαν να χρησιμοποιηθούν ή χρησιμοποιούνται ως βιομετρικές υπογραφές.

2.1 DNA

Το DNA (Deoxyribonucleic acid) ή αλλιώς δεοξυριβονουκλεϊκό οξύ είναι ένα νουκλεϊκό οξύ που περιέχει τις γενετικές πληροφορίες οι οποίες καθορίζουν τη βιολογική ανάπτυξη όλων των κυτταρικών μορφών ζωής αλλά και των περισσότερων ιών. Πρόκειται για ένα μονοδιάστατο κώδικα ο οποίος είναι μοναδικός σε κάθε άνθρωπο, εκτός από την περίπτωση των πανομοιότυπων (μονοζυγωτικών) διδύμων. Επειδή σε ορισμένα σημεία του είναι ξεχωριστό σε κάθε άνθρωπο, έχουν αναπτυχθεί μέθοδοι βασιζόμενες στην ταυτοποίηση του DNA και βρίσκουν εφαρμογή στην Ιατρική, στην Εγκληματολογία και τα τελευταία χρόνια σε μελέτες της Ιστορίας και της Ανθρωπολογίας.

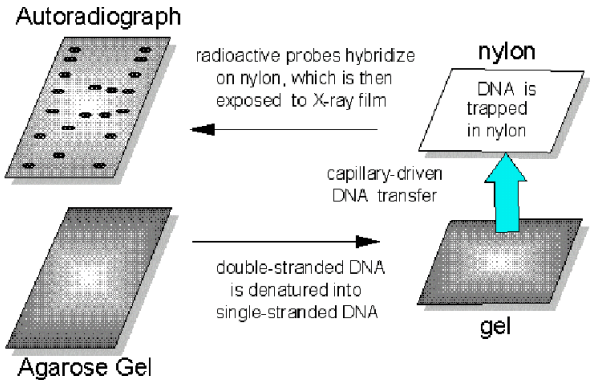
Όλοι οι ζωντανοί οργανισμοί προκύπτουν από πολύπλοκες αναπτυξιακές επιδράσεις οι οποίες γίνονται μεταξύ γονεϊκών και εξωτερικών κυττάρων. Γενετικό υλικό μπορούμε να πάρουμε από διάφορα σημεία του σώματός μας όπως το σάλιο, το αίμα, το σπέρμα, τα ούρα, τα μαλλιά, τα δόντια, τα κόκκαλα και τον ιστό. Κάθε κύτταρο ενός σημείου του σώματός μας, μας παρέχει κάποιες πληροφορίες σχετικά με το συγκεκριμένο μέρος. Όμως σε όλα τα κύτταρα το DNA είναι το ίδιο και παραμένει το ίδιο με την πάροδο του χρόνου. Για να γίνει κατανοητό το πως βοηθά η ανάλυση του DNA να ξεχωρίσουμε δυο άτομα, θα πρέπει να βρεθούν οι διαφορές στο γενετικό τους υλικό. Σε ποσοστό 99.5% - 99.9% το DNA των ανθρώπων είναι κοινό, πράγμα το οποίο σημαίνει ότι μόνο 0.1% - 0.5% διαφέρει. Το μικρό αυτό ποσοστό του ανθρώπινου γονιδίου ωστόσο, περιέχει χιλιάδες ζεύγη βάσεων που διαφέρουν από άνθρωπο σε άνθρωπο και μας βοηθούν να τους ξεχωρίσουμε. Το μόριο του DNA αποτελείται από τη γραμμική διάταξη τεσσάρων (4) βασικών μονάδων οι οποίες ονομάζονται νουκλεοτίδια ή αζωτούχες βάσεις. Οι βάσεις αυτές είναι η αδεδίνη (A), η κυτοσίνη (C), η γουανίνη (G) και η θυμίνη (T) οι οποίες ανάλογα με τη σειρά αληλουχίας τους σε τριάδες καθορίζουν τα γενετικά χαρακτηριστικά του ατόμου. Η δομή του DNA αποτελείται από δυο πολυνουκλεοτιδικές αλυσίδες σε μορφή αντιτακτών κλώνων που σχηματίζουν μια δεξιόστροφη διπλή έλικα. Οι δυο κλώνοι συγκρατούνται μεταξύ τους με δεσμούς υδρογόνου οι οποίοι προκύπτουν από καθορισμένα συμπληρωματικά ζευγάρια των αζωτούχων βάσεων. Μεταξύ της αδεδίνης και της θυμίνης σχηματίζονται δυο δεσμοί υδρογόνου ενώ μεταξύ γουανίνης και κυτοσίνης τρεις δεσμοί υδρογόνου.

Η διαδικασία ανάλυσης ξεκινά αφού έχουμε στα χέρια μας το δείγμα DNA ενός ατόμου. Καλό θα ήταν συλλέξουμε το δείγμα από το στόμα του ατόμου για την αποφυγή μολύνσεων. Σε περίπτωση που αυτό δεν εξυπηρετεί την εφαρμογή μπορούμε να το συλλέξουμε με έναν από τους τρόπους που αναφέρθηκαν παραπάνω. Από το δείγμα προκύπτει η βιομετρική αναφορά η οποία συγκρίνεται με τις αναφορές ταυτότητας που υπάρχουν στη βάση δεδομένων ενός server ή ενός client ή ακόμη και σε κάποιο token ανάλογα με την αρχιτεκτονική του συστήματος. Έχουν αναπτυχθεί μέχρι σήμερα αρκετοί μέθοδοι για τη σύγκριση των δυο αναφορών. Παρακάτω θα παρουσιαστούν κάποιοι από τους πιο γνωστούς.

2.1.1 Ανάλυση RFLP (Restriction Fragment Length Polymorphism)

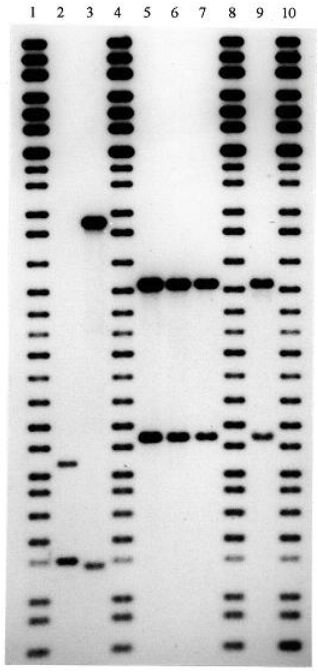
Στην ανάλυση RFLP ή ανάλυση πολυμορφισμού μήκους περιοριστικών τμημάτων, το δείγμα DNA είναι χωρισμένο σε κομμάτια. Για την τμηματοποίηση αυτή ευθύνονται κάποια ένζυμα περιορισμού τα οποία μπορούν να αναγνωρίσουν και να κόψουν το DNA σε κάθε σημείο όπου εμφανίζεται μια συγκεκριμένη αλληλουχία DNA. Τα σημεία αυτά ονομάζονται variable number tandem repeats (VNTR, ποικίλου αριθμού διαδοχικές επαναλήψεις) και είναι γνωστά γιατί

η μορφή τους ποικίλει από το ένα άτομο στο άλλο. Το μέγεθος των τμημάτων που θα δημιουργηθούν είναι διαφορετικό μεταξύ τους γιατί εξαρτάται από το πλήθος των επαναλήψεων της αλληλουχίας. Μετά τη δημιουργία των τμημάτων αυτών, το DNA διασπάται σε τμήματα σύμφωνα με μια διαδικασία γνωστή ως ηλεκτροφόρηση σε πήκτωμα, κατά την οποία εφαρμόζεται ένα ηλεκτρικό πεδίο. Έτσι όσα τμήματα είναι φορτισμένα αρνητικά έλκονται από θετικά φορτία και πραγματοποιείται η αναδιάταξή τους σχηματίζοντας λωρίδες από το μεγαλύτερο στο μικρότερο. Στη συνέχεια τα τμήματα χωρίζονται σε ενιαία σκέλη και μεταφέρονται σε μια νάιλον μεμβράνη. Κάτω από τις κατάλληλες συνθήκες ενώνονται ξανά στα σωστά σημεία δημιουργώντας έτσι διπλή έλικα(υβριδισμός) και μετά εκτίθενται σε φιλμ ακτίνων-Χ. Το τελικό μας δείγμα θα έχει περίπου τη μορφή όπως ένα barcode σουπερμάρκετ.



Εικόνα 2.1 Αναπαράσταση μεθόδου RFLP. Πραγματοποιείται η διάσπαση διπλής έλικας του DNA, μεταφέρονται τα τμήματα DNA σε νάιλον μεμβράνη, υβριδοποιούνται οι ραδιενεργοί ανιχνευτές και εκτίθενται σε ακτίνες-Χ.

Το δείγμα αυτό μπορεί να αποτελέσει είτε βιομετρική αναφορά, είτε αναφορά ταυτότητας. Στην περίπτωση που αποτελεί αναφορά ταυτότητας αποθηκεύεται σε μια βάση δεδομένων μαζί με άλλα στοιχεία που απαρτίζουν μια αναφορά ταυτότητας όπως το όνομα, ο αριθμός ταυτότητας, αριθμός άδειας οδήγησης κλπ. Στην περίπτωση που αποτελεί βιομετρική αναφορά, συγκρίνεται με το δείγμα της αναφοράς ταυτότητας για την ταυτοποίηση ή όχι των δειγμάτων.



Εικόνα 2.2 Η τελική μορφή του δείγματος μετά την ολοκλήρωση της ανάλυσης RFLP.

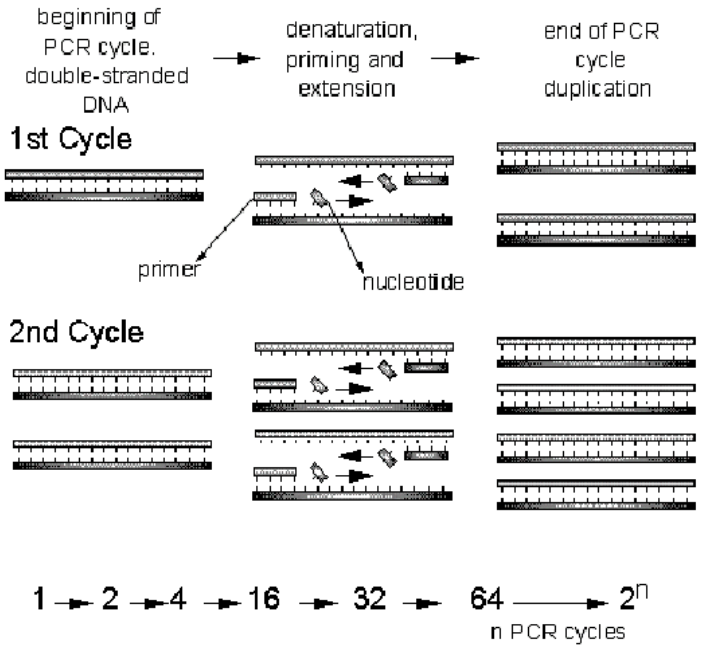
2.1.2 Ανάλυση PRC (Polymerase Chain Reaction)

Η ανάλυση PCR ή ανάλυση αλυσιδωτής αντίδρασης πολυμεράσης είναι μια επιστημονική τεχνική στη μοριακή βιολογία η οποία έχοντας ένα ενιαίο κομμάτι ή κάποια αντίγραφα του DNA, μπορεί να δημιουργήσει χιλιάδες ή και εκατομμύρια αντίγραφα του κομματιού αυτού. Το δείγμα μας επομένως μπορεί, για παράδειγμα, να είναι μια τρίχα ή μια μόνο σταγόνα αίμα. Η αναπαραγωγή της συγκεκριμένης αλληλουχίας καθορίζεται από το ένζυμο Taq πολυμεράση, το οποίο μπορεί να επιβιώσει και σε πολύ μεγάλες θερμοκρασίες. Αυτό είναι και το κλειδί στην ανάλυση PCR, διότι οι εναλλαγές στη θερμοκρασία είναι πάρα πολλές και πολύ μεγάλες. Η μέθοδος αυτή βασίζεται σε επαναλαμβανόμενους κύκλους θέρμανσης και ψύξης της αντίδρασης για την τήξη και την ενζυμική αναπαραγωγή του DNA. Σύμφωνα με την ανάλυση της μεθόδου PCR στο Wikipedia [www.wikipedia.com] υπάρχουν τρία (3) βασικά στάδια:

Στο πρώτο στάδιο πραγματοποιείται η **αποδιάταξη του DNA**. Εδώ το δείγμα θα πρέπει να βρίσκεται σε υψηλή θερμοκρασία, γι’ αυτό και θερμαίνεται στους 94-98°C για περίπου 20-30 δευτερόλεπτα. Αυτό προκαλεί την τήξη του DNA και έχει σαν αποτέλεσμα τη διάσπαση της διπλής έλικας DNA σε μονόκλινα μόρια DNA.

Στο δεύτερο στάδιο πραγματοποιείται η **αναδιάταξη του DNA**. Εδώ η κάθε αλυσίδα (ο κάθε κλώνος) χρησιμοποιείται σαν αντίγραφο για να πολλαπλασιαστεί το μέρος που μας ενδιαφέρει (DNA στόχος). Η θερμοκρασία μειώνεται στους 50-60°C για 20-40 δευτερόλεπτα και έτσι οι εκκινητές (μικρά συνθετικά τμήματα DNA) προσκολλούν στο στόχο.

Στο τρίτο στάδιο πραγματοποιείται η **επέκταση του DNA**. Εδώ η θερμοκρασία εξαρτάται από το ένζυμο που χρησιμοποιείται, για παράδειγμα το ένζυμο DNA πολυμεράση έχει βέλτιστη δραστηριότητα στους 75-80°C ενώ το ένζυμο Taq πολυμεράση στους 72°C. Σε αυτή τη θερμοκρασία λοιπόν αφού έχουν προσκολληθεί οι εκκινητές στο στόχο χρησιμοποιούνται σαν υπόστρωμα με αποτέλεσμα να πυροδοτείται μια αλυσιδωτή αντίδραση και στις δυο έλικες του DNA και έτσι δημιουργούνται οι νέοι κλώνοι.



Εικόνα 2.3 Αναπαράσταση μεθόδου PCR.
Αποδιάταξη, αναδιάταξη και επέκταση του DNA.

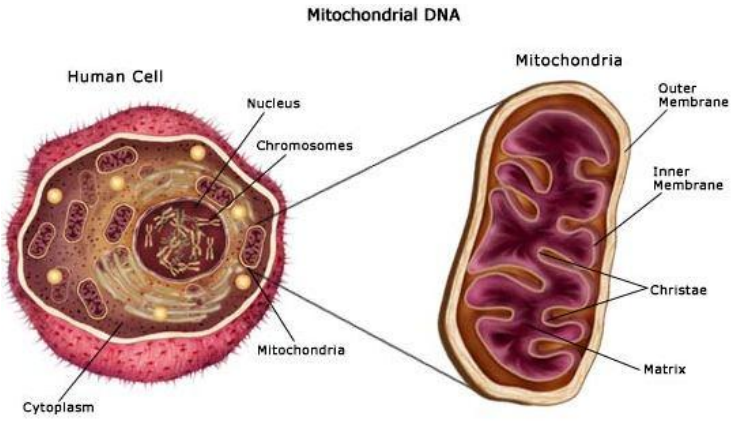
Είναι προφανές ότι με αυτό τον τρόπο το αρχικό μας δείγμα πολλαπλασιάζεται εκθετικά με τις επαναλήψεις των κύκλων. Επομένως, ακόμα και σε περίπτωση που το δείγμα είναι μικρό σε ποσότητα μπορεί να πολλαπλασιαστεί. Όπως και στην ανάλυση RFLP το δείγμα αυτό μπορεί να αποτελέσει βιομετρική αναφορά ή αναφορά ταυτότητας.

2.1.3 Ανάλυση STR (Short Tandem Repeat)

Όπως στην ανάλυση PCR έτσι και στην ανάλυση STR (short tandem repeats - μικρές επαναληπτικές αλληλουχίες νουκλεοτιδίων) χρησιμοποιούνται τα τμήματα DNA που ονομάζονται VNTR, με τη διαφορά ότι εδώ τα VNTR τμήματα είναι περίπου μια τάξη μεγέθους μικρότερα και τα ζεύγη βάσεων είναι εκατοντάδες και όχι χιλιάδες. Σε κάθε άνθρωπο ο αριθμός μονάδων επανάληψης διαφέρει, και αυτό μπορεί να χρησιμοποιηθεί για να γίνει η διάκριση ή η ταύτιση μεταξύ δυο δειγμάτων. Σε κάθε STR τμήμα η μονάδα επανάληψης απαρτίζεται από 3-4 ζεύγη βάσεων, και αυτή μπορεί να επαναλαμβάνεται από λίγες έως δωδεκάδες φορές. Τα αλληλόμορφα τμήματα μέσα σε αυτό είναι λίγα και ποικίλουν, μπορεί να είναι 5 - 20, ανάλογα με το τμήμα DNA. Τα τμήματα που θα βρεθούν ότι είναι αλληλόμορφα μπορούν να συγκριθούν άμεσα με μια κλίμακα αλληλομορφίας έχοντας τον ίδιο βαθμό πηκτικότητας και έτσι η σύγκριση και η ανάλυση να γίνει πιο εύκολα διότι αναλύονται ταυτόχρονα πολλά αλληλόμορφα τμήματα. Ένα πλεονέκτημα της μεθόδου αυτής είναι ότι μπορεί να αναλύσει δείγματα τα οποία υστερούν και σε ποσότητα αλλά και σε ποιότητα, καθώς μπορεί να εφαρμόσει την ανάλυση PCR και να πολλαπλασιάσει το δείγμα. Τέλος ένα άλλο πλεονέκτημα είναι ότι είναι δυνατόν να επιλεγούν εκείνα τα αλληλόμορφα τμήματα τα οποία είναι κατανεμημένα σε πιο σωστό βαθμό αντίστοιχα με κάποια άλλα.

2.1.4 Ανάλυση μιτοχονδριακού DNA

Μιτοχόνδρια υπάρχουν στα ευκαρυωτικά κύτταρα ενός οργανισμού και το πλήθος τους ανέρχεται σε εκατοντάδες σε κάθε κύτταρο. Πρόκειται για ημιαυτόνομα οργανίδια τα οποία παράγουν την ενέργεια του κυττάρου και συνεπώς και του οργανισμού. Διπλασιάζονται από μόνα τους και έχουν το δικό τους αυτόνομο DNA και μάλιστα σε αρκετά αντίγραφα. Το μιτοχονδριακό DNA είναι διαφορετικό από το DNA του πυρήνα κάθε κυττάρου. Κληρονομείται μόνο από τα γονίδια της μητέρας και έτσι συγγενείς όπως αδέρφια, ανίψια ή ξαδέρφια που προέρχονται από ίδια μητέρα, γιαγιά, προγιαγιά θα έχουν το ίδιο μιτοχονδριακό DNA.



Εικόνα 2.4 Αριστερά παρουσιάζεται το DNA του πυρήνα ενός κυττάρου και δεξιά το DNA ενός μιτοχονδρίου.

Το συστατικό που αναλύεται σύμφωνα με αυτή τη μέθοδο είναι το μιτοχονδριακό DNA. Η διερεύνηση της ποικιλομορφίας του μιτοχονδριακού DNA μπορεί να πραγματοποιηθεί με δύο μεθοδολογίες, τη μέθοδο RFLP (τεχνική ανάλυσης πολυμορφισμού μήκους περιοριστικών τμημάτων) και τη μέθοδο PCR (τεχνική αλυσιδωτής αντίδρασης πολυμεράσης) οι οποίες έχουν αναλυθεί παραπάνω. Εξαιτίας του μικρού μεγέθους του και των πολυάριθμων αντιγράφων σε ένα κύτταρο, το μιτοχονδριακό DNA είναι συνήθως ο τύπος DNA που θα έχει απομείνει σε ένα δείγμα το οποίο είναι μικρό, παλιό και σε κακή κατάσταση. Για το λόγο αυτό είναι ιδιαίτερα χρήσιμο στον κλάδο της Ανθρωπολογίας. Η συγκεκριμένη μέθοδος χρησιμοποιείται επίσης όταν η ανάλυση του πυρηνικού DNA δεν είναι δυνατή διότι η ποσότητα ή η ποιότητά του δεν είναι επαρκής.

Τέλος, σύμφωνα με το γεγονός ότι συγγενείς όπως αδέρφια, ξαδέρφια κλπ έχουν κοινό μιτοχονδριακό DNA μας οδηγεί στο συμπέρασμα πως υπάρχει μεγάλη πιθανότητα να γίνει λανθασμένη ταυτοποίηση δυο δειγμάτων τα οποία ανήκουν σε τέτοιους συγγενείς.

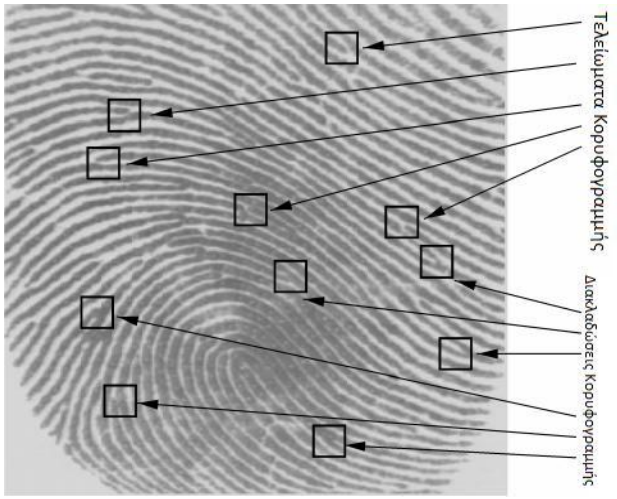
2.2 Δακτυλικά αποτυπώματα

Πρόκειται για ένα μοναδικό πρότυπο κάθε ατόμου που αποτελείται από κοιλάδες και κορυφογραμμές πάνω στην επιφάνεια κάθε δακτύλου. Τα δακτυλικά αποτυπώματα κάθε ανθρώπου είναι μοναδικά, κάτι που ισχύει και στην περίπτωση των μονοζυγωτικών (πανομοιότυπων) διδύμων. Αρχίζουν να παίρνουν μορφή κατά τον τρίτο με τέταρτο μήνα της κύησης και μέχρι τον έβδομο έχουν σχηματιστεί. Η διάταξη των κοιλάδων και των

κορυφογραμμών είναι διαφορετική σε κάθε δάκτυλο του χεριού ή του ποδιού. Σε ένα δακτυλικό αποτύπωμα εκτός από τις κοιλάδες και τις κορυφογραμμές μπορούν να εντοπιστούν έως και 150 διαφορετικά τοπικά χαρακτηριστικά (νησίδες, περιφράξεις, μικρές κορυφογραμμές) ανώμαλα κατανεμημένα πάνω στο δάκτυλο, τα οποία ονομάζονται μικρολεπτομέρειες. Δύο βασικά χαρακτηριστικά τέτοιων μικρολεπτομερειών είναι τα σημεία Galton. Ονομάστηκαν έτσι από τον Francis Galton (1821-1911) που ήταν ο πρώτος που παρατήρησε πως παραμένουν αναλλοίωτες κατά τη διάρκεια της ζωής ενός ατόμου. Τα δύο αυτά σημεία είναι το τελείωμα και οι διακλαδώσεις των κορυφογραμμών και παίζουν σημαντικό ρόλο στη διαδικασία ταυτοποίησης δυο δειγμάτων.

Τελείωμα κορυφογραμμών καλείται το σημείο εκείνο όπου μια κορυφογραμμή τελειώνει απότομα.

Διακλάδωση κορυφογραμμών καλείται το σημείο εκείνο όπου μια κορυφογραμμή χωρίζεται σε δυο νέες κορυφογραμμές.



Εικόνα 2.5 Μικρολεπτομέρειες ενός δακτυλικού αποτυπώματος.

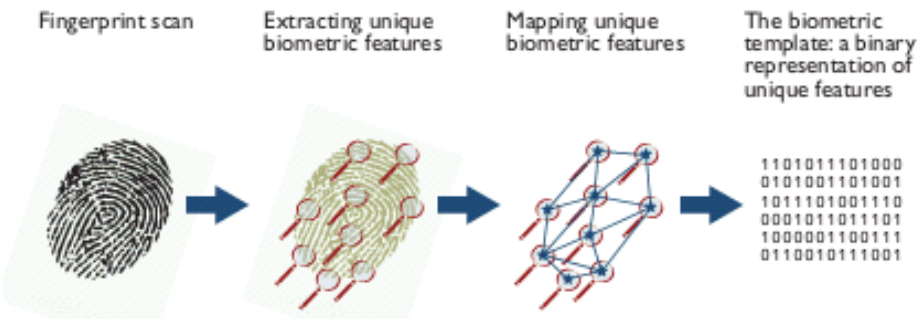
2.2.1 Διαδικασία ταυτοποίησης δακτυλικών αποτυπωμάτων

Η χρήση δακτυλικών αποτυπωμάτων ως μέθοδος ταυτοποίησης ενός ατόμου ξεκίνησε στα τέλη του 19^{ου} αιώνα. Το 1975 το Ομοσπονδιακό Γραφείο Ερευνών (FBI) χρηματοδότησε την ανάπτυξη σαρωτών δακτυλικών αποτυπωμάτων και έτσι δημιουργήθηκε ένα πρότυπο σύστημα αναγνώρισης.

Σύμφωνα με την εταιρεία Frost & Sullivan [www.frost.com] η βασική διαδικασία που ακολουθείται αποτελείται από τέσσερα (4) στάδια:

Σάρωση εγγραφών: Στο στάδιο αυτό σαρώνεται το αποτύπωμα του κάθε χρήστη και αντιστοιχίζεται με την ταυτότητά του στο σύστημα. Συνήθως υπάρχει κάποια επίβλεψη έτσι ώστε να μη δημιουργηθεί και διαδοθεί ψευδή ταυτότητα.

Δημιουργία προτύπου και αποθήκευση: Από τη σάρωση της επιφάνειας του δακτύλου του χρήστη, προκύπτουν κάποια βιομετρικά χαρακτηριστικά. Με βάση τα χαρακτηριστικά αυτά, δημιουργείται το βιομετρικό πρότυπο του δακτυλικού αποτυπώματός του.



Εικόνα 2.6 Διαδικασία δημιουργίας βιομετρικού προτύπου δακτυλικού αποτυπώματος.

Άμεση σάρωση: Το στάδιο αυτό πραγματοποιείται κάθε φορά που ένα άτομο ζητά πρόσβαση σε κάποιο σύστημα. Κάθε σαρωτής έχει τη δυνατότητα να διακρίνει ένα ζωντανό δακτυλικό αποτύπωμα από ένα τεχνητό. Έτσι κάθε φορά που κάποιος ζητά πρόσβαση στο σύστημα του ζητείται να σαρώσει το δάκτυλό του. Πραγματοποιείται η σάρωση και ο σαρωτής επικυρώνει την δημιουργία υπαρκτού δακτύλου.

Αυτοματοποιημένη αντιστοίχηση: Εδώ, το πρότυπο του δακτυλικού αποτυπώματος που δημιουργήθηκε κατά τη διάρκεια της άμεσης σάρωσης συγκρίνεται με το αντίστοιχο πρότυπο που δημιουργήθηκε κατά τη διάρκεια της σάρωσης εγγραφών και παράγεται ένα αποτέλεσμα. Εάν το αποτέλεσμα αυτό είναι μεγαλύτερο από μια κατώτατη δυνατή τιμή (κατώφλι), τότε υφίσταται ταυτοποίηση των δυο δειγμάτων.

Φυσικά η διαδικασία αυτή υλοποιείται σε κάθε εφαρμογή ανάλογα με τις απαιτήσεις της εκάστοτε εφαρμογής. Για παράδειγμα, η αναφορά ταυτότητας μπορεί να αποθηκευτεί σε μια κάρτα ή κάποιο συμβολικό πιστοποιητικό έτσι ώστε να μη μπορεί να κλαπεί ή να παραμορφωθεί. Όταν ο χρήστης της κάρτας ζητήσει πρόσβαση στο σύστημα, θα ζητηθεί η επαλήθευση του δακτυλικού του αποτυπώματος. Πραγματοποιείται λοιπόν η άμεση σάρωση του δακτύλου του, η δημιουργία της βιομετρικής αναφοράς και στη συνέχεια η σύγκριση και η επαλήθευση, ή όχι, των δυο αναφορών.
Ένα άλλο παράδειγμα είναι όταν το δακτυλικό αποτύπωμα χρησιμοποιηθεί και σαν ταυτότητα για το χρήστη αλλά και σαν κωδικός πρόσβασης. Κατά τη σάρωση εγγραφών η αναφορά ταυτότητας του χρήστη αποθηκεύεται σε μια βάση δεδομένων με αναφορές ταυτοτήτων άλλων χρηστών. Έτσι, κάθε φορά που κάποιος χρήστης ζητά πρόσβαση στο σύστημα, του ζητείται η άμεση σάρωση του δακτύλου του, η δημιουργία βιομετρικής αναφοράς και στη συνέχεια συγκρίνεται με όλες τις αναφορές ταυτοτήτων της βάσης και να γίνει, ή όχι, η ταυτοποίηση με κάποια από τις υπάρχουσες εγγραφές.

2.3 Αναγνώριση προσώπου

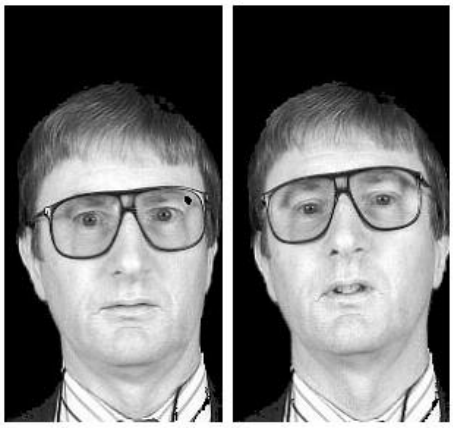
Το πρόσωπο είναι ένα μέρος στο ανθρώπινο σώμα το οποίο δεν είναι καλυμμένο από ρούχα. Πάνω σ' αυτό υπάρχουν χαρακτηριστικά που μπορούν να αποτελέσουν μια βιομετρική υπογραφή. Βέβαια δεν είναι όλα τα χαρακτηριστικά αμετάβλητα ώστε να χρησιμοποιηθούν για την αναγνώριση του ατόμου. Τα μαλλιά ή τα φρύδια για παράδειγμα δεν είναι αξιόπιστα χαρακτηριστικά αφού αλλάζουν συνεχώς σχήμα, μήκος, χρώμα ή καλύπτονται από κάποιο καπέλο ή γυαλιά. Γενικά το μακιγιάζ μπορεί να αλλάξει τελείως το πρόσωπο, καθώς επίσης και ο χρόνος.

Παρ’ όλα αυτά, υπάρχουν χαρακτηριστικά που μένουν αναλλοίωτα, όπως η ακριβής θέση των ματιών, η μύτη, το στόμα, το πηγούνι, τα οποία εξαρτώνται από το σαγόνι και το κρανίο.

Το γεγονός ότι τα συστήματα αναγνώρισης προσώπου κρίθηκαν κατάλληλα σε ποικίλες εφαρμογές και αποτελεσματικά για τη φιλικότητά τους προς το χρήστη είναι δυο λόγοι που έπαιξαν ρόλο στην εξέλιξη και εμβάθυνση των συστημάτων αυτών. Αν και υπάρχουν κι άλλα βιομετρικά χαρακτηριστικά (αποτύπωμα, ίριδα κλπ), στην περίπτωση του προσώπου το άτομο δεν χρειάζεται να έχει επαφή με το σύστημα και μπορεί ακόμη να πραγματοποιηθεί έλεγχος και από απόσταση. Σύμφωνα με την εταιρία FingerTec [2009] ο συνδυασμός των δυο μεθόδων, αναγνώριση προσώπου δυο διαστάσεων (2D) και τριών διαστάσεων (3D) μπορεί να αποφέρει καλύτερα αποτελέσματα και αποδόσεις.

2.3.1 Αναγνώριση προσώπου δυο διαστάσεων (2D)

Τα πρώτα συστήματα αναγνώρισης προσώπου πραγματοποιήθηκαν με βάση την ανάλυση PCA (Principal Components Analysis) όπου οι βιομετρικές αναφορές προέκυπταν από τη φωτογραφία του προσώπου και όχι από την απευθείας σάρωσή του. Στόχος της ανάλυσης αυτής είναι να βρεθούν τα eigenfaces. Eigenfaces ονομάζονται χαρακτηριστικά στην επιδερμίδα του προσώπου τα οποία αναφέρονται στα μάτια, στη μύτη, στο στόμα, σε καμπύλες των κόκκαλων κλπ. Αν στην αρχική εικόνα ένα χαρακτηριστικό είναι περισσότερο ορατό από κάποιο άλλο, τότε τα eigenfaces που αντιστοιχούν σ’ αυτό θα πρέπει να είναι περισσότερα από αυτό που δεν είναι τόσο ορατό. Οι παρακάτω εικόνες αποτελούν ένα παράδειγμα για τη δημιουργία eigenfaces.



Εικόνα 2.7 Εικόνες προσώπου προς αναγνώριση
(a) Εικόνα που υπάρχει στη βάση δεδομένων. (b) Εικόνα που **δεν** υπάρχει στη βάση.

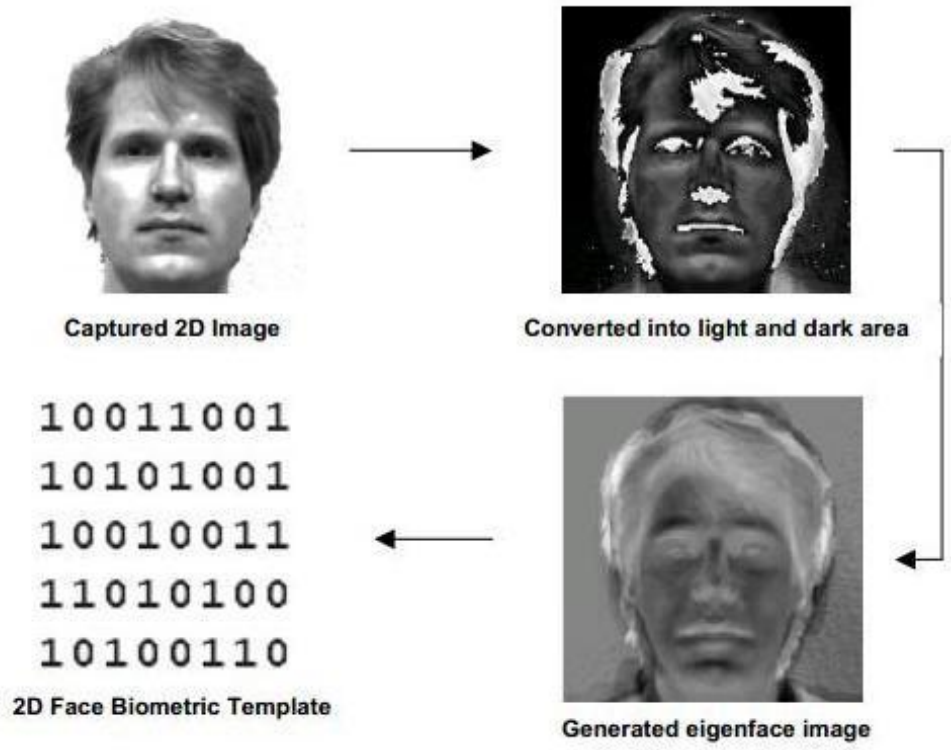
(a) 40 eigenfaces (b) 100 eigenfaces (c) 450 eigenfaces

Εικόνα 2.8 Ανακατασκευές προσώπου για τη δημιουργία eigenfaces της εικόνας 2.6 (a)

(a) 40 eigenfaces (b) 100 eigenfaces (c) 450 eigenfaces

Εικόνα 2.9 Ανακατασκευές προσώπου για τη δημιουργία eigenfaces της εικόνας 2.6 (b)

Η διαδικασία αναγνώρισης προσώπου δυο διαστάσεων ξεκινά με τη καταγραφή του προσώπου στο σύστημα με τη μορφή φωτογραφίας. Αφού αποκτηθεί η φωτογραφία μετατρέπεται σε μια φωτογραφία με σκοτεινές και φωτεινές περιοχές. Εντοπίζονται και δημιουργούνται τα eigenfaces κάθε φωτογραφίας και στη συνέχεια συγκρίνονται. Ο αλγόριθμος που χρησιμοποιείται αρχικά διαμορφώνει μια μέση εικόνα του προσώπου με βάση τα eigenfaces που έχουν δημιουργηθεί. Αθροίζει δηλαδή τα eigenfaces και τα διαιρεί με το πλήθος των φωτογραφιών. Με βάση αυτή τη μέση εικόνα υπολογίζονται οι αποστάσεις των χαρακτηριστικών που ορίζουν τα eigenfaces, τα οποία ονομάζονται διανύσματα. Δημιουργείται ένας πίνακας με τα πρότυπα των διανυσμάτων ο οποίος αποτελεί και το λεξικό της μεθόδου. Τέλος ξαναδημιουργείται η εικόνα με βάση τα διανύσματα εφαρμόζοντας στο καθένα κβαντοποίηση, αντικαθιστώντας δηλαδή το κάθε διάνυσμα με το πλησιέστερο πρότυπό του από τον πίνακα.



Εικόνα 2.10
Αναπαράσταση δημιουργίας βιομετρικού προτύπου κατά την δισδιάστατη αναγνώριση προσώπου.

Χρησιμοποιώντας συστήματα αναγνώρισης δυο διαστάσεων το μέγεθος της εικόνας είναι σχετικά μικρό και έτσι δεν δεσμεύεται μεγάλος χώρος στη μνήμη του συστήματος προκειμένου να πραγματοποιηθεί η ταυτοποίηση. Εμφανίστηκαν όμως προβλήματα όταν έπρεπε το σύστημα να αναγνωρίσει άτομα που περίστρεφαν το κεφάλι τους και δεν μπορούσαν να ανιχνεύσουν την πρόσοψή τους. Ο φωτισμός, οι εκφράσεις που τυχόν πάρει ένα πρόσωπο ή το μακιγιάζ είναι προβλήματα που επηρεάζουν το αποτέλεσμα της εικόνας δίνοντας εικόνες με περιορισμένα έως καθόλου χαρακτηριστικά. Ως εκ τούτου, ο φωτισμός και το στήσιμο του κεφαλιού αποτέλεσαν τους βασικούς λόγους για την υποβάθμιση των συστημάτων αναγνώρισης προσώπου με δυο διαστάσεις.

2.3.2 Αναγνώριση προσώπου τριών διαστάσεων

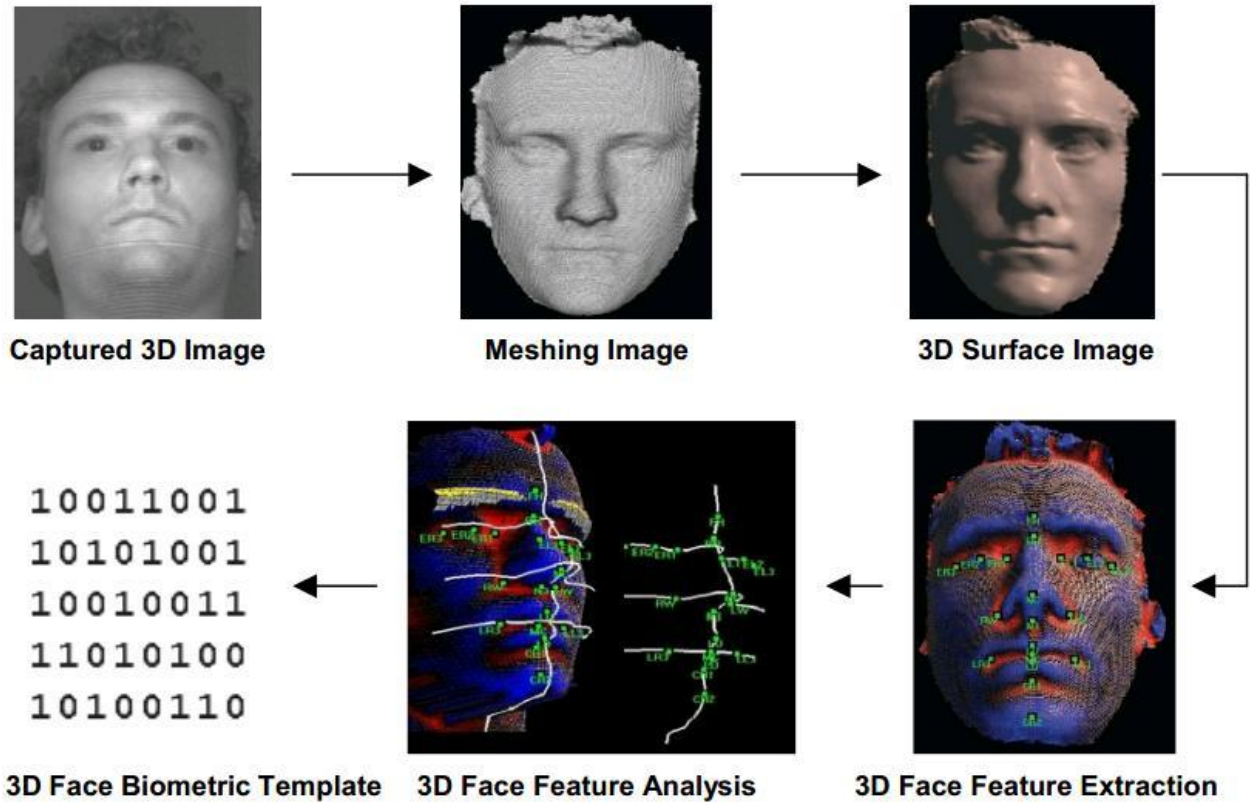
Εδώ η ταυτοποίηση του ατόμου πραγματοποιείται με τη χρήση της τρισδιάστατης γεωμετρίας του προσώπου. Πρόκειται για ένα σύστημα που αποτελείται από ένα σύνολο μεθόδων που επεξεργάζονται ένα σύνολο δεδομένων τριών διαστάσεων τα οποία αναπαριστούν το σχήμα του προσώπου και του κεφαλιού σαν ένα εύρος δεδομένων ή σαν πολυγωνικά πλέγματα. Μετρώντας, επομένως, γεωμετρικά το πρόσωπο του ατόμου επιτυγχάνεται μεγαλύτερη ακρίβεια σε σύγκριση με τη μέτρηση του προσώπου σε δυο διαστάσεις. Έτσι οι λεπτομέρειες του προσώπου είναι περισσότερες, το πρόσωπο δεν αλλοιώνεται και τα προβλήματα που εμφανίστηκαν στην 2D αναγνώριση αντιμετωπίστηκαν.

Σύμφωνα με την εταιρία FingerTec [2009] η διαδικασία αναγνώρισης προσώπου με τρεις διαστάσεις αποτελείται από τέσσερα βασικά στάδια.

1. Συσκευή

2. Επεξεργασία δεδομένων
3. Εξαγωγή χαρακτηριστικών
4. Έλεγχος ταυτοποίησης

Το πρώτο στάδιο σχετίζεται με την καταλληλότητα της συσκευής. Δεν μπορούνε όλες οι συσκευές να πραγματοποιήσουν λήψη 3D δεδομένων. Απαιτείται ένας σαρωτής με επιφάνεια τριών διαστάσεων και κάμερα VGA. Έχοντας λοιπόν τον κατάλληλο σαρωτή, πραγματοποιείται η λήψη των δεδομένων τα οποία αποστέλλονται στον επεξεργαστή του συστήματος προς επεξεργασία.
Στο δεύτερο στάδιο πραγματοποιείται η επεξεργασία των ληφθέντων δεδομένων. Αρχικά μειώνεται ο θόρυβος που τυχόν υπάρχει στα δεδομένα και ανασυντίθεται η τριπλή επιφάνεια έχοντας εξομαλυνθεί τα πρόσθετα-άχρηστα δεδομένα προκειμένου να αποφευχθούν τυχόν κενά και να βελτιωθούν τυχόν ατέλειες.
Το τρίτο στάδιο απαρτίζεται από δυο σκέλη. Εδώ εξάγονται τα χαρακτηριστικά του προσώπου που θα δημιουργήσουν τη βιομετρική αναφορά. Στο πρώτο σκέλος, έχοντας τη βελτιστοποιημένη τριπλή επιφάνεια πραγματοποιείται η σημασιολογική ανάλυση του προσώπου. Θέτονται κάποια σημεία της επιφάνειας του προσώπου ως ορόσημα για το κρανίο και το πρόσωπο του δείγματος και η επιφάνεια τοποθετείται σε ένα γενικό τοπολογικό χάρτη του προσώπου. Στο δεύτερο σκέλος εξάγεται η καμπυλότητα των ορόσημων αυτών, καμπύλες δηλαδή που κατά κάποιο τρόπο εφάπτονται στην επιφάνεια του προσώπου. Οι καμπύλες αυτές χρησιμοποιούνται για να δημιουργηθεί ένα πρότυπο προσώπου του δείγματος που αποτελεί τη βιομετρική αναφορά.
Το τελευταίο στάδιο είναι ο έλεγχος ταυτοποίησης. Εδώ, η βιομετρική αναφορά συγκρίνεται μια-προς-μια με όλες τις αναφορές ταυτότητας στη βάση του συστήματος. Κάθε σύγκριση έχει σαν αποτέλεσμα έναν αριθμό, τον αριθμό ομοιότητας των δύο προτύπων. Το πρότυπο με τον μεγαλύτερο βαθμό ομοιότητας είναι εκείνο που ταυτίζεται με το δείγμα μας.



Εικόνα 2.11 Αναπαράσταση δημιουργίας βιομετρικού προτύπου κατά την τρισδιάστατη αναγνώριση προσώπου.

Οι ανθρώπινες εκφράσεις, ο προσανατολισμός του κεφαλιού, ο διαφορετικός φωτισμός δεν επηρεάζουν πλέον την αναπαράσταση του κεφαλιού στην τρισδιάστατη μορφή του. Ακόμη κι αν το κεφάλι έχει κλίση μεγαλύτερη από γωνία 45^{o} μοιρών τα χαρακτηριστικά που είναι απαραίτητα μπορούν να εξαχθούν. Με όλα αυτά, η ακρίβεια των αποτελεσμάτων είναι μεγαλύτερη σε σύγκριση με αυτή παλιότερων μεθόδων. Το μόνο μειονέκτημα του συστήματος αυτού είναι η απόκριση του συστήματος η οποία θα είναι πιο αργή λόγω του πλήθους των προτύπων στη βάση δεδομένων που πρέπει να συγκριθούν με το δείγμα μας.

Εν κατακλείδι, και με τις δύο μεθόδους πραγματοποιείται ταυτοποίηση δυο δειγμάτων. Ο αλγόριθμος δυο διαστάσεων βασίζεται σε θεωρητικές πληροφορίες προσπαθώντας να δημιουργήσει ένα υπολογιστικό μοντέλο που περιγράφει ένα πρόσωπο με βάση χαρακτηριστικά που περιέχονται στο ίδιο το πρόσωπο. Ενώ ο αλγόριθμος αναγνώρισης τριών διαστάσεων βασίζεται στη γεωμετρία του προσώπου που αποτελείται από την ανατομία του κεφαλιού και όχι από την εξωτερική εμφάνιση που επηρεάζεται από περιβαλλοντικούς παράγοντες. Η συνδυαστική χρήση της 3D και 2D αναγνώρισης είναι μια άλλη προσέγγιση. Οι περισσότεροι σαρωτές μπορούν να αποκτήσουν την τρισδιάστατη μορφή και σύσταση του αντικειμένου που σαρώνουν. Αν για παράδειγμα μια φωτογραφία έχει τραβηχτεί με το κεφάλι να έχει μια συγκεκριμένη κλίση, τότε χρησιμοποιώντας την 3D αναγνώριση μπορεί να μετατραπεί το τρισδιάστατο μοντέλο σύμφωνα με τη συγκεκριμένη κλίση και μετά να εξαχθούν τα χαρακτηριστικά, παράγοντας έτσι καλύτερη απόδοση.

2.4 Σάρωση ίριδας

Η ίριδα είναι ένας μυς στο εσωτερικό του ματιού που ρυθμίζει το μέγεθος της κόρης ανάλογα με την ποσότητα του φωτός που εισέρχεται στο μάτι. Πρόκειται για το χρωματιστό μέρος του ματιού του οποίου το χρώμα καθορίζεται από την ποσότητα της χρωστικής ουσίας μελατονίνης μέσα στο μυ. Ένα χαρακτηριστικό που παίζει μεγάλο ρόλο στη διαφορετικότητα δυο ματιών είναι το δοκιδωτό πλέγμα, ένας ιστός που δίνει έμφαση στη διαίρεση της ίριδας με έναν ακτινωτό τρόπο που σχηματίζεται από τον όγδοο μήνα της κύησης. Η ίριδα έχει πάνω από 266 *"βαθμούς ελευθερίας"* που συμβολίζουν τον αριθμό των παραλλαγών μιας ίριδας. Αυτό είναι και το στοιχείο που επιτρέπει μια ίριδα να διακριθεί από μια άλλη.

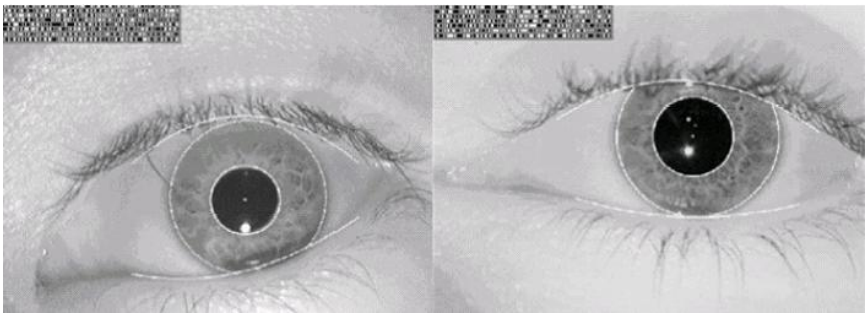
Εικόνα 2.12 Διάφορα δείγματα ίριδας.

Σύμφωνα με ένα άρθρο του SANS Institute [2002] η καταγραφή της ίριδας στο σύστημα, είτε για τη δημιουργία της ταυτότητας αναφοράς είτε της βιομετρικής αναφοράς, απαρτίζεται από 3 μέρη.

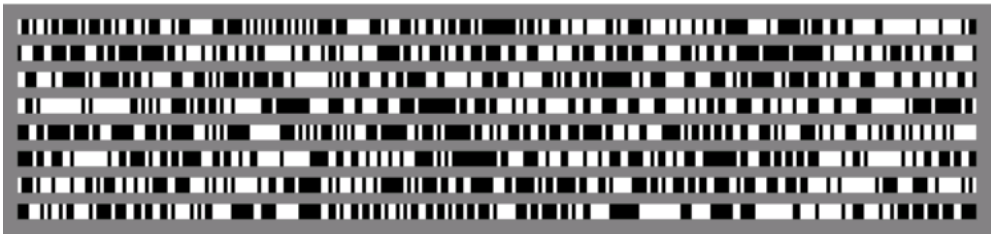
- Σύλληψη της εικόνας.
- Καθορισμός της θέσης της ίριδας και βελτιστοποίηση της εικόνας.
- Αποθήκευση (και σύγκριση για τη βιομετρική αναφορά) της εικόνας.

Η εικόνα της ίριδας συνήθως καταγράφεται με μια κάμερα η οποία θα εξασφαλίσει επαρκή ανάλυση και ευκρίνεια έτσι ώστε να γίνει πιο εύκολη η αναγνώριση. Ο χρήστης τοποθετεί το μάτι του σε μια συσκευή και βλέπει μια εικόνα, όμως μια πηγή φωτός πέφτει πάνω στο μάτι του προκειμένου να αποκτηθεί η φωτογραφία της ίριδας. Είναι σημαντικό στο εσωτερικό του μοτίβου της ίριδας να υπάρχει επαρκής αντίθεση και αυτό καθορίζεται από αυτή τη πηγή φωτός με την προϋπόθεση όμως να μη δυσαρεστεί το χρήστη. Η εικόνα που θα αποκτηθεί θα πρέπει να είναι καλά πλαισιωμένη, με την ίριδα στο κέντρο της φωτογραφίας, έτσι ώστε το αποτέλεσμα να μην είναι μισό μάτι, ή πηγούνι ή κάποιο άλλο μέρος του προσώπου. Αναπόσπαστο κομμάτι αυτής της διαδικασίας είναι και η κατάργηση των πρόσθετων εικόνων όπως οι αντανακλάσεις, οι οπτικές εκτροπές κλπ. που υπάρχουν στη φωτογραφία. Σε πιο σύγχρονα, αυτοματοποιημένα συστήματα, χρησιμοποιείται μια σειρά από κάμερες που εντοπίζουν το πρόσωπο και την ίριδα αυτόματα καθιστώντας την όλη διαδικασία πιο εύκολη.

Στον καθορισμό της θέσης της ίριδας το σύστημα αναγνώρισης προσδιορίζει την εικόνα που έχει την καλύτερη εστίαση και καθαρότητα της ίριδας. Η εικόνα στη συνέχεια αναλύεται για να προσδιοριστεί το εξωτερικό όριο της ίριδας που συναντά το λευκό σκληρό χιτώνα του ματιού, το όριο της κόρης και το κέντρο της κόρης. Αυτό έχει σαν αποτέλεσμα την ακριβή τοποθεσία του κυκλικού της ίριδας. Αφού βρεθεί η τοποθεσία της ίριδας προσδιορίζονται οι περιοχές της εικόνας που είναι κατάλληλες για την εξαγωγή των χαρακτηριστικών. Για τη βελτιστοποίησή της αφαιρούνται οι τομείς που καλύπτονται από τα βλέφαρα, τις βαθιές σκιές και τις ανακλαστικές περιοχές.



Εικόνα 2.13 Εντοπισμός ακριβής θέσης της ίριδας.



Εικόνα 2.14 Φωτογραφική αναπαράσταση του IrisCode.

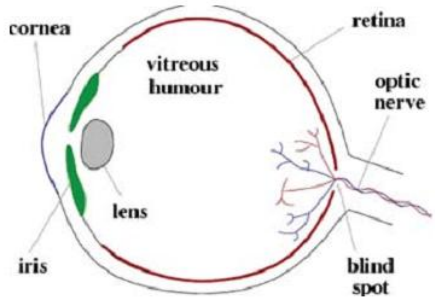
Αφού συλληφθεί η εικόνα, με τη χρήση ενός αλγορίθμου φιλτράρονται και χαρτογραφούνται τα τμήματα της ίριδας σε εκατοντάδες διανύσματα γνωστά ως phasors. Οι αλγόριθμοι αυτοί λαμβάνουν υπόψη τους τις αλλαγές που μπορεί να συμβούν στην ίριδα, όπως η συστολή και διαστολή της κόρης σε αντίδραση στο φως. Παράγεται λοιπόν ένα αρχείο 512 byte,

γνωστό ως IrisCode το οποίο αποτελεί την ταυτότητα αναφοράς ή τη βιομετρική ταυτότητα ανάλογα με το στάδιο στο οποίο βρίσκεται η ταυτοποίηση. Όταν πρόκειται για την εγγραφή του χρήστη στη βάση δεδομένων, και κατ' επέκταση για την αναφορά ταυτότητας, το αρχείο αυτό αποθηκεύεται στη βάση του συστήματος, ενώ αντίθετα όταν πρόκειται για την επαλήθευση ενός χρήστη, και κατ' επέκταση για βιομετρική αναφορά, το αρχείο αυτό χρησιμοποιείται για τη σύγκριση με όλα τα αποθηκευμένα προφίλ στη βάση. Η σύγκριση μεταξύ των αναφορών γίνεται ελέγχοντας ένα-ένα τα bit. Αρχικά το πρώτο bit της βιομετρικής αναφοράς συγκρίνεται με το πρώτο bit των αναφορών ταυτότητας, στη συνέχεια το δεύτερο bit, το τρίτο κ.ο.κ. Στα bit που δεν ταιριάζουν αποδίδεται μια αξία, ενώ σ' αυτά που ταιριάζουν αποδίδεται μηδενική αξία. Στο τέλος ο συνολικός αριθμός των διαφορετικών bit διαιρείται με το συνολικό αριθμό των bit και προκύπτει ένα ποσοστό που ορίζει τη διαφορά των δυο δειγμάτων. Η διαδικασία αυτή ονομάζεται απόσταση Hamming. Αν για παράδειγμα η απόσταση Hamming είναι ίση με 0,20 τότε οι δυο IrisCode διαφέρουν κατά 20%. Επομένως τα δείγματα ταυτίζονται κατά 80%.

Οι ιδιότητες της φυσιολογίας μιας ίριδας αποτελούν ένα σημαντικό πλεονέκτημα ως απόδειξη γνησιότητας μιας και είναι μοναδικές για τον καθένα. Δεν αλλοιώνονται με το χρόνο και εξαιτίας της ανατομίας του ανθρώπινου σώματος είναι δύσκολο να παραμορφωθούν. Ακόμη κι αν ο χρήστης με το χρόνο αποκτήσει μυωπία, πρεσβυωπία ή άλλες αντίστοιχες παθήσεις οι ιδιότητες της ίριδας δεν αλλάζουν. Στην περίπτωση της τύφλωσης και του καταρράκτη βέβαια υπάρχει δυσκολία στην αναγνώριση της ίριδας. Εκτός από τα σωματικά οφέλη, στη σημερινή εποχή η τεχνολογία σάρωσης της ίριδας χαρακτηρίζεται από την ευχρηστία της μιας και δεν υπάρχει καμία επαφή μεταξύ του ματιού και της κάμερας. Επίσης η σάρωση πραγματοποιείται ακόμα κι αν ο χρήστης φορά γυαλιά ή φακούς επαφής. Στην τεχνολογία αυτή τα ποσοστά σφάλματος είναι χαμηλά, επομένως παρέχει ένα αξιόπιστο αποτέλεσμα για τον έλεγχο ταυτότητας.

2.5 Σάρωση αμφιβληστροειδή

Ο αμφιβληστροειδής χιτώνας βρίσκεται στο πίσω μέρος της επιφάνειας του ματιού και επεξεργάζεται το φως που εισέρχεται από την κόρη του ματιού. Πρόκειται για έναν λεπτό ιστό που απαρτίζεται από νευρικά κύτταρα και τροφοδοτείται με αίμα από τριχοειδής αιμοφόρα αγγεία. Η σάρωσή του βασίζεται στο πρότυπο των αιμοφόρων αγγείων, τα οποία παρέχουν ένα αρκετά σύνθετο σχέδιο που δεν είναι παρόμοιο ούτε στην περίπτωση των διδύμων. Η βασική ιδέα για την υλοποίηση αυτής της μεθόδου έγκειται στο γεγονός ότι η υπέρυθρη ακτινοβολία απορροφάται πιο γρήγορα από τα αιμοφόρα αγγεία σε σχέση με τους περιβάλλοντες ιστούς.

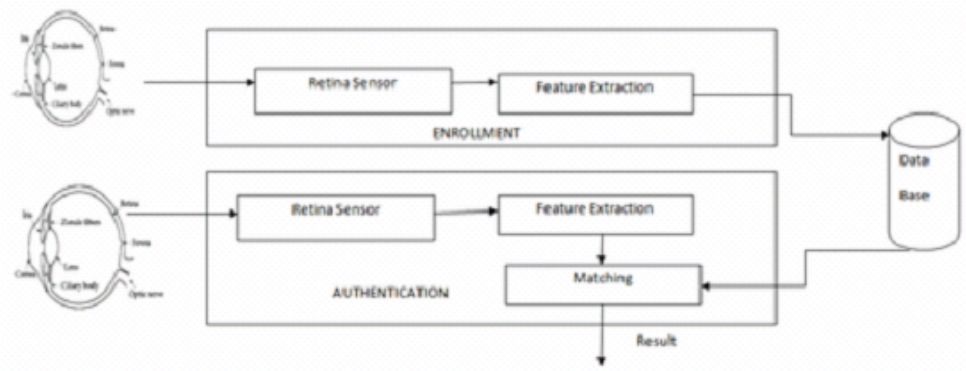


Εικόνα 2.15 Πλάγια όψη του ματιού (retina-αμφιβληστροειδής).

Εικόνα 2.16 Απεικόνιση των αιμοφόρων αγγείων.

Για τη δημιουργία της αναφοράς ταυτότητας απαιτείται συγκεκριμένο υλικό και λογισμικό μιας και η απόκτηση της εικόνας του αμφιβληστροειδή είναι δύσκολη. Ο χρήστης τοποθετεί το μάτι του σε ένα ενσωματωμένο στη συσκευή φακό και απολαμβάνει ένα θέαμα, μια εικόνα. Για να αποκτηθεί η φωτογραφία θα πρέπει να εστιάσει στο φακό ώστε το μάτι να είναι όσο το δυνατόν ακίνητο. Μια πηγή χαμηλής έντασης φωτός λοιπόν χρησιμοποιείται για να ανιχνεύσει την αγγειακή δομή από τον αμφιβληστροειδή. Συνήθως χρειάζονται 3 με 5 αποδεκτές εικόνες για να εξασφαλιστεί η εγγραφή. Αφού αποκτηθεί η εικόνα το λογισμικό που χρησιμοποιείται συγκεντρώνει τα μοναδικά χαρακτηριστικά των αιμοφόρων αγγείων. Δημιουργείται το προφίλ του ανθρώπου και αποθηκεύεται στη βάση των δεδομένων.

Κατά τη δημιουργία της βιομετρικής αναφοράς, ακολουθείται η ίδια διαδικασία με αυτή της εγγραφής, με μόνη διαφορά ότι δεν αποθηκεύεται στη βάση των δεδομένων. Αφού λοιπόν ολοκληρωθεί η διαδικασία και εξαχθούν τα χαρακτηριστικά του αμφιβληστροειδή συγκρίνονται με τα προφίλ που είναι αποθηκευμένα στη βάση. Η σύγκριση της βιομετρικής αναφοράς με τις αναφορές ταυτότητας συγκρίνονται με αναλογία ένα-προς-πολλά, έχοντας βέβαια μια εικόνα υψηλής ποιότητας. Σε αντίθετη περίπτωση είναι πολύ πιθανό να μη πραγματοποιηθεί ταυτοποίηση των δυο δειγμάτων ακόμα κι αν πρόκειται για το ίδιο μάτι, τον ίδιο άνθρωπο.



Εικόνα 2.17 Διάγραμμα διαδικασίας ταυτοποίησης με σάρωση αμφιβληστροειδή.

Αν και ο αμφιβληστροειδής μπορεί να μεταβληθεί σε περιπτώσεις διαβήτη, γλαυκώματος, εκφυλιστικών διαταραχών, συνήθως παραμένει αμετάβλητος από τη γέννηση μέχρι το θάνατο. Βρίσκεται βαθειά μέσα στα μάτια κάποιου, προστατεύεται καλά λόγω της ανατομίας του ανθρώπινου σώματος και είναι εξαιρετικά απίθανο να μεταβληθεί από περιβαλλοντικούς παράγοντες. Για τους λόγους αυτούς φαίνεται να είναι το πιο ακριβές και αξιόπιστο βιομετρικό χαρακτηριστικό. Οι εγγραφές απαιτούν παρατεταμένη συγκέντρωση και ικανότητα από το χρήστη, πράγμα που δυσαρεστεί πολλούς χρήστες. Η ευχρηστία δεν θα λέγαμε ότι είναι το δυνατό σημείο της μεθόδου αυτής. Οι χρήστες ισχυρίζονται πως είναι δύσκολο στη χρήση, αισθάνονται φόβο και δυσφορία με το γεγονός ότι πρέπει να τοποθετήσουν τα μάτια τους πολύ κοντά στη συσκευή, φοβούνται μήπως το φως ή η ίδια η συσκευή βλάψει τα μάτια τους.

2.6 Αναγνώριση αυτιού

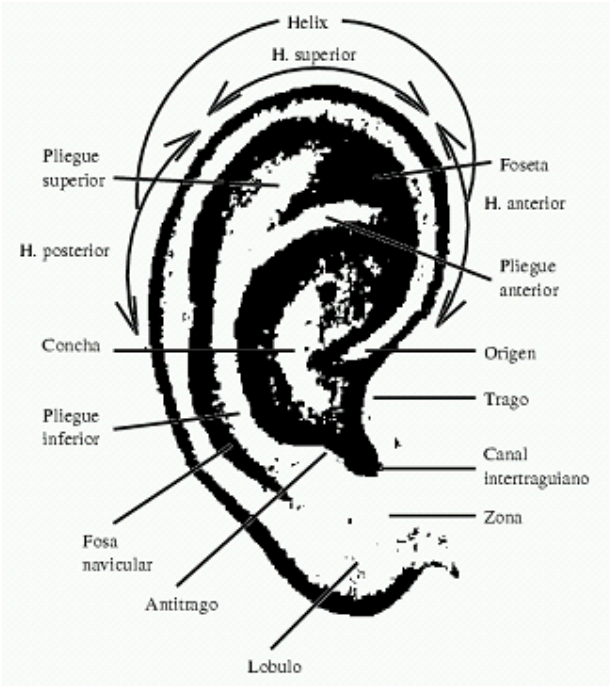
Η αναγνώριση αυτιού δεν ήταν από τις πρώτες επιλογές στην βιομετρία για την αναγνώριση ενός ανθρώπου. Η πιθανότητα να χρησιμοποιηθεί το αυτί ως βιομετρικό χαρακτηριστικό άρχισε να εμφανίζεται και να υποστηρίζεται περίπου το 1890 στη Γαλλία. Ο

Γάλλος εγκληματολόγος Alphonse Bertillon ξεκίνησε να χρησιμοποιεί τα χαρακτηριστικά του αυτιού στον κλάδο της εγκληματολογίας. Για να μπορέσουν να το χαρακτηρίσουν ως βιομετρικό γνώρισμα έπρεπε να αποδείξουν ότι πληροί όλες τις προϋποθέσεις. Ο Alfred Iannarelli εφαρμόζοντας δυο μελέτες απέδειξε τη μοναδικότητα του αυτιού. Η πρώτη μελέτη απαρτίζονταν από 10000 τυχαία δείγματα στην Καλιφόρνια, και η δεύτερη μελέτη περιείχε δείγματα από αδέρφια και πανομοιότυπα δίδυμα. Οι δύο αυτές μελέτες απέδειξαν πως το αυτί είναι ένα μοναδικό φυσιολογικό χαρακτηριστικό αφού βρέθηκε ότι η δομή του διαφέρει από άνθρωπο σε άνθρωπο, ακόμα και για τα πανομοιότυπα δίδυμα. Στην παρακάτω εικόνα είναι διακριτές οι διαφορές της δομής του αυτιού βλέποντας δύο τυχαία δείγματα από τις εικόνες των αυτιών που παρουσιάζονται.

Εικόνα 2.18 Απεικόνιση διαφόρων αυτιών για την κατανόηση της διαφορετικότητάς τους.

2.6.1 Ανατομία του αυτιού

Η ανατομία του αυτιού μπορεί να χαρακτηρίσει έναν άνθρωπο καθώς τα σημεία που το απαρτίζουν είναι πολλά και όχι ίδια σε κάθε αυτί. Το πλήθος και η θέση των σημείων αυτών διαφέρει από έρευνα σε έρευνα και από προσέγγιση σε προσέγγιση. Σύμφωνα με έρευνα του πανεπιστημίου Khulna στο Μπαγκλαντές [2007] τα βασικά στοιχεία του αυτιού είναι η έλικα, η οποία χαρακτηρίζεται από 3 σημεία που καθορίζουν την καμπυλότητά της, (το πρόσθιο, το ανώτερο και το οπίσθιο τμήμα), η ανθέλικα η οποία χαρακτηρίζεται επίσης από 3 σημεία καμπυλότητας (το πρόσθιο, το ανώτερο και το κατώτατο τμήμα), ο τριγωνικός λάκκος του αυτιού, η κόγχη, η πρόσθια εντομή, ο τράγος, ο αντιτράγος, η μεσοτράγειος εντομή, ο σκαφοειδής λάκκος, και ο λοβός του αυτιού. Παρακάτω παρουσιάζεται μια εικόνα όπου φαίνονται τα σημεία αυτά.



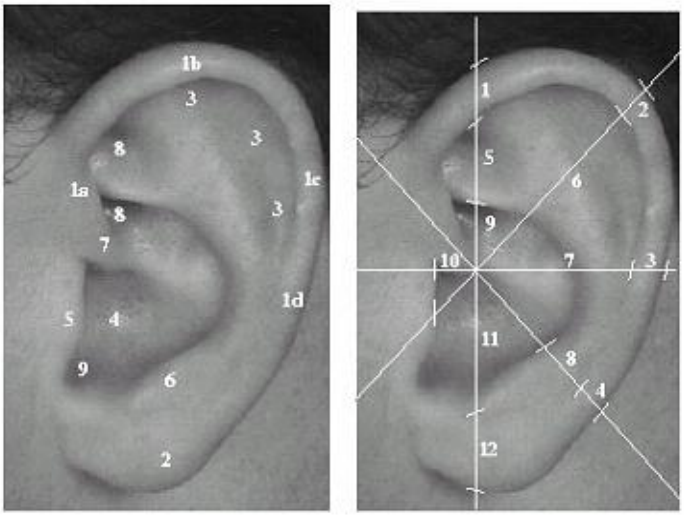
Εικόνα 2.19 Ανατομία του αυτιού.

- Helix (H.anterior, H.superior, H.posterior) / Έλικα (πρόσθιο, ανώτερο, οπίσθιο)
- Antihelix (pliegue anterior, pliegue superior, pliegue inferior / Ανθέλικα (πρόσθιο, ανώτερο, κατώτερο)
- Foseta / (τριγωνικός) Λάκκος
- Concha / Κόγχη
- Origen / Πρόσθια εντομή
- Trago / Τράγος
- Canal intertraguiano / Μεσοτράγειος εντομή
- Fosa navicular / Σκαφοειδής λάκκος
- Antitrago / Αντιτράγος
- Lobulo / Λοβός

Η δομή του αυτιού δεν επιδέχεται μεγάλες αλλαγές με το πέρασμα του χρόνου αν και η βαρύτητα παίζει σημαντικό ρόλο στην αλλαγή του. Από την ηλικία τεσσάρων μηνών έως και τα 8 χρόνια, η δομή του αυτιού αλλάζει συνεχώς, από τα 8 χρόνια έως τα 70 παραμένει σταθερή, και από τα 70 και πάνω αλλάζει και πάλι. Βρίσκεται στο πλάγιο μέρος του κεφαλιού πράγμα που σημαίνει πως σε κάθε περίπτωση κατά τη διάρκεια αναγνώρισης το φόντο του αυτιού είναι γνωστό. Στα διάφορα σημεία του το χρώμα είναι ίδιο και δεν μπορεί να επηρεαστεί από τις διάφορες καταστάσεις φωτισμού. Σε σύγκριση με άλλα βιομετρικά χαρακτηριστικά (πρόσωπο, ίριδα κλπ) στο αυτί δεν μπορούνε να προκύψουν αλλαγές από παράγοντες όπως το μακιγιάζ, το μούσι, τα γένια, παρά μόνο από μακριά μαλλιά που καλύπτουν σημεία του αυτιού.

2.6.2 Προσεγγίσεις για την αναγνώριση του αυτιού

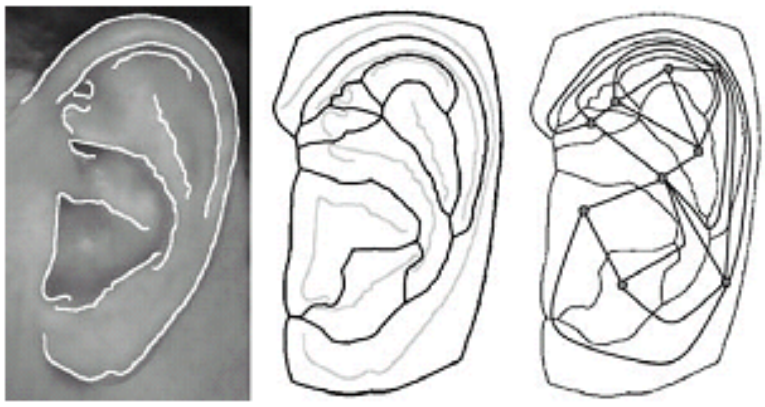
Έχουνε αναπτυχθεί διάφοροι μέθοδοι και προσεγγίσεις για την αναγνώριση του ανθρώπου χρησιμοποιώντας το αυτί. Πάνω από 100 χρόνια γίνονται προσπάθειες για την κατάλληλη προσέγγιση αναγνώρισης αυτιού. Το σύστημα που ανέπτυξε ο **Alfred Iannarelli** περίπου το 1950 βασίστηκε στη λήψη 12 μετρήσεων που λαμβάνονται από 9 σημεία του αυτιού. Εάν σε μια φωτογραφία του αυτιού τοποθετήσουμε μια νοητή πυξίδα με 8 ακτίνες θα χωρίσει τη φωτογραφία σε 8 διαστήματα με γωνίες 45^{o}. Θα πρέπει η κάθετη γραμμή αναφοράς να είναι τέτοια έτσι ώστε να αγγίζει ταυτόχρονα το ανώτερο σημείο της έλικας του αυτιού και το κατώτερο σημείο του τράγου του αυτιού. Καλύτερη διευθέτηση επιτυγχάνεται με μία δεύτερη γραμμή αναφοράς η οποία επεκτείνεται από την κόγχη του αυτιού προς τα πάνω αλλά και προς τα κάτω. Με βάση αυτές τις γραμμές εξάγονται κάποια σημεία μετρήσεων που χρησιμοποιούνται για την αναγνώριση του ατόμου.



(a) Ανατομία αυτιού (b) Μετρήσεις αυτιού

Εικόνα 2.20 (a) 1.Στεφάνι έλικας, 2.Λοβός, 3.Ανθέλικα, 4.Κόγχη, 5.Τράγος, 6.Αντιτράγος, 7.Πρόσθια εντομή, 8.Τριγωνικός λάκκος, 9.Μεσοτράγειος εντομή (b) Τα σημεία ανθρωπομετρικών μετρήσεων με βάση το σύστημα του A.Iannarelli

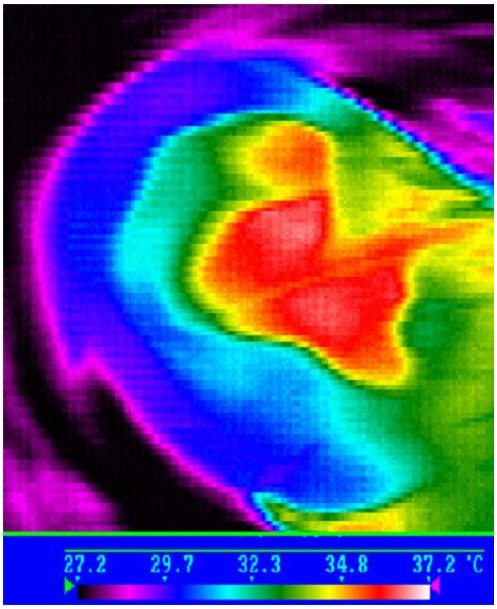
Οι **Burge και Burger** ήταν οι πρώτοι που προσπάθησαν να διερευνήσουν το αυτί σαν βιομετρικό χαρακτηριστικό. Υποστήριξαν τη μοντελοποίηση του αυτιού σαν μια γραφική παράσταση. Σύμφωνα με την πρότασή τους, το αυτί κάθε ατόμου απεικονίζεται σαν γράφημα γειτνίασης με βάση το διάγραμμα Voronoi. Με αυτό τον τρόπο κατάφεραν να εξάγουν τα καμπυλωτά τμήματα του αυτιού. Στη συνέχεια ανέπτυξαν έναν αλγόριθμο και μια νέα γραφική παράσταση ο οποίος εστιάζει στις εσφαλμένες καμπύλες που μπορούν να προκύψουν από λάθος φωτισμό, σκίαση κλπ. Παρατήρησαν πως τα σημεία του αυτιού είναι τόσο ισχυρά που καθιστούν δυνατή την ανίχνευση του αυτιού και από απόσταση. Τέλος, αναγνώρισαν το πρόβλημα των μαλλιών που παρεμποδίζουν την καθαρή εικόνα του αυτιού και πρότειναν τη χρήση θερμικής απεικόνισης για την αντιμετώπισή του.



(a) Αποτύπωμα αυτιού (b) Διάγραμμα Voronoi (c) Γραφικό μοντέλο

Εικόνα 2.21 Στάδια κατά την δημιουργία του γραφικού μοντέλου σύμφωνα με τον αλγόριθμο των Burge και Burger.

Η χρήση **θερμικής απεικόνισης** είναι μια άλλη προσέγγιση. Πρόκειται για μια φωτογραφία του αυτιού η οποία δημιουργείται από το υπέρυθρο φως του αντικειμένου. Στη θερμική απεικόνιση χρησιμοποιείται η υφή και η κατάτμηση των χρωμάτων του αυτιού όπως φαίνεται και στην εικόνα 2.21. Η θερμοκρασία των μαλλιών κυμαίνεται μεταξύ 27,2 έως 29,7 βαθμούς Κελσίου, ενώ του πτερυγίου (έλικα) του αυτιού μεταξύ 30 έως 37,2 βαθμούς Κελσίου. Υπάρχει η δυνατότητα να αποκλειστούν κάποιες θερμοκρασίες από τη θερμική εικόνα. Απορρίπτοντας έτσι του βαθμούς κάτω των 30 βαθμών Κελσίου στην ουσία εξαφανίζουμε τις τρίχες των μαλλιών. Σε μια προφίλ φωτογραφία του ατόμου όπου το αυτί είναι ορατό, ο πυρήνας του αυτιού θα είναι το θερμότερο μέρος και το θερμότερο μέρος της φωτογραφίας αναμένεται να έχει μια διαφορά θερμοκρασίας 8 βαθμών Κελσίου με τον παράγοντα μαλλιά. Όπως φαίνεται και στην παρακάτω εικόνα το εύρος τιμών που απεικονίζουν το αυτί είναι από 29,8 έως 37,2 βαθμούς Κελσίου, ενώ το εύρος τιμών από 27,2 έως 29,7 απεικονίζει το φόντο του αυτιού μέσα στο οποίο περιλαμβάνονται και τα μαλλιά.



Εικόνα 2.22 Απεικόνιση αυτιού με τη χρήση θερμογράφου

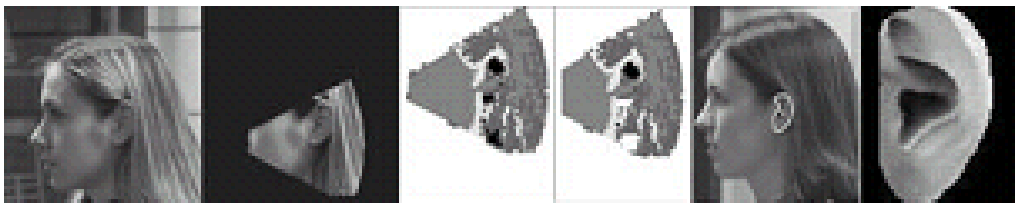
Η **Principal Components Analysis** είναι μια άλλη δημοφιλή προσέγγιση. Βασική προϋπόθεση της ανάλυσης αυτής είναι η εικόνα του αυτιού να είναι καλά κομμένη έτσι ώστε να περιέχει μόνο το αυτί και όχι άλλες άχρηστες πληροφορίες. Ο **Hurley** χρησιμοποίησε τη μέθοδο αυτή σε ένα υποσύνολο από 252 φωτογραφίες του ίδιου αυτιού. Από το δείγμα δημιουργήθηκε ένας ειδικός πίνακας που ονομάζεται projection matrix μαζί με κάποιες τιμές οι οποίες ονομάζονται βάρη (weights). Το σύνολο των βαρών αυτών αντιπροσωπεύει την κύρια εικόνα του αυτιού και είναι ιδανικό για βιομετρική σύγκριση αφού με μια απλή διανυσματική αφαίρεση μπορεί να υπολογιστεί η απόσταση των σημείων αυτών. Έτσι, έχοντας τα βάρη και τις αποστάσεις μπορεί να παραχθεί ένα εύλογο τηλεομοιότυπο του αυτιού.

Φυσικά και η τρισδιάστατη μορφή του λοβού του αυτιού δεν πέρασε απαρατήρητη. Οι **Yan και Bowyer** ανέπτυξαν τη δική τους προσέγγιση δίνοντας την προσοχή τους στο λοβό του αυτιού. Χρησιμοποίησαν λοιπόν έναν σαρωτή ακτίνας Minolta VIVID 910 προκειμένου να ανιχνεύσει το αυτί και να συλλάβει το βάθος του λοβού αλλά και το χρώμα του αντικειμένου. Ανέπτυξαν ένα δικό τους σύστημα χρησιμοποιώντας τη δισδιάστατη και τρισδιάστατη υπόσταση του αντικειμένου

για να εξάγουν τα χαρακτηριστικά του αυτιού αλλά και για να ξεχωρίσουν το αυτί από σκουλαρίκια ή τρίχες μαλλιών που τυχόν υπάρχουν στην εικόνα. Η διαδικασία εξόρυξης των χαρακτηριστικών του αυτιού περιλαμβάνει πολλαπλά στάδια που εκμεταλλεύονται τα στοιχεία των 2 και 3 διαστάσεων για να ανιχνεύσουν την καμπυλότητα του πυρήνα του αυτιού, την περιφέρεια του αυτιού και τελικά να κρατήσουν μόνο το αυτί από τη φωτογραφία. Σύμφωνα με τους D.J. Hurley, B. Arbab-Zavar and M.S.Nixon [2007] τα βήματα για την ανίχνευση του πυρήνα του αυτιού είναι τα παρακάτω

i. Πραγματοποιείται μια γεωμετρική επεξεργασία στην εικόνα για να εντοπιστεί η άκρη της μύτης, η οποία λειτουργεί ως κομβικό σημείο.
ii. Ανιχνεύεται το πρόσωπο και το αυτί έχοντας σαν σημείο αναφοράς το ανθρώπινο δέρμα έτσι ώστε να απομονωθεί από ρούχα, τρίχες μαλλιών κλπ.
iii. Στην επιφάνεια της εικόνας, που έχει προκύψει από το παραπάνω βήμα, απεικονίζονται με μαύρο χρώμα όλες οι περιοχές του αυτιού που έχουν ένα βάθος.
iv. Οι περιοχές αυτές αποτελούνε όλες τον πιθανό πυρήνα του αυτιού. Κατανέμονται και ταξινομούνται και στη συνέχεια επιλέγεται η περιοχή εκείνη που είναι πιθανότερο να αποτελεί τον πυρήνα του αυτιού.

Έχοντας βρει λοιπόν τον πυρήνα του αυτιού έχει οριοθετηθεί κατά κάποιο τρόπο η τελική εικόνα. Χρησιμοποιώντας το χρώμα από την δισδιάστατη εικόνα και το βάθος από την τρισδιάστατη εικόνα προσδιορίζεται το περίγραμμα του αυτιού και έτσι από ολόκληρη τη φωτογραφία έχουμε απομονώσει το αυτί.



Εικόνα 2.23 Εξόρυξη αυτιού. (από αριστερά στα δεξιά) ανίχνευση δέρματος, εύρεση και επιλογή του πυρήνα του αυτιού, θέση περιγράμματος αυτιού, 3D εξόρυξη αυτιού.

2.7 Αναγνώριση βαδίσματος

Οι άνθρωποι ισχυρίστηκαν πως μπορούν να αναγνωρίσουν κάποιο κοντινό τους πρόσωπου από το βάδισμά του. Αυτό ήταν το έναυσμα για την ανάπτυξη και εξέλιξη της αναγνώρισης βαδίσματος. Σύμφωνα με τους Jeffrey E. Boyd και James J. Little [2005] *βάδισμα ορίζεται ο συντονισμένος και κυκλικός συνδυασμός των κινήσεων που έχουν ως αποτέλεσμα την ανθρώπινη κίνηση. Οι κινήσεις που πραγματοποιούνται συντονίζονται με βάση ένα συγκεκριμένο πρότυπο προκειμένου να συμβεί το βάδισμα. Οι κινήσεις του βαδίσματος επαναλαμβάνονται καθώς ο άνθρωπος κάνει κύκλους μεταξύ των βημάτων εναλλάσσοντας τα πόδια του. Τόσο ο συντονισμός όσο και η κυκλική φύση της κίνησης κάνει το βάδισμα ένα μοναδικό φαινόμενο.* Οι Bertenthal και Pinto [1993] προσδιόρισαν τρεις σημαντικούς παράγοντες για την καλύτερη αντίληψη του βαδίσματος.

i. **Συχνότητα διοχέτευσης**. Όλες οι συνιστώσες που απαρτίζουν το βηματισμό θα πρέπει να έχουν την ίδια συχνότητα.
ii. **Κλείδωμα φάσης**. Οι σχέσεις μεταξύ των συνιστωσών του βηματισμού παραμένουν σταθερές. Η κλειδωμένη φάση διαφέρει για τους διαφορετικούς τύπους μετακίνησης όπως είναι το περπάτημα σε σχέση με το τρέξιμο.
iii. **Σωματική αξιοπιστία.** Η κίνηση θα πρέπει σωματικά να είναι μια εύλογη ανθρώπινη κίνηση.

Προκειμένου να εκτιμηθεί το βάδισμα με κάποιο κοινό πλαίσιο, προτείνεται η ακόλουθη προσέγγιση για να κατανοηθούν τα συστήματα ανάλυσης βάδισης.

1. Τα σήματα ταλάντωσης που προέρχονται από το σύστημα αναγνωρίζονται ότι έχουν όντως κυκλική κίνηση.
2. Καθορίζεται το πώς τα σήματα ταλάντωσης καθορίζουν τη συχνότητα διοχέτευσης, το κλείδωμα φάσης και τη σωματική αξιοπιστία
3. Καθορίζεται το πώς τα σήματα ταλάντωσης μεταφράζονται σε χαρακτηριστικά που μπορούν να χρησιμοποιηθούν για την αναγνώριση.

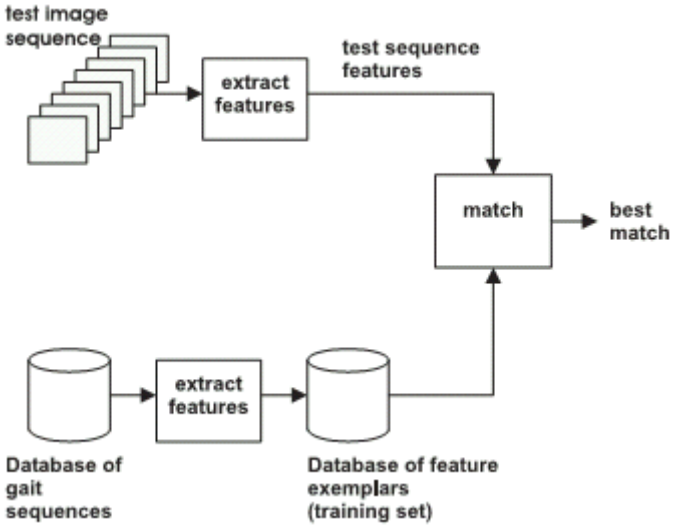
Στοιχεία όπως το έδαφος στο οποίο περπατά ο άνθρωπος, κάποιος τραυματισμός που τυχόν έχει στο σώμα του, τα παπούτσια που φοράει, η μυϊκή του ενδυνάμωση, η κούραση που τυχόν έχει εκείνη τη στιγμή, η κουλτούρα και η προσωπική του ιδιοσυγκρασία καθορίζουν το χαρακτηριστικό του βάδισμα. Όλα αυτά είναι παράγοντες που παίζουν ρόλο στην αναγνώριση του βηματισμού.

2.7.1 Στοιχεία αναγνώρισης βηματισμού

Με βάση το άρθρο των Jeffrey E. Boyd και James J. Little [2005] τέσσερα (4) είναι τα βασικά στοιχεία κατά την αναγνώριση του βηματισμού.

1. Αφαίρεση παρασκηνίου. Η αφαίρεση του παρασκηνίου έχει σαν στόχο να απομονώσει όλα τα αντικείμενα της εικόνας τα οποία είναι στατικά. Αν και υπάρχουν πολλές παραλλαγές για αυτή τη διαδικασία, η βασική ιδέα είναι η εξής. Αρχικά εκτιμώνται οι ιδιότητες των εικονοστοιχείων (pixels) στο στατικό παρασκήνιο και αφαιρούνται οι πραγματικές τιμές τους από το εκτιμώμενο παρασκήνιο. Δίνεται ένα συγκεκριμένο κατώφλι τιμών (η μικρότερη δυνατή τιμή) και αν η διαφορά είναι μεγαλύτερη τότε το εικονοστοιχείο αποτελεί μέρος ενός κινούμενου αντικειμένου.
2. Φιγούρα. Η αφαίρεση του παρασκηνίου παρέχει ένα σύνολο εικονοστοιχείων που απαρτίζουν την περιφέρεια ενός κινουμένου αντικειμένου. Σε κάποιες περιπτώσεις μπορεί να ενδιαφέρει μόνο αυτό το περίγραμμα το οποίο καλείται φιγούρα, ή αλλιώς σιλουέτα.
3. Οπτική ροή. Πρόκειται για ένα πεδίο κίνησης, μια προβολή της κίνησης στο επίπεδο μιας εικόνας. Η οπτική ροή αναφέρεται στη μετακίνηση ή τη ροή των φωτεινών εικονοστοιχείων σε ένα σύνολο από εικόνες, μια ακολουθία εικόνων. Αν και το πεδίο κίνησης με την οπτική ροή δεν είναι το ίδιο, συχνά η οπτική ροή χρησιμοποιείται ως προσέγγιση για το πεδίο κίνησης μιας και η ροή των εικονοστοιχείων προκύπτει από την παρατηρούμενη κίνηση.
4. Εικόνα ενεργειακής κίνησης και εικόνα ιστορικής κίνησης.(Motion energy image –MEI και Motion History Image –MHI). Και οι δύο εικόνες προέρχονται από ακολουθίες εικόνων. Στην MEI ένα εικονοστοιχείο επισημαίνει κατά πόσο υπήρξε οποιοδήποτε κίνηση σ' αυτό σε προηγούμενο καρέ χωρίς όμως να μπορεί να ορίσει κάποιο χρονοδιάγραμμα για τη σειρά με ποια κινήθηκαν τα εικονοστοιχεία. Η MHI υποδεικνύει πόσο πρόσφατη είναι η

κίνηση σε κάθε εικονοστοιχείο. Όσο πιο φωτεινό είναι ένα εικονοστοιχείο τόσο πιο πρόσφατη είναι η κίνησή του.



Εικόνα 2.24 Διάγραμμα διαδικασίας αναγνώρισης βηματισμού.

2.7.2 Τεχνικές αναγνώρισης βηματισμού

Ο Gafurov [2007] κατηγοριοποιεί την αναγνώριση του βηματισμού σε τρεις βασικές τεχνικές. Την τεχνική βασισμένη στη μηχανική όραση, τη τεχνική βασισμένη σε αισθητήρα δαπέδων και την τεχνική βασισμένη σε αισθητήρες που φορά ο άνθρωπος. Και οι τρεις αναλύονται παρακάτω.

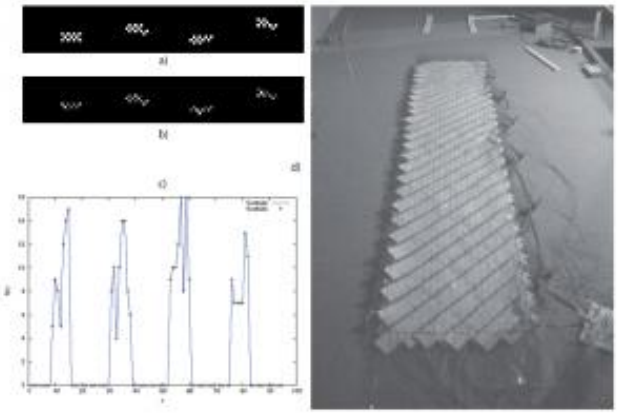
2.7.2.1 Μηχανική όραση

Σ αυτή την κατηγορία ο βηματισμός καταγράφεται από κάποια βιντεοκάμερα από απόσταση. Το βίντεο ή η εικόνα που θα καταγραφεί χρησιμοποιούνται για την εξαγωγή κάποιων χαρακτηριστικών όπως είναι ο βηματισμός και ο ρυθμός του ή οι σωματικές παράμετροι όπως το ύψος, η απόσταση μεταξύ κεφαλιού-λεκάνης, η μέγιστη απόσταση μεταξύ λεκάνης-ποδιών ή η ανθρώπινη σιλουέτα. Ανάλογα την εφαρμογή επιλέγονται και τα αντίστοιχα χαρακτηριστικά. Το βασικό πλεονέκτημα της μηχανικής όρασης είναι ότι μπορεί να καταγραφεί διακριτικά από απόσταση και εν αγνοία του χρήστη.

Εικόνα 2.25 Παράδειγμα εξαγωγής της ανθρώπινης σιλουέτας.

2.7.2.2 Αισθητήρας δαπέδου

Σύμφωνα με αυτή την τεχνική ο βηματισμός καταγράφεται από αισθητήρες οι οποίοι τοποθετούνται σε κάποιο χαλί στο πάτωμα. Έτσι όταν κάποιος περπατά κατά μήκος του χαλιού αυτού, μετριέται η δύναμη που ασκεί στο έδαφος η οποία είναι γνωστή και ως Ground Reaction Force. Τρία άλλα χαρακτηριστικά που μπορούν να εξαχθούν είναι το μήκος του διασκελισμού, ο ρυθμός του διασκελισμού και το χρονικό διάστημα που ολοκληρώνεται ένα βήμα, το χρονικό διάστημα δηλαδή από τη στιγμή που πατά τα δάκτυλα του ενός ποδιού μέχρι τη στιγμή που πατά τη φτέρνα του ίδιου ποδιού. Το βασικό πλεονέκτημα της τεχνικής αυτής είναι η διακριτικές συλλογές δεδομένων. Επίσης εκτός από την παροχή πληροφοριών ταυτότητας μπορεί να αναφέρει πληροφορίες για την τοποθεσία του ατόμου μέσα σε ένα κτίριο.



Εικόνα 2.26 Καταγραφή δύναμης που ασκείται στο έδαφος και απεικόνιση αισθητήρα δαπέδου.

2.7.2.3 Αισθητήρες σε ενδυμασία

Η τεχνική αυτή βασίζεται στην καταγραφή του βηματισμού φορώντας αισθητήρες κίνησης στο σώμα του ατόμου σε διάφορα σημεία όπως στη μέση, στα παπούτσια, στον αστράγαλο, στον καρπό του χεριού, στην τσέπη του παντελονιού κ.ο.κ. Η επιτάχυνση του βηματισμού η οποία καταγράφεται από τον αισθητήρα, χρησιμοποιείται για τον έλεγχο ταυτότητας. Εκτός από τους αισθητήρες που μετράνε το μέτρο της επιτάχυνσης (επιταχυνσιονόμετρα), υπάρχουν αισθητήρες που μετρούν την περιστροφή και τον αριθμό των μοιρών ανά δευτερόλεπτο (αισθητήρες γυροσκοπίου), τη δύναμη κατά τη βάδιση (αισθητήρες δύναμης) κ.α. Ένα από τα κύρια

πλεονεκτήματα της τεχνικής αυτής σε σχέση με άλλα βιομετρικά χαρακτηριστικά είναι η μη ενοχλητική συλλογή των δεδομένων που απαιτούνται.

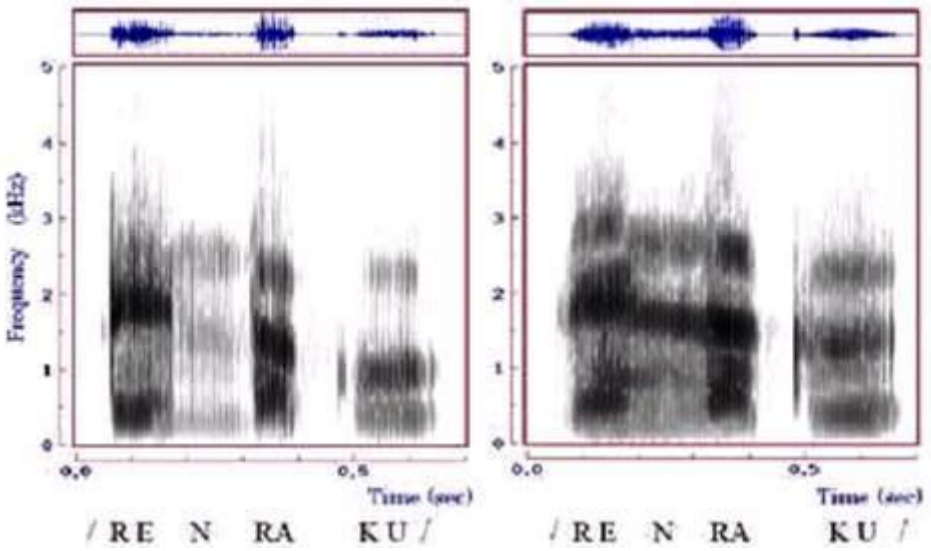
Εικόνες 2.27 και 2.28 Συνδεδεμένος αισθητήρας στη ζώνη του παντελονιού και στην κνήμη αντίστοιχα.

2.8 Αναγνώριση φωνής

Για τον έλεγχο ταυτοποίησης της φωνής κύρια προϋπόθεση είναι η μοναδικότητα της φωνής σε κάθε άνθρωπο στον τόνο και την έντασή της. Στη μοναδικότητα αυτή βέβαια συμβάλλουν κι άλλοι παράγοντες όπως το μέγεθος και το σχήμα του στόματος, του λάρυγγα, της μύτης και τα δόντια τα οποία καλούνται αρθρωτές, το μέγεθος, το σχήμα και η ένταση των φωνητικών χορδών. Η πιθανότητα όλα αυτά να είναι ίδια σε δυο άτομα είναι πολύ μικρή. Η γλώσσα, το σαγόνι, ο τρόπος που οι μύες χρησιμοποιούν τα χείλη καθορίζουν τον τρόπο με τον οποίο μιλά ο άνθρωπος. Η ομιλία παράγεται από τον αέρα που περνά από τους πνεύμονες, το λάρυγγα και τους αρθρωτές. Η διαφορετική θέση των αρθρωτών παράγουν και διαφορετικούς ήχους. Σαν αποτέλεσμα δημιουργείται ένα φωνητικό πρότυπο το οποίο αναλύεται με ένα φασματογράφημα. Το φασματογράφημα εμφανίζει το χρόνο, τη συχνότητα των δονήσεων των φωνητικών χορδών και το εύρος της έντασης.

Το πρώτο στάδιο της αναγνώρισης φωνής είναι να παραχθεί ένα πραγματικό δείγμα φωνής το οποίο θα χρησιμοποιηθεί ως αναφορά ταυτότητας. Το άτομο εγγράφεται στη βάση δεδομένων αναπαράγοντας μια λεκτική φράση ή μια σειρά αριθμών. Τη στιγμή που θα ζητήσει την πρόσβαση σε κάποιο σύστημα θα πρέπει να πραγματοποιηθεί η επαλήθευση της φωνής του. Υπάρχουν δυο περιπτώσεις αναγνώρισης της φωνής. Η εξαρτώμενη του κειμένου, και η ανεξάρτητη του κειμένου. Στην πρώτη περίπτωση του ζητείται να επαναλάβει αρκετές φορές τη φράση ή την ακολουθία αριθμών η οποία είναι ίδια με αυτή κατά την εγγραφή. Στη δεύτερη περίπτωση του ζητείται να αρθρώσει μια φράση ή μια ακολουθία αριθμών κατά βούληση. Το δείγμα αυτό, είτε της πρώτης είτε της δεύτερης περίπτωσης αποτελεί τη βιομετρική αναφορά. Η αναφορά ταυτότητας έχει ήδη ψηφιακή μορφή, μετατρέπεται και η βιομετρική αναφορά σε ψηφιακή μορφή και στη συνέχεια μπορούν να επεξεργαστούν. Τέλος πραγματοποιείται η πιστοποίηση ή όχι του ατόμου. Η βιομετρική αναφορά συγκρίνεται με κάθε αναφορά ταυτότητας που υπάρχει στη βάση και από κάθε σύγκριση προκύπτει μια βαθμολογία. Η βαθμολογία αυτή ορίζει την πιθανότητα ότι το άτομο είναι αυτός που ισχυρίζεται ότι είναι ή όχι. Με βάση ένα κατώφλι που έχει οριστεί από

το σύστημα προκύπτει η τελική απόφαση σε χρονικό διάστημα μικρότερο του ενός δευτερολέπτου.



Εικόνα 2.29 Οπτική αναπαράσταση φωνητικών αποτυπωμάτων της ίδιας λέξης από δυο διαφορετικούς ομιλητές.

Η ακρίβεια του αποτελέσματος αυτού εξαρτάται και από εξωτερικούς παράγοντες. Για παράδειγμα η συσκευή που χρησιμοποιήθηκε κατά την εγγραφή της φωνής στη βάση δεδομένων μπορεί να είναι διαφορετική από αυτή που χρησιμοποιείται για την καταγραφή της βιομετρικής αναφοράς. Ο θόρυβος, η ασθένεια, η ηλικία μπορούν να αλλοιώσουν τη φωνή και κατά συνέπεια να διαστρεβλώσουν το αποτέλεσμα.

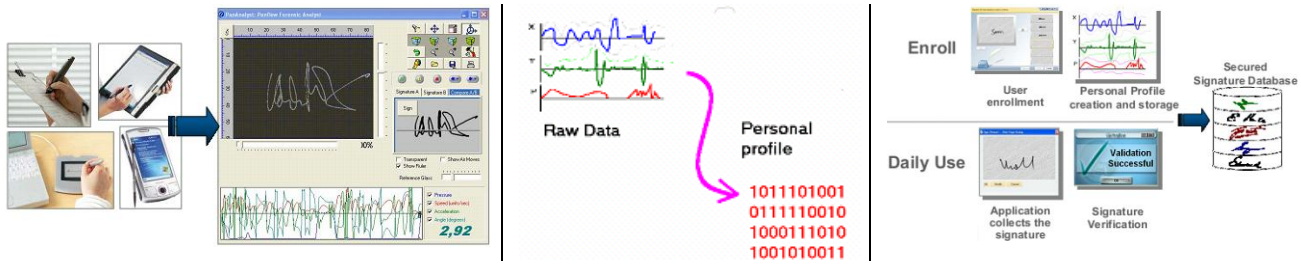
Τα πλεονεκτήματα του βιομετρικού αυτού χαρακτηριστικού είναι η ευχρηστία, η εύκολη αποδοχή από τους χρήστες, το μικρό μέγεθος της κάθε εγγραφής στη βάση δεδομένων που δεν ξεπερνά το 1K και η υψηλή ταχύτητα του συστήματος. Ένα φωνητικό αποτύπωμα χρόνου 2-8 δευτερολέπτων είναι αρκετό για την πιστοποίησή όχι δυο δειγμάτων, η οποία ολοκληρώνεται σε μισό δευτερόλεπτο. Το σύστημα όμως είναι επιρρεπή σε όσους θελήσουν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Εάν για παράδειγμα κάποιος εν δυνάμει εισβολέας αναπαράγει κάποιο ηχογραφημένο μήνυμα του εξουσιοδοτημένου χρήστη τη στιγμή που του ζητηθεί να πει μια φράση, τότε είναι πολύ πιθανό να αποκτήσει πρόσβαση στο σύστημα. Για το λόγο αυτό δεν προτιμάται η χρήση της φωνή και μόνο για την πιστοποίηση ενός ατόμου, αλλά ο συνδυασμός της με κάποιο άλλο φυσιολογικό χαρακτηριστικό όπως είναι η ίριδα, το πρόσωπο, το αυτί κλπ.

2.9 Αναγνώριση υπογραφής

Η δυναμική υπογραφή είναι μια βιομετρική τεχνική βασισμένη στη συμπεριφορά του ανθρώπου με σκοπό την αναγνώριση των ανατομικών και συμπεριφοριστικών χαρακτηριστικών ενός ατόμου όταν αυτό εκθέτει την υπογραφή του. Στο εμπόριο εκτός από τις δυναμικές συσκευές υπογραφών υπάρχουν και τα ηλεκτρονικά συστήματα λήψης υπογραφών. Αυτά τα δυο δεν είναι ίδια και δεν πρέπει να συγχέονται καθώς τα συστήματα λήψης υπογραφών δεν αναλύουν την

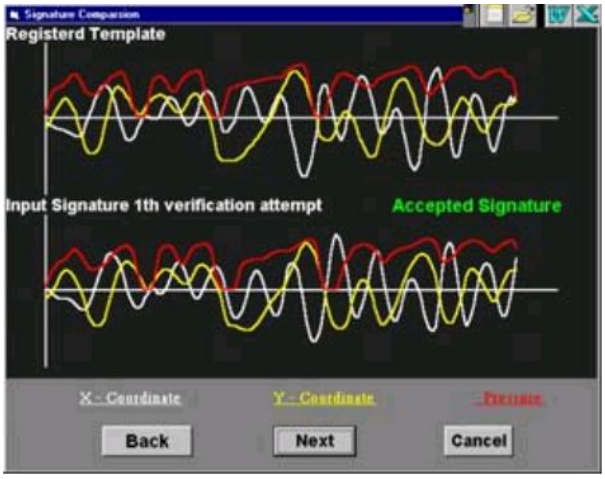
υπογραφή αλλά χρησιμοποιούνται σε εμπορικές συναλλαγές όταν απαιτείται η λήψη άδειας από κάποιον. Αντιθέτως στις δυναμικές συσκευές υπογραφών η υπογραφή αντιμετωπίζεται ως μια σειρά από κινήσεις που περιλαμβάνουν μοναδικά βιομετρικά δεδομένα όπως η δομή της γραφής, ο προσδιορισμός της πένας, ο ρυθμός, η ταχύτητα, η πίεση, η επιτάχυνση της γραφής.

Και σ' αυτή την τεχνική αναγνώρισης ατόμου η βασική διαδικασία είναι αρχικά η εγγραφή και αποθήκευση της αναφοράς ταυτότητας, και στη συνέχεια η απόκτηση και η σύγκριση της βιομετρικής αναφοράς με τα αποθηκευμένα στη βάση δεδομένων πρότυπα. Για την εγγραφή απαιτούνται παραπάνω από μια υπογραφές, συνήθως έξι και πάνω, διότι ποτέ δυο υπογραφές δεν είναι ακριβώς ίδιες, πάντα θα υπάρχει μια μικρή απόκλιση. Συλλέγονται με σύγχρονες συσκευές που περιέχουν οθόνες αφής και πένα όπως είναι τα tablets ή τα PDA στις οποίες ο χρήστης γράφει την υπογραφή του με τον ίδιο τρόπο που θα το έκανε και σε ένα χαρτί. Υπάρχουν



Εικόνα 2.30 (αριστερά) Συστήματα και λογισμικό λήψης υπογραφής.
Εικόνα 2.31 (κέντρο) Μετατροπή των δεδομένων της υπογραφής σε δυαδική μορφή.
Εικόνα 2.32 (δεξιά) Διάγραμμα διαδικασίας αναγνώρισης φωνής.

συστήματα που διαχειρίζονται πολλά προφίλ για ένα χρήστη. Για παράδειγμα ένας χρήστης μπορεί να έχει ένα προφίλ με μια τυπική υπογραφή και ένα προφίλ με την υπογραφή με τα αρχικά του. Η υπογραφή αυτή επεξεργάζεται, εξάγονται κάποια χαρακτηριστικά, μετατρέπεται σε δυαδική μορφή και με αυτή τη μορφή αποθηκεύεται ως αναφορά ταυτότητας στο προφίλ του χρήστη. Κατά τη διάρκεια που ο χρήστης ζητά πρόσβαση στο σύστημα, του ζητείται η υπογραφή του, από την οποία εξάγονται τα βιομετρικά χαρακτηριστικά όπως αυτά που αναφέρθηκαν παραπάνω και δημιουργείται η βιομετρική αναφορά. Οι αναφορές αναλύονται σε τρεις διαστάσεις στους x,y και z άξονες. Οι θέσεις x και y δείχνουν τις αλλαγές στην ταχύτητα στις αντίστοιχες κατευθύνσεις και η θέση z δείχνει τις αλλαγές της πίεσης ως προς το χρόνο. Η βιομετρική αναφορά συγκρίνεται με τις αναφορές ταυτοτήτων και τελικά επιλέγεται το προφίλ εκείνο που η αναφορά ταυτότητας του είναι πιο κοντά στην βιομετρική αναφορά.



Εικόνα 2.33 Γραφική απεικόνιση των δυναμικών χαρακτηριστικών της υπογραφής

Υπάρχουν συστήματα που ενσωματώνουν μια λειτουργία τέτοια ώστε να λαμβάνονται υπόψη οι φυσικές αλλαγές ή τα ολισθήματα που συμβαίνουν στην υπογραφή με το πέρας του χρόνου. Άλλα συστήματα όμως, πιο σύγχρονα, κάθε φορά που πραγματοποιείται μια αυθεντικοποίηση, παρακολουθούν τις σταδιακές μεταβολές της υπογραφής του χρήστη, έτσι ώστε να μην απορρίψουν το χρήστη αργότερα. Τα δυναμικά χαρακτηριστικά μιας υπογραφής είναι πολύπλοκα και μοναδικά για κάθε άτομο και είναι πολύ δύσκολο να αντιγραφούν, σε αντίθεση με μια στατική εικόνα (φωτογραφία) που μπορεί να αναπαρασταθεί από πλαστογράφο, από κάποιο υπολογιστή ή κάποιο φωτοαντίγραφο. Αν παρ' όλα αυτά όμως κάποιος καταφέρει και εισβάλλει στο σύστημα μια φορά, δεν θα είναι εύκολο να εισβάλλει ξανά με ευκολία, καθώς δεν θα πετύχει την "ξένη" υπογραφή με την ίδιο τρόπο. Εν κατακλείδι, παρά την αντοχή της δυναμικής αναγνώρισης υπογραφής, τα χαρακτηριστικά από προϊστορικούς χρόνους έχουν μεγάλες διακυμάνσεις και αυτό κάνει συχνά την αναγνώριση της δυναμικής υπογραφής δύσκολη.

Κεφάλαιο 3^{ο} Διερεύνηση μοντέλων εφαρμογής βιομετρικών συστημάτων και αρχιτεκτονικής υλοποίησης

Με τον καιρό οι απαιτήσεις των συστημάτων αυξάνονται και η τεχνολογία εξελίσσεται. Σήμερα τα βιομετρικά συστήματα είναι περισσότερα από ένα και διακρίνονται σε κατηγορίες ανάλογα με τη τοποθεσία αποθήκευσης και σύγκρισης των αναφορών ταυτότητας και των βιομετρικών αναφορών. Στο κεφάλαιο αυτό θα αναλύσουμε τους τύπους των μοντέλων που χρησιμοποιούνται σε πραγματικές εφαρμογές μέχρι και σήμερα. Πριν όμως, θα περιγράψουμε τις τοποθεσίες όπου αποθηκεύονται ή και συγκρίνονται οι αναφορές. Μια αναφορά, είτε πρόκειται για αναφορά ταυτότητας είτε για βιομετρική αναφορά μπορεί να αποθηκευτεί ή να συγκριθεί σε κάποιο server, client ή token.

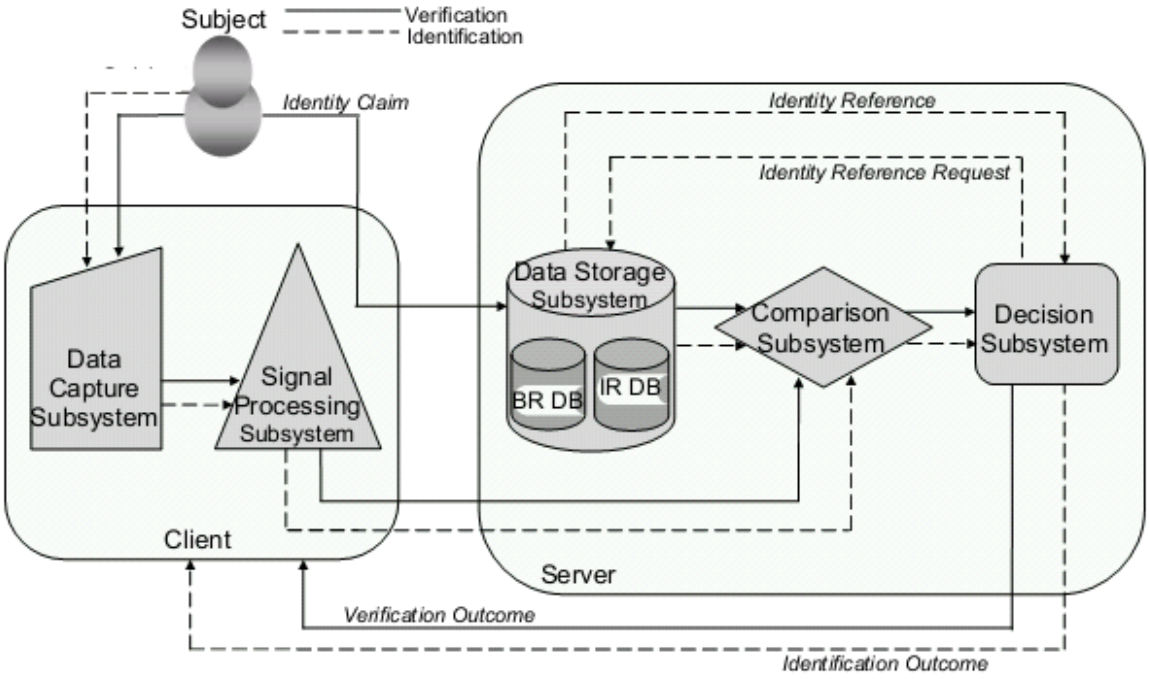
Server ή αλλιώς και εξυπηρετητής, ονομάζεται ένας υπολογιστής με τον οποίο συνδέονται ένας ή και περισσότεροι client υπολογιστές με τη χρήση δικτύου. Ο server μπορεί να αποθηκεύει, να διαχειρίζεται, να ανακτά, να προστατεύει πληροφορίες, να δημιουργεί αντίγραφα ασφαλείας και να χειρίζεται τις αιτήσεις των clients. Ένας server δεν ξεκινά ποτέ την επικοινωνία, αλλά είναι εκείνος που απαντά στις αιτήσεις των client υπολογιστών. Ο server ο οποίος αποθηκεύει και διαχειρίζεται πληροφορίες σχετικές με βιομετρικές αναφορές και αναφορές ταυτότητας καλείται "biometric authentication server".

Client ή αλλιώς πελάτης, είναι κι αυτός ένας υπολογιστής ή ένα λειτουργικό σύστημα το οποίο εκτελεί κάποιες εντολές. Clients θεωρούνται σήμερα και τα smartphones ή τα PDA. Ο client είναι εκείνος που ξεκινά πάντα μια επικοινωνία με τον server. Ένας client τρέχει το λογισμικό των γραφικών διεπαφών χρήστη, δημιουργεί τα αιτήματα για τις πληροφορίες που αναζητά, τα αποστέλλει στο server και αποθηκεύει τις επιστρεφόμενες πληροφορίες. Στη προκειμένη περίπτωση ο client παρέχει στον server ή σε κάποιο token υπηρεσίες ενός βιομετρικού συστήματος και τη διασύνδεση με τον server ή το token.

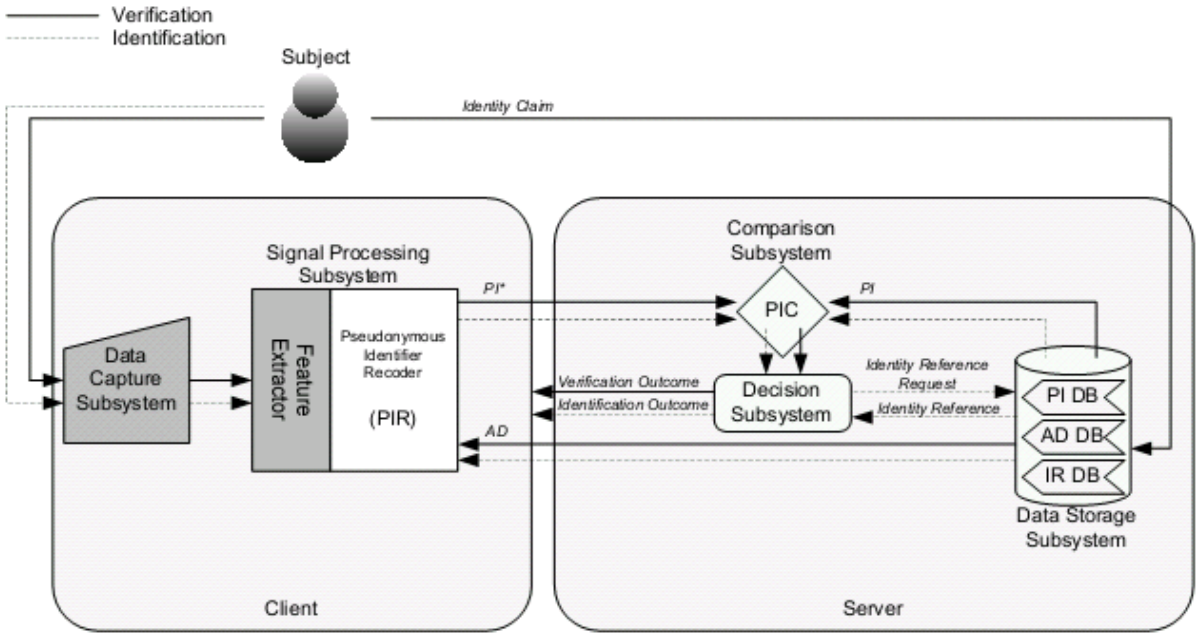
Token ή αλλιώς μάρκα ή δείγμα ταυτότητας, είναι μια μικρή φορητή συσκευή που επιτρέπει πρόσβαση σε μια υπηρεσία δικτύου. Η συσκευή αυτή μπορεί να είναι σε μορφή έξυπνης κάρτας, USB stick, ηλεκτρονικού διαβατηρίου. Οι συσκευές αυτές μπορούν να αποθηκεύσουν δεδομένα, και στην προκειμένη περίπτωση βιομετρικές αναφορές, καθώς επίσης και κάποιες φορές μπορούν να επιτρέψουν τη σύγκριση δυο αναφορών. Τα περισσότερα, αν όχι όλα τα token διαθέτουν βιομετρικούς αισθητήρες ώστε να μπορούν να καταγράψουν βιομετρικά δεδομένα και να τα αποθηκεύσουν.

3.1 Αποθήκευση στον server και σύγκριση στον server

Σύμφωνα με τον τύπο αυτό, τα δεδομένα αποθηκεύονται και συγκρίνονται στον server. Αρχικά η βιομετρική αναφορά και η αναφορά ταυτότητας συσχετίζονται στο πλαίσιο της διαδικασίας εγγραφής όπου και αποθηκεύονται στον server. Τη στιγμή που ο χρήστης επιθυμεί να πιστοποιήσει την ταυτότητά του, υποβάλλει ένα βιομετρικό χαρακτηριστικό του στον client. Αφού υποστεί την απαραίτητη επεξεργασία, εξάγονται κάποια βιομετρικά δεδομένα τα οποία μεταφέρονται στο server προκειμένου να πραγματοποιηθεί η σύγκριση με τις αναφορές ταυτότητας. Το μοντέλο αυτό χρησιμοποιείται και για ταυτοποίηση αλλά και για επαλήθευση δειγμάτων. Απαραίτητη βέβαια προϋπόθεση για αυτό είναι να εμπιστεύεται ο server τα στοιχεία που καταγράφονται από τον client. Επίσης από τη στιγμή που η διαδικασία πραγματοποιείται στον server απαιτείται αξιόπιστη ασφάλεια δεδομένων και ασφάλεια του δικτύου. Το μεγάλο αυτοματοποιημένο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων AFIS συνήθως εφαρμόζεται με βάση το μοντέλο αυτό, αν και από άποψη προστασίας ιδιωτικών δεδομένων δεν συνίσταται. Η σύγκριση πραγματοποιείται με δυο τρόπους, είτε συγκρίνοντας την αναφορά ταυτότητας με τη βιομετρική αναφορά, είτε συγκρίνοντας την αναφορά ταυτότητας με μια νέα βιομετρική αναφορά. Στην πρώτη περίπτωση συγκρίνεται η βιομετρική αναφορά που δημιουργήθηκε και αποθηκεύτηκε στον server κατά την εγγραφή του χρήστη, ενώ στη δεύτερη περίπτωση η νέα βιομετρική αναφορά δημιουργείται τη στιγμή που ο χρήστης υποβάλλει κάποιο χαρακτηριστικό του για αναγνώριση . Παρακάτω παρουσιάζονται διαγράμματα και για τις δυο περιπτώσεις.



Εικόνα 3.1 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση στο server και σύγκριση στο serverμε τη χρήση βιομετρικής αναφοράς.



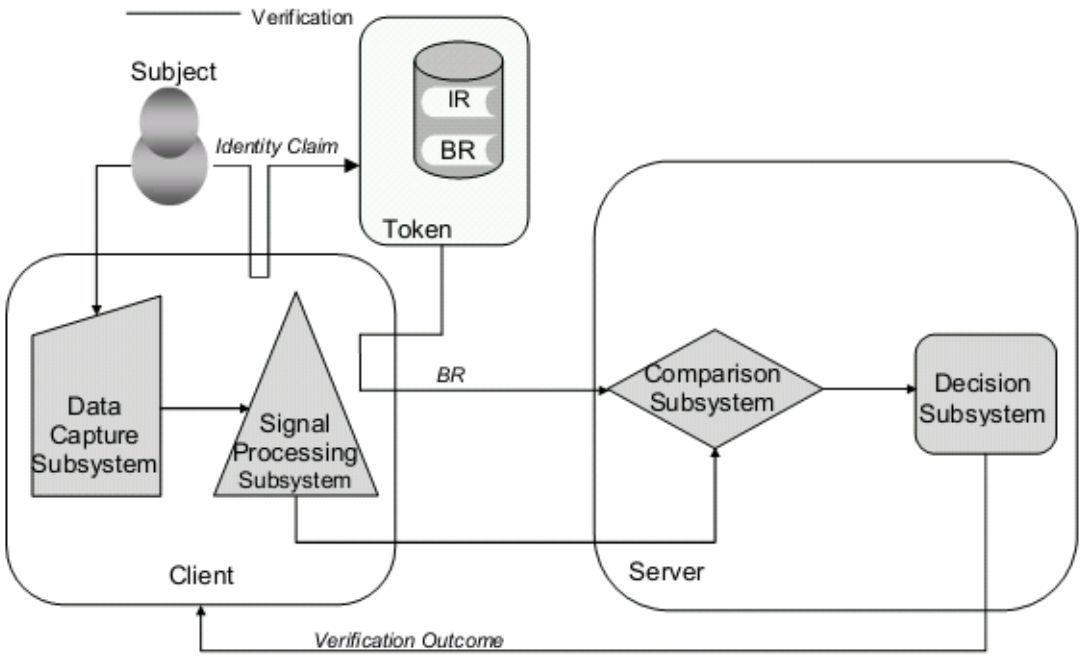
PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
PIC: Pseudonymous Identifier Comparator / Συγκριτής ψευδώνυμου αναγνώρισης
IR: Identity Reference / Αναφορά αυτότητας

Εικόνα 3.2 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση στον server και σύγκριση στον server με δημιουργία και χρήση νέας βιομετρικής αναφοράς.

3.2 Αποθήκευση σε token και σύγκριση στον server

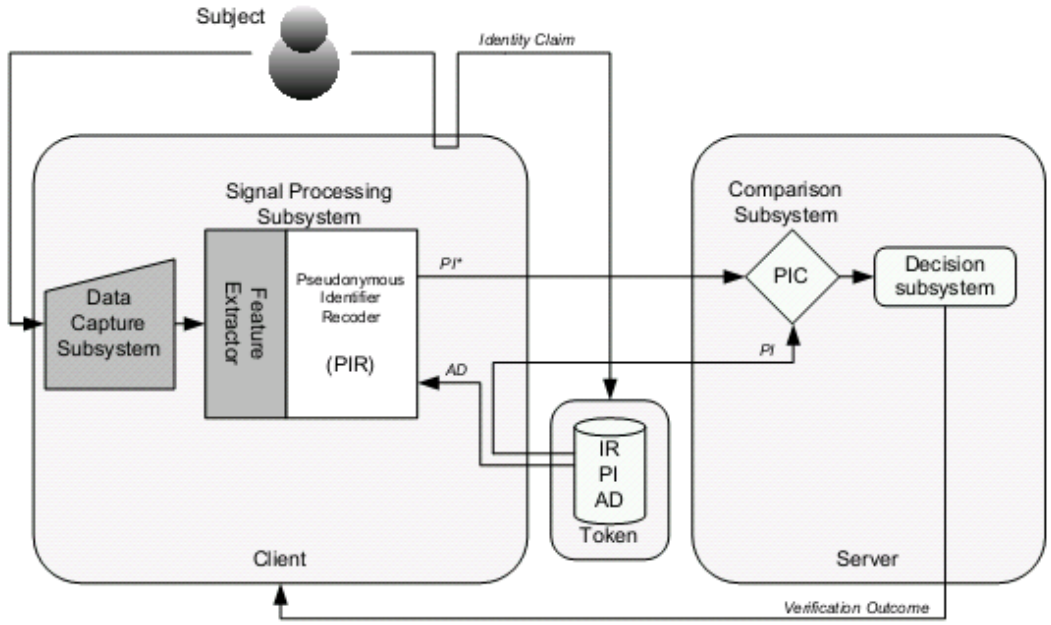
Στο μοντέλο αυτό χρησιμοποιείται μια εξωτερική συσκευή, ένα token, το οποίο αναλύσαμε παραπάνω, στο οποίο αποθηκεύονται οι αναφορές ταυτότητας. Όπως και στο προηγούμενο μοντέλο, η αναφορά ταυτότητας και η βιομετρική αναφορά συσχετίζονται κατά τη διαδικασία εγγραφής. Κατά τη διαδικασία επαλήθευσης ενός χρήστη ο client καταγράφει τα βιομετρικά δεδομένα από το χαρακτηριστικό που υποβάλλει ο χρήστης και τα επεξεργάζεται. Αφού πραγματοποιηθεί η απαραίτητη επεξεργασία αποστέλλει τα δεδομένα στον server όπου και θα πραγματοποιηθεί η σύγκριση. Το μοντέλο αυτό ενδείκνυται για επαλήθευση/ταυτοποίηση δειγμάτων και όχι για αναγνώριση καθώς δεν υπάρχει άλλη, παρά μόνο μια βιομετρική αναφορά για σύγκριση. Ο χρήστης που επιθυμεί να πιστοποιήσει την ταυτότητά του θα πρέπει να έχει μαζί του το token, να το συνδέσει στον client και να υποβάλλει κάποιο βιομετρικό χαρακτηριστικό του. Ο client στέλνει τα επεξεργασμένα δεδομένα στον server, το token στέλνει την αναφορά ταυτότητας στον server και πραγματοποιείται η σύγκριση.

Απαραίτητη προϋπόθεση εδώ είναι ο server να εμπιστεύεται τα δεδομένα που καταγράφει ο client. Δεν απαιτείται τόσο η ασφάλεια δεδομένων καθώς πρόκειται για μια μόνο αναφορά η οποία είναι αποθηκευμένη σε εξωτερική συσκευή και μάλιστα την κρατά στα χέρια του ο ίδιος ο χρήστης. Απαιτείται όμως η ασφάλεια του δικτύου για την προστατευμένη μεταφορά των δεδομένων από το token και των δεδομένων που ανιχνεύονται από τον client. Με αυτό τον τρόπο ο server εξασφαλίζει ότι τα δεδομένα προέρχονται από την διαδικασία εγγραφής και όχι από κάποια παρεμβολή στο δίκτυο.



Εικόνα 3.3 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση σε token και σύγκριση στον server με χρήση βιομετρικής αναφοράς.

Και σ' αυτό το μοντέλο η πιστοποίηση των αναφορών μπορεί να πραγματοποιηθεί και με τη δημιουργία νέας βιομετρικής αναφοράς. Στην περίπτωση αυτή, κατά τη διαδικασία εγγραφής δημιουργείται ένα ψευδώνυμο αναγνώρισης (PI) το οποίο αποθηκεύεται στο token. Κατά τη διάρκεια της πιστοποίησης στο server αποστέλλεται το ψευδώνυμο αναγνώρισης που αποθηκεύτηκε στο token και το καινούριο/ανακατασκευασμένο ψευδώνυμο αναγνώρισης (PI*) που εξάγεται από το βιομετρικό χαρακτηριστικό που υποβάλλει ο χρήστης τη στιγμή εκείνη.



PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
PIC: Pseudonymous Identifier Comparator / Συγκριτής ψευδώνυμου αναγνώρισης
IR: Identity Reference / Αναφορά αυτότητας

Εικόνα 3.4 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση σε token και σύγκριση στον server με δημιουργία και χρήση νέας βιομετρικής αναφοράς.

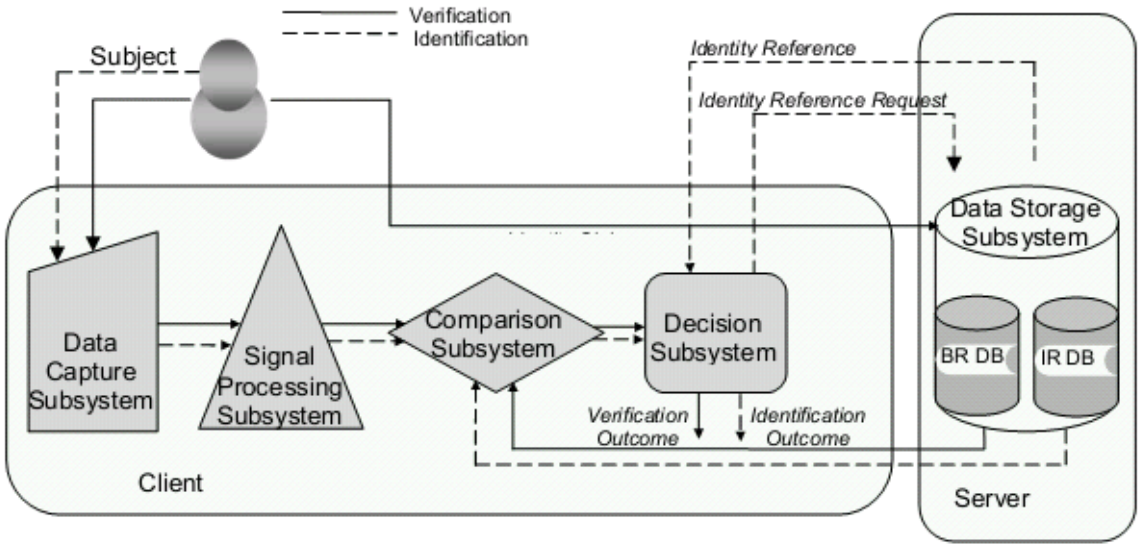
3.3 Αποθήκευση στον server και σύγκριση στον client

Στο συγκεκριμένο μοντέλο, αποθηκεύονται στον server οι βιομετρικές αναφορές και η σύγκριση για την ταυτοποίηση ή την αναγνώριση πραγματοποιείται στον client. Όπως και στα προηγούμενα μοντέλα, η αναφορά ταυτότητας και η βιομετρική αναφορά του χρήστη συσχετίζονται κατά τη διαδικασία εγγραφής, κατά την οποία αποθηκεύεται στον server η αναφορά ταυτότητας κάθε χρήστη που εγγράφεται. Το μοντέλο αυτό υποστηρίζει την ταυτοποίηση αλλά και την αναγνώριση ενός χρήστη. Ο χρήστης ο οποίος επιθυμεί να πιστοποιήσει την ταυτότητά του ή να αναγνωριστεί η ταυτότητά του, υποβάλλει στον client κάποιο βιομετρικό χαρακτηριστικό του. Ο client θα καταγράψει και θα επεξεργαστεί τα βιομετρικά χαρακτηριστικά του χρήστη και στη συνέχεια θα ζητήσει από τον server την αντίστοιχη ταυτότητα αναφοράς, προκειμένου να πραγματοποιήσει τη σύγκριση μεταξύ των δυο αναφορών. Ο server κατόπιν του αιτήματος αποστέλλει την αναφορά ταυτότητας και στη συνέχεια πραγματοποιείται η σύγκριση στον client. Ο client που χρησιμοποιείται σ' αυτό το μοντέλο βιομετρικού συστήματος θα πρέπει να είναι

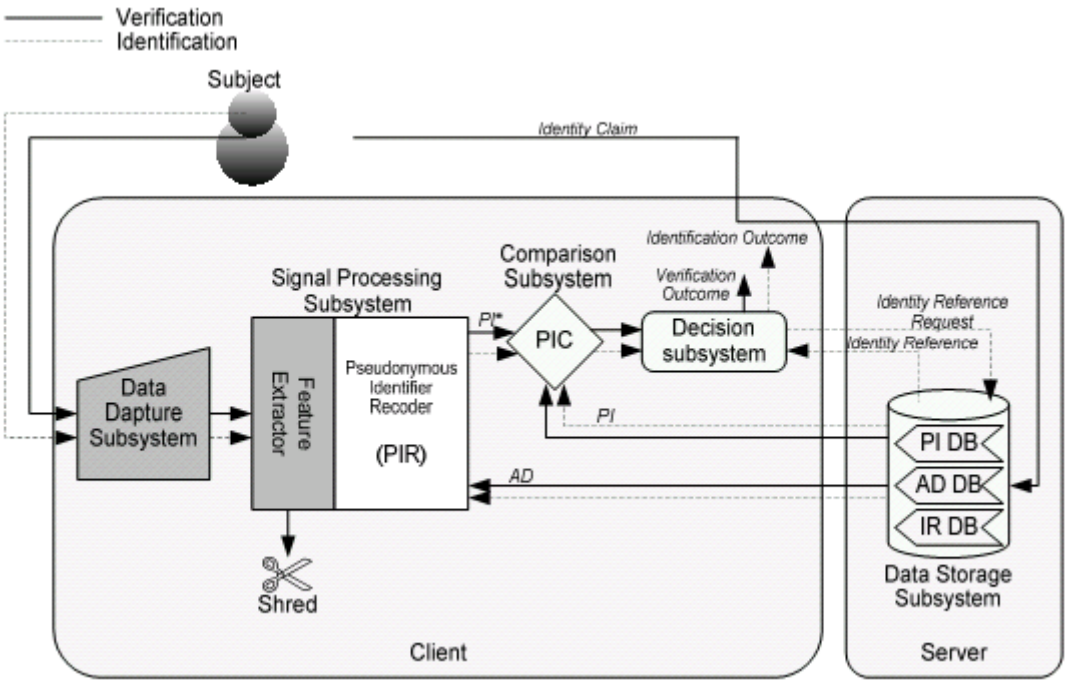
εξοπλισμένος με ένα βιομετρικό αισθητήρα προκειμένου να καταγράψει το χαρακτηριστικό που υποβάλλει ο χρήστης καθώς και ένα αλγόριθμο για τη σύγκριση των αναφορών και την απόφαση αναγνώρισης ή ταυτοποίησης.

Απαραίτητη προϋπόθεση για τη σωστή λειτουργία του μοντέλου αυτού είναι ο client να εμπιστεύεται τα δεδομένα που του αποστέλλει ο server. Απαιτείται η ύπαρξη μιας αξιόπιστης βάσης δεδομένων αφού τα δεδομένα είναι αποθηκευμένα στο server. Επίσης η ασφάλεια του δικτύου είναι απαραίτητη για την προστασία ιδιωτικών δεδομένων των χρηστών.

Η σύγκριση των αναφορών μπορεί να πραγματοποιηθεί είτε με τη χρήση υπάρχουσας βιομετρικής αναφοράς είτε με δημιουργία καινούριας.



Εικόνα 3.5 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση στον server και σύγκριση στον client με χρήση βιομετρικής αναφοράς.

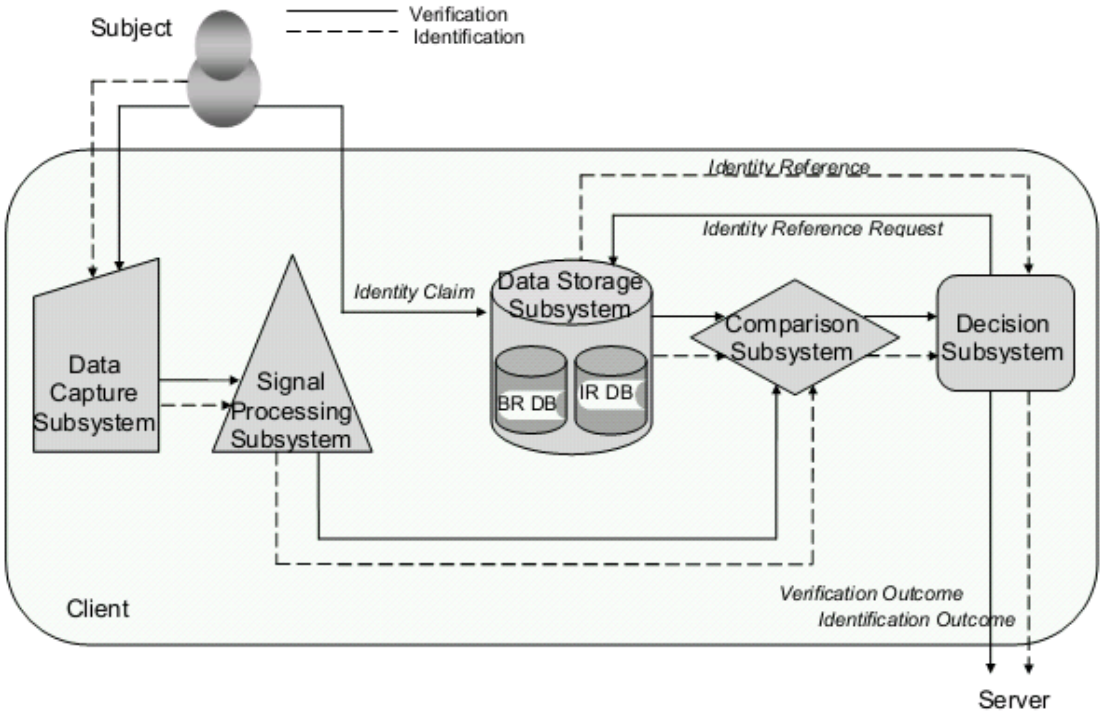


PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
IR: Identity Reference / Αναφορά αυτότητας

Εικόνα 3.6 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση στον server και σύγκριση στον client με δημιουργία και χρήση νέας βιομετρικής αναφοράς.

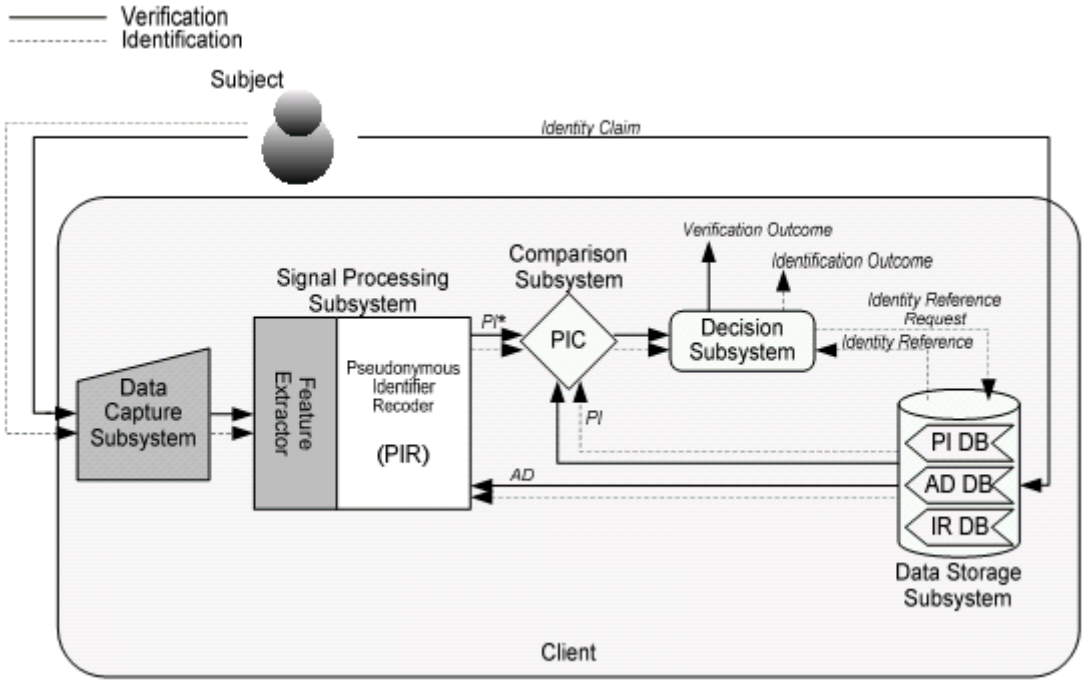
3.4 Αποθήκευση στον client και σύγκριση στον client

Στο πρότυπο αυτό οι βιομετρικές αναφορές αποθηκεύονται στον client και εκεί πραγματοποιείται και η σύγκριση. Βιομετρική αναφορά και αναφορά ταυτότητας κάθε χρήστη σχετίζονται κατά τη διαδικασία εγγραφής του. Όταν κάποιος χρήστης εγγράφεται στη βάση δεδομένων, αποθηκεύεται στον client η αναφορά ταυτότητας η οποία συσχετίζεται με τη βιομετρική αναφορά. Το μοντέλο αυτό ενδείκνυται για ταυτοποίηση αλλά και για αναγνώριση κάποιου χρήστη. Ο client είναι απαραίτητο να διαθέτει ένα βιομετρικό αισθητήρα για την καταγραφή βιομετρικών χαρακτηριστικών και ένα αλγόριθμο για τη σύγκριση και τη λήψη απόφασης ταυτοποίησης/αναγνώρισης ή μη. Έτσι λοιπόν, ο χρήστης που επιθυμεί να αναγνωριστεί ή να πιστοποιήσει την ταυτότητά του υποβάλλει στον client κάποιο βιομετρικό χαρακτηριστικό του. Ο client καταγράφει το χαρακτηριστικό, το επεξεργάζεται, ανακτά από τη μνήμη του τη βιομετρική αναφορά και πραγματοποιεί τη σύγκριση. Αφού ληφθεί η απόφαση την αποστέλλει στο server. Σε κάποιες περιπτώσεις ο client λειτουργεί ανεξάρτητα από το server πράγμα που σημαίνει πως δεν υπάρχει σύνδεση δικτύου μαζί του, και σε άλλες περιπτώσεις η τελική πιστοποίηση μπορεί να γίνει από το server ο οποίος επιβεβαιώνει τα αποτελέσματα της επαλήθευσης που δίνονται από τον client.



Εικόνα 3.7 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση στον client και σύγκριση στον client με τη χρήση βιομετρικής αναφοράς.

Το συγκεκριμένο σύστημα δεν απαιτεί υψηλές απαιτήσεις ασφάλειας δικτύου καθώς τα δεδομένα δεν μεταφέρονται σε κάποιο server. Απαιτείται όμως η ύπαρξη μιας αξιόπιστης βάσης δεδομένων στον client και συνίσταται η δημιουργία νέας βιομετρικής αναφοράς. Το μοντέλο αυτό χρησιμοποιείται συνήθως για την εξακρίβωση της γνησιότητας των ατόμων που χρησιμοποιούν συσκευές όπως προσωπικοί υπολογιστές γραφείου, φορητούς υπολογιστές και κινητά τηλέφωνα. Τώρα όσον αφορά την προστασία των προσωπικών δεδομένων των χρηστών, το μοντέλο αυτό είναι περισσότερο ευνοϊκό σε σύγκριση με τα μοντέλα τα οποία χρησιμοποιούν μια κεντρική βάση δεδομένων.



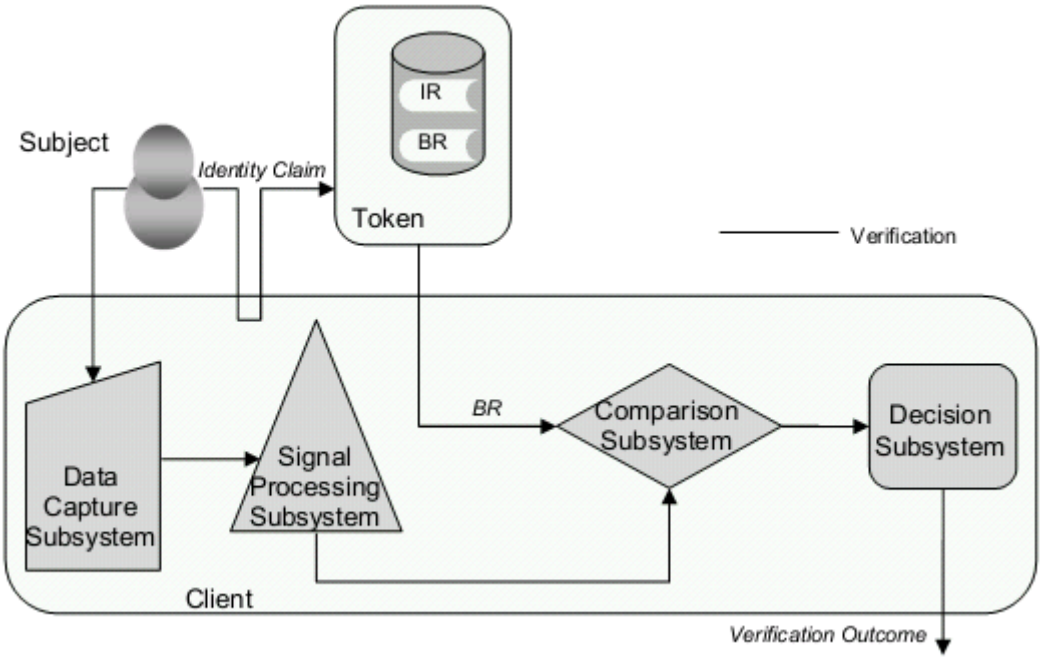
PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
IR: Identity Reference / Αναφορά αυτότητας

Εικόνα 3.8 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση στον client και σύγκριση στον client με δημιουργία και χρήση νέας βιομετρικής αναφοράς.

3.5 Αποθήκευση σε token και σύγκριση στον client

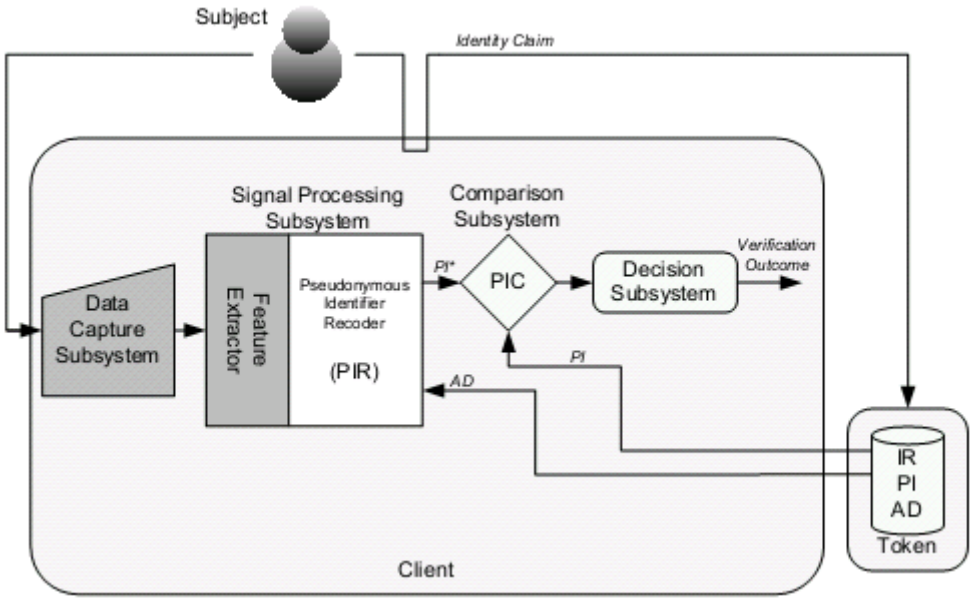
Σ΄ αυτό το μοντέλο βιομετρικού συστήματος τα βιομετρικά στοιχεία αποθηκεύονται σε κάποιο token, ενώ η σύγκριση πραγματοποιείται στον client. Κατά τη διάρκεια της εγγραφής συσχετίζονται η βιομετρική αναφορά και η αναφορά ταυτότητας κάθε χρήστη. Το συγκεκριμένο μοντέλο μπορεί να χρησιμοποιηθεί για την ταυτοποίηση ενός προσώπου. Ο client πρέπει να διαθέτει κατάλληλο εξοπλισμό για την ολοκλήρωση της διαδικασίας. Η ύπαρξη ενός βιομετρικού αισθητήρα είναι απαραίτητη, όπως επίσης και η ύπαρξη ενός αλγορίθμου για τη σύγκριση και τη λήψη απόφασης. Ο χρήστης λοιπόν που επιθυμεί να εισέλθει σε ένα σύστημα και ζητά να πιστοποιήσει την ταυτότητά του υποβάλλει στον client το token, από το οποίο ο client παίρνει τη βιομετρική αναφορά, και κάποιο βιομετρικό χαρακτηριστικό του, το οποίο ο client καταγράφει και επεξεργάζεται. Αφού υποστεί την απαραίτητη επεξεργασία τα δεδομένα που έχουν εξαχθεί συγκρίνονται, πάνω στον client, με τη βιομετρική αναφορά από το token και λαμβάνεται η απόφαση πιστοποίησης η μη.

Όσον αφορά τις απαιτήσεις ασφάλειας στο συγκεκριμένο σύστημα, από τη στιγμή που δεν υπάρχει σύνδεση μεταξύ client και server η ασφάλεια δικτύου δεν είναι υψίστης σημασίας, όμως η βάση δεδομένων που χρησιμοποιείται απαιτείται να είναι αξιόπιστη αφού εκεί αποθηκεύονται προσωπικά δεδομένα των χρηστών. Εφόσον στο μοντέλο μας δεν χρησιμοποιείται κάποια κεντρική βάση δεδομένων η ασφάλεια προσωπικών δεδομένων είναι υψηλότερη σε σύγκριση με συστήματα που χρησιμοποιούν κεντρικές βάσεις δεδομένων.



Εικόνα 3.9 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση σε token και σύγκριση στον client με τη χρήση βιομετρικής αναφοράς.

Εδώ ο client μπορεί να θεωρηθεί και σαν ένα διαδραστικό μηχάνημα το οποίο χρησιμοποιείται σε δημόσιους χώρους όπως τα αεροδρόμια ή άλλα δημόσια κτήρια για την επαλήθευση ταυτότητας. Οι βιομετρικές αναφορές και οι αναφορές ταυτότητας μπορούν να αποθηκευτούν σε ένα chip το οποίο μπορεί να είναι ενσωματωμένο στο token, όπως για παράδειγμα στα ηλεκτρονικά διαβατήρια. Σήμερα, στον έλεγχο των συνόρων με τη χρήση ηλεκτρονικών διαβατηρίων χρησιμοποιείται το συγκεκριμένο μοντέλο στα συστήματα πιστοποίησης.



PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα

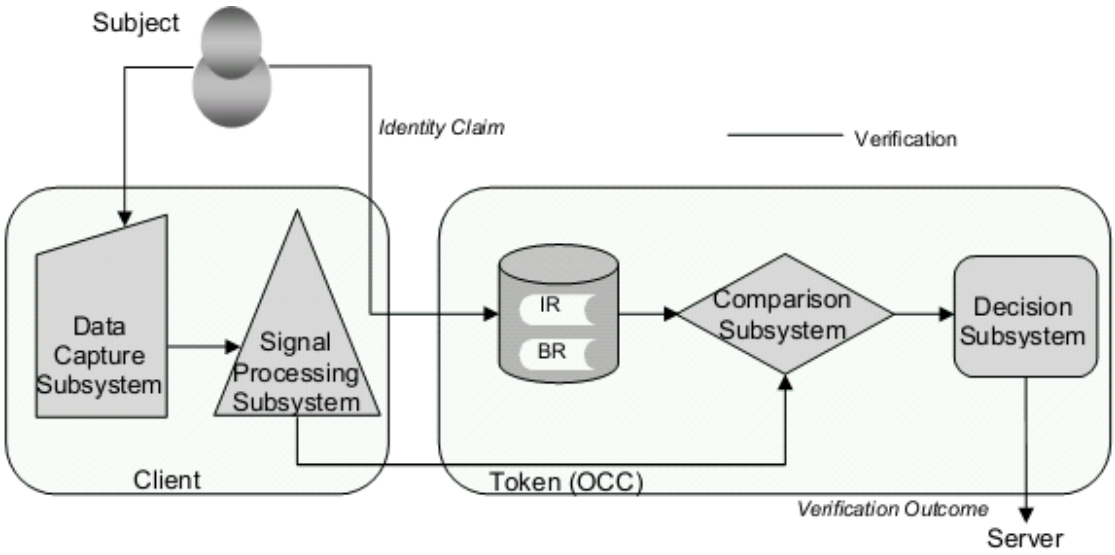
IR: Identity Reference / Αναφορά αυτότητας

Εικόνα 3.10 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση σε token και σύγκριση στον client με δημιουργία και χρήση νέας βιομετρικής αναφοράς.

Και στις δυο περιπτώσεις η επικοινωνία μεταξύ client και token, δηλαδή η εντολή προς το token για την καταγραφή των βιομετρικών χαρακτηριστικών και η μεταφορά τους στη συνέχεια θα πρέπει να πραγματοποιηθεί σύμφωνα με τη χρήση μηχανισμού μηνυμάτων ISO/IEC 7816-4.

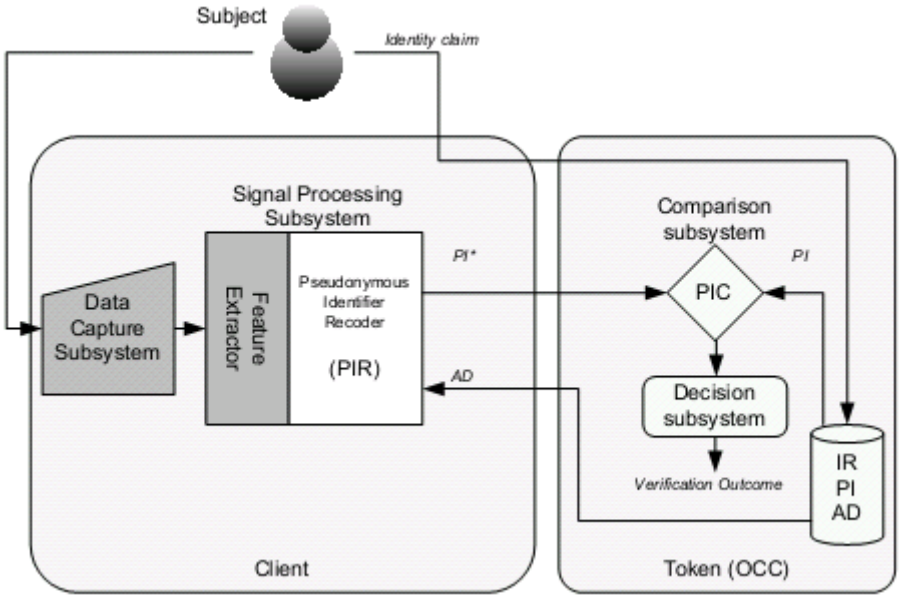
3.6 Αποθήκευση σε token και σύγκριση σε token

Σύμφωνα με αυτό το μοντέλο, στο token είναι αποθηκευμένα τα απαραίτητα δεδομένα για τη σύγκριση η οποία πραγματοποιείται στο token. Όπως και σε κάθε άλλο μοντέλο, οι δυο αναφορές κάθε χρήστη συσχετίζονται κατά την εγγραφή του χρήστη στο σύστημα. Για την ανάπτυξη του μοντέλου αυτού είναι απαραίτητος ο σωστός εξοπλισμός του token και του client. Το token θα πρέπει να διαθέτει έναν αλγόριθμο σύγκρισης και λήψης απόφασης και ο client θα πρέπει να έχει ένα βιομετρικό αισθητήρα για την καταγραφή δεδομένων. Τη στιγμή που κάποιος χρήστης επιθυμεί να πιστοποιήσει την ταυτότητά του θα πρέπει να υποβάλει στον client το token αλλά και κάποιο σημείο του σώματός του ως βιομετρικό χαρακτηριστικό. Ο client λαμβάνει και επεξεργάζεται το βιομετρικό χαρακτηριστικό, στη συνέχεια αποστέλλει τα εξαγόμενα δεδομένα και την αναφορά ταυτότητας στο token το οποίο πραγματοποιεί τη σύγκριση με τη βιομετρική αναφορά και το τελικό αποτέλεσμα καταλήγει στον server. Το μοντέλο αυτό ενδείκνυται μόνο για πιστοποίηση και όχι για αναγνώριση αφού στο token υπάρχει μόνο μια βιομετρική αναφορά και μια αναφορά ταυτότητας, αυτές του συγκεκριμένου χρήστη. Αποτελεί τον πιο ισχυρό μηχανισμό προστασίας των προσωπικών δεδομένων εφόσον αυτά είναι αποθηκευμένα στο token και κατά τη διαδικασία αναγνώρισης δεν συνδέονται με κάποια βάση δεδομένων.



Εικόνα 3.11 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση σε token και σύγκριση σε token με χρήση βιομετρικής αναφοράς.

Και σ’ αυτό το μοντέλο η σύγκριση μπορεί να γίνει είτε με τη χρήση υπάρχουσας βιομετρικής αναφοράς είτε με τη δημιουργία νέας. Στη δεύτερη περίπτωση ο client κατά την επεξεργασία των βιομετρικών χαρακτηριστικών χρειάζεται τα βοηθητικά δεδομένα και όχι το ψευδώνυμο αναγνώρισης (PI) όπως σε άλλα μοντέλα. Επομένως πριν ο client αποστείλει στο token τα δεδομένα για την αναγνώριση ζητά από αυτό να του μεταφερθούν τα βοηθητικά δεδομένα (AD), και το ψευδώνυμο αναγνώρισης παραμένει στο token.



PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
PIC: Pseudonymous Identifier Comparator / Συγκριτής ψευδώνυμου αναγνώρισης
IR: Identity Reference / Αναφορά αυτότητας

Εικόνα 3.12 Διάγραμμα βιομετρικού συστήματος. Αποθήκευση σε token και σύγκριση σε token με ανάκληση βιομετρικής αναφοράς.

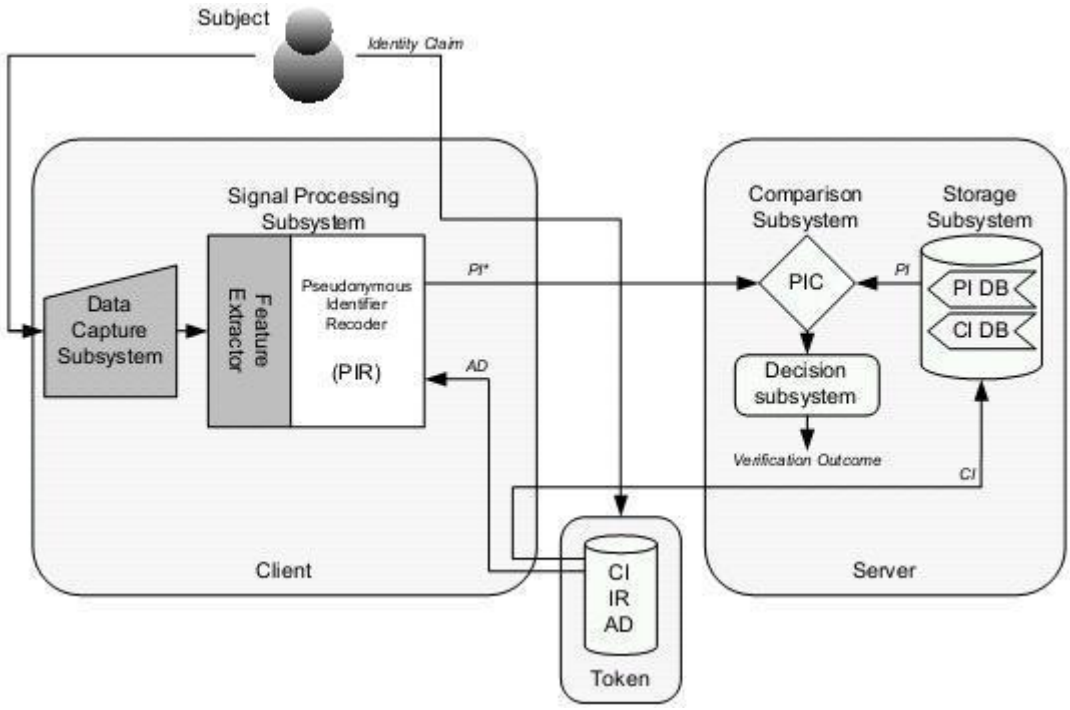
Και στις δυο περιπτώσεις η επικοινωνία μεταξύ client και token, δηλαδή η εντολή για την έναρξη της διαδικασίας και η αποστολή της τελικής απόφασης θα πρέπει να πραγματοποιηθούν σύμφωνα με τη χρήση μηχανισμού μηνυμάτων ISO/IEC 7816-4.

3.7 Κατανεμημένη αποθήκευση σε token και server και σύγκριση στον server

Το μοντέλο αυτό, όπως και το επόμενο που θα εξετάσουμε παρακάτω έχουνε μια ιδιαιτερότητα. Η βιομετρική αναφορά που χρησιμοποιείται κατά τη σύγκριση δημιουργείται εκείνη τη στιγμή. Ας αναλύσουμε όμως το συγκεκριμένο μοντέλο. Εδώ τα δεδομένα που χρησιμοποιούνται είναι κατανεμημένα σε ξεχωριστούς αποθηκευτικούς χώρους, τον server και το token. Κατά τη διάρκεια της εγγραφής λοιπόν κάθε χρήστη, δημιουργείται ένα ψευδώνυμο αναγνώρισης (PI) το οποίο αποθηκεύεται στο server και συνοδεύεται από ένα κοινό

αναγνωριστικό (CI). Το κοινό αυτό αναγνωριστικό αποθηκεύεται και στο token, μαζί με τα βοηθητικά δεδομένα (AD) και την αναφορά ταυτότητας (IR). Τη στιγμή που κάποιος χρήστης επιθυμεί να πιστοποιήσει την ταυτότητά του υποβάλλει στον client το token και κάποιο βιομετρικό του χαρακτηριστικό. Κατά τη διάρκεια της επαλήθευσης το token αποστέλλει στον client τα βοηθητικά δεδομένα και το κοινό αναγνωριστικό. Ο client με βάση τα υποβαλλόμενα δεδομένα δημιουργεί ένα νέο ψευδώνυμο αναγνώρισης (PI*) και το μεταφέρει στο server μαζί με το κοινό αναγνωριστικό. Ο server στη συνέχεια συγκρίνει τα δυο αναγνωριστικά, το ψευδώνυμο αναγνωριστικό που υπήρχε στη βάση δεδομένων (PI) και το νέο ψευδώνυμο αναγνωριστικό (PI*). Με βάση αυτή τη σύγκριση ο server κοινοποιεί και το τελικό αποτέλεσμα.

Ένα από τα πλεονεκτήματα του μοντέλου αυτού είναι ότι η νέα βιομετρική αναφορά κατανέμεται σε δυο αποθηκευτικούς χώρους –server και token– πράγμα που κάνει την επαλήθευση πιο έγκυρη και ασφαλής γιατί και οι δυο χώροι θα πρέπει να περιέχουν τα σωστά δεδομένα. Με αυτό τον τρόπο μειώνεται ο κίνδυνος παραβίασης των δεδομένων διότι για να μπορέσει κάποιος να παραβιάσει τα δεδομένα θα πρέπει να παραβιάσει τα δεδομένα και στο token αλλά και στον server. Ένα άλλο πλεονέκτημα του συστήματος είναι η ανάκληση βιομετρικών δεδομένων από το server, χωρίς να χρειάζεται η πρόσβαση στο token. Επίσης ένα τρίτο πλεονέκτημα είναι πως η διαδικασία πιστοποίησης της ταυτότητας του χρήστη εξαρτάται κυρίως από τον ίδιο αφού το token βρίσκεται στην ιδιοκτησία του.



PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
PIC: Pseudonymous Identifier Comparator / Συγκριτής ψευδώνυμου αναγνώρισης
IR: Identity Reference / Αναφορά αυτότητας
CI: Common Identifier / Κοινό αναγνωριστικό

Εικόνα 3.13 Διάγραμμα βιομετρικού συστήματος. Κατανεμημένη αποθήκευση σε token και server και σύγκριση στον server.

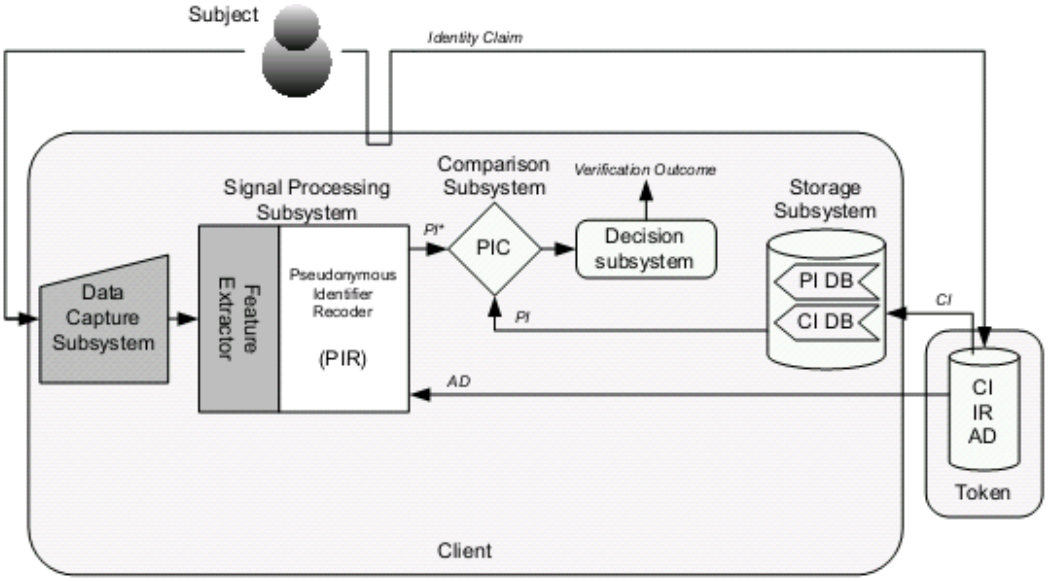
Το μοντέλο αυτό μπορεί να υποστεί κάποιες τροποποιήσεις χωρίς να αλλάξει η βασική του λειτουργία.

- Η αναφορά ταυτότητας μπορεί να αποθηκευτεί στον server αντί να αποθηκευτεί στο token.
- Προκειμένου να μη χρησιμοποιηθεί κάποια εξωτερική συσκευή (token), η αναφορά ταυτότητας (IR), τα βοηθητικά δεδομένα (AD) και το κοινό αναγνωριστικό (CI) μπορούν να αποθηκευτούν στη μνήμη του client και το ψευδώνυμο αναγνώρισης (PI) με το κοινό αναγνωριστικό (CI) να αποθηκευτούν στον server.
- Μπορεί να εφαρμοστεί αναγνώριση τριών παραγόντων στο μοντέλο αυτό αν το ψευδώνυμο αναγνώρισης (PI) αποθηκευτεί στον server αλλά και στο token. Σ΄ αυτή την περίπτωση η μονάδα η οποία πραγματοποιεί τη σύγκριση των ψευδώνυμων αναγνώρισης (PIC) λαμβάνει το ψευδώνυμο αναγνώρισης (PI) από το token, το ψευδώνυμο αναγνώρισης (PI) από τον server και το νέο ψευδώνυμο αναγνώρισης (PI*) από τον client και συγκρίνει και τα τρία ψευδώνυμα.

Σήμερα το μοντέλο αυτό εφαρμόζεται συνήθως σε συστήματα που σχετίζονται με συναλλαγές όπως για παράδειγμα online συναλλαγές με πιστωτική κάρτα, e-banking.

3.8 Κατανεμημένη αποθήκευση σε token και server και σύγκριση στον client

Όπως αναφέρθηκε παραπάνω, το μοντέλο αυτό έχει την ιδιαιτερότητα ότι η βιομετρική αναφορά που χρησιμοποιείται κατά τη σύγκριση δημιουργείται εκείνη τη στιγμή. Κατά τη διαδικασία εγγραφής η αναφορά ταυτότητας (IR), τα βοηθητικά δεδομένα (AD), και ένα κοινό αναγνωριστικό (CI) αποθηκεύονται σε μια εξωτερική συσκευή-ένα token, ενώ το ψευδώνυμο αναγνώρισης (PI) και το κοινό αναγνωριστικό (CI) αποθηκεύονται στη μνήμη του client. Όταν ο χρήστης επιθυμεί να εισέλθει στο σύστημα, θα πρέπει να υποβάλλει το token και κάποιο βιομετρικό του χαρακτηριστικό. Κατά τη διάρκεια της επαλήθευσής του λοιπόν, το token κοινοποιεί το κοινό αναγνωριστικό (CI) και τα βοηθητικά δεδομένα (AD) στον client. Ο client με βάση το κοινό αναγνωριστικό (CI), ανακτά το αντίστοιχο ψευδώνυμο αναγνωριστικό (PI) που είναι αποθηκευμένο στη βάση του και μεταφέρει τα βοηθητικά δεδομένα (AD) στη μονάδα καταγραφής του ψευδώνυμου αναγνωριστικού (PIR) η οποία δημιουργεί ένα νέο ψευδώνυμο αναγνώρισης (PI*) με βάση το υποβαλλόμενο βιομετρικό χαρακτηριστικό του χρήστη. Τα δυο ψευδώνυμα αναγνωριστικά, το υπάρχον στη βάση (PI) και το νέο που μόλις δημιουργήθηκε (PI*) συγκρίνονται και το αποτέλεσμα διαβιβάζεται στη μονάδα απόφασης για να κοινοποιηθεί το τελικό αποτέλεσμα.



PI: Pseudonymous Identifier / Ψευδώνυμο αναγνώρισης
AD: Auxiliary Data / Βοηθητικά δεδομένα
PIC: Pseudonymous Identifier Comparator / Συγκριτής ψευδώνυμου αναγνώρισης
IR: Identity Reference / Αναφορά αυτότητας
CI: Common Identifier / Κοινό αναγνωριστικό

Εικόνα 3.14 Διάγραμμα βιομετρικού συστήματος. Κατανεμημένη αποθήκευση σε token και server και σύγκριση στον client.

Το μοντέλο αυτό μπορεί να υποστεί κάποιες τροποποιήσεις χωρίς να αλλάξει η βασική του λειτουργία.

- Η αναφορά ταυτότητας (IR) μπορεί να αποθηκευτεί στον client, και όχι σε κάποιο token.
- Το ψευδώνυμο αναγνώρισης (PI) μπορεί να αποθηκευτεί στο token και τα βοηθητικά δεδομένα (AD) στον client.

Σήμερα το μοντέλο αυτό εφαρμόζεται συνήθως σε συστήματα κατάλληλα για δημόσιους χώρους, όπως αεροδρόμια και δημόσια κτήρια ή υπηρεσίες όπου απαιτείται η επαλήθευση ταυτότητας. Για παράδειγμα ένα τέτοιο σύστημα χρησιμοποιείται στον έλεγχο των συνόρων με τη χρήση των ηλεκτρονικών διαβατηρίων.

Εν κατακλείδι, τα περισσότερα βιομετρικά συστήματα απαρτίζονται συνήθως από ένα server, έναν ή περισσότερους clients που συνδέονται με το server μέσω δικτύου και κάποια εξωτερική συσκευή (token). Η ασφάλεια του κάθε βιομετρικού συστήματος ελέγχου ταυτότητας εξαρτάται τόσο από τις διαδικασίες που εκτελούνται, όσο και από το λειτουργικό σύστημα των συσκευών που καταγράφουν τα βιομετρικά χαρακτηριστικά του κάθε χρήστη. Εάν οι βιομετρικές συσκευές και οι απομακρυσμένες συσκευές που χρησιμοποιούνται σε ένα σύστημα διαθέτουν υψηλό επίπεδο ασφάλειας εξασφαλίζουν αξιόπιστα δεδομένα. Ταυτόχρονα εάν οι διαδικασίες που εκτελούνται σ ένα σύστημα, εκτελούνται με ασφάλεια, τότε η μονάδα που πιστοποιεί την ταυτότητα ενός προσώπου μπορεί να παρέχει το καλύτερο δυνατό αποτέλεσμα.

Πίνακας 1: Συγκριτική κατάταξη των μοντέλων εφαρμογής Βιομετρικών συστημάτων

Μοντέλο		Κατάλληλο ΓΙΑ		Ασφάλεια		Ενδεικτική χρήση
Αποθήκευση βιομετρικής υπογραφής	**Σύγκριση βιομετρικής υπογραφής**	**Πιστοποίηση Ταυτότητας**	**Αναγνώριση Ταυτότητας**	**ΠΛΕΟΝΕΚΤΗΜΑΤΑ**	**ΜΕΙΟΝΕΚΤΗΜΑΤΑ**	
server	**server**	ΝΑΙ	ΝΑΙ	• Ευκολία για το χρήστη (χωρίς χρήση token).	• Κίνδυνος παραβίασης προσωπικών δεδομένων. • Ασφάλεια δικτύου client-server.	Σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων AFIS
token	**server**	ΝΑΙ	ΟΧΙ	• Προστασία προσωπικών δεδομένων. • Η διαδικασία πιστοποίησης εξαρτάται από το χρήστη αφού έχει το token.	• Κίνδυνος παραβίασης προσωπικών δεδομένων. • Ασφάλεια δικτύου client-server.	Χρήση ATM με χρήση κάρτας
server	**client**	ΝΑΙ	ΝΑΙ	• Ευκολία για το χρήστη (χωρίς χρήση token).	• Απαιτείται αξιόπιστη βάση δεδομένων. • Ασφάλεια δικτύου client-server.	Σύστημα εισαγωγής υπαλλήλων μιας εταιρίας με χρήση καρτών
client	**client**	ΝΑΙ	ΝΑΙ	• Υψηλή προστασία πρ. δεδομένων σε σχέση με συστήματα που χρησιμοποιούν κεντρική βάση δεδομένων. • Ευκολία για το χρήστη (χωρίς χρήση token).	• Απαιτείται αξιόπιστη βάση δεδομένων.	Άνοιγμα προσωπικού Η/Υ με χρήση δακτυλικού αποτυπώματος
token	**client**	ΝΑΙ	ΟΧΙ	• Υψηλή προστασία πρ. δεδομένων, και μέγιστη όταν δεν χρησιμοποιείται κεντρική βάση δεδομένων.	• Απαιτείται αξιόπιστη βάση δεδομένων.	e-passports

**Η συνέχεια του πίνακα υπάρχει στην επόμενη σελίδα.

Συγκριτική κατάταξη των μοντέλων εφαρμογής Βιομετρικών συστημάτων

Μοντέλο		Κατάλληλο ΓΙΑ		Ασφάλεια		Ενδεικτική χρήση
Αποθήκευση βιομετρικής υπογραφής	**Σύγκριση βιομετρικής υπογραφής**	**Πιστοποίηση Ταυτότητας**	**Αναγνώριση Ταυτότητας**	**ΠΛΕΟΝΕΚΤΗΜΑΤΑ**	**ΜΕΙΟΝΕΚΤΗΜΑΤΑ**	
token	**token**	ΝΑΙ	ΟΧΙ	• Το πιο ασφαλές σύστημα για την προστασία πρ. δεδομένων. • Η διαδικασία πιστοποίησης εξαρτάται από το χρήστη αφού έχει το token.	• Για την ανάκληση βιομετρικών δεδομένων απαιτείται η χρήση token. • Κίνδυνος κλοπής του token και επομένως όλου του συστήματος και όλων των δεδομένων.	Ηλεκτρονική θυρίδα τραπέζης
token & server	**server**	ΝΑΙ	ΟΧΙ	• Αποθήκευση βιομετρικής ταυτότητας σε 2 χώρους, επομένως πιο έγκυρη και ασφαλής πιστοποίηση. • Ανάκληση βιομετρικών χαρακτηριστικών χωρίς πρόσβαση στον server. • Η διαδικασία πιστοποίησης εξαρτάται από το χρήστη αφού έχει το token.	• Διάρκεια, αφού ελέγχει και τους δύο χώρους για την πιστοποίηση	On-line συναλλαγές, e-banking
token & server	**client**	ΝΑΙ	ΟΧΙ	• Αποθήκευση βιομετρικής ταυτότητας σε 2 χώρους, επομένως πιο έγκυρη και ασφαλής πιστοποίηση. • Η διαδικασία πιστοποίησης εξαρτάται από το χρήστη αφού έχει το token.	• Διάρκεια, αφού ελέγχει και τους δύο χώρους για την πιστοποίηση	e-passports

Κεφάλαιο 4ο BioAPI

Το Δεκέμβριο του 1998 αναπτύχθηκε μια πολυεπίπεδη αρχιτεκτονική από το BioAPI Consortium έχοντας σαν στόχο να δημιουργήσει μια διεπαφή προγράμματος εφαρμογής η οποία θα είναι συμβατή με ένα ευρύ φάσμα βιομετρικών προγραμμάτων εφαρμογής και τεχνολογιών. Το BioAPI Consortium απαρτίζεται από πάνω από 120 οργανισμούς που έχουν κοινό στόχο να προωθήσουν την ανάπτυξη της αγοράς βιομετρικών στοιχείων. Οι απαραίτητες προδιαγραφές της εφαρμογής κυκλοφόρησαν το Μάρτιο του 2000 και λίγους μήνες αργότερα, το Σεπτέμβριο του 2000 κυκλοφόρησε και η εφαρμογή. Στο κεφάλαιο αυτό και θα αναλυθούν τα βασικά μέρη του BioAPI και θα κατανοηθεί η λειτουργικότητά του.

4.1 Τι είναι το BioAPI

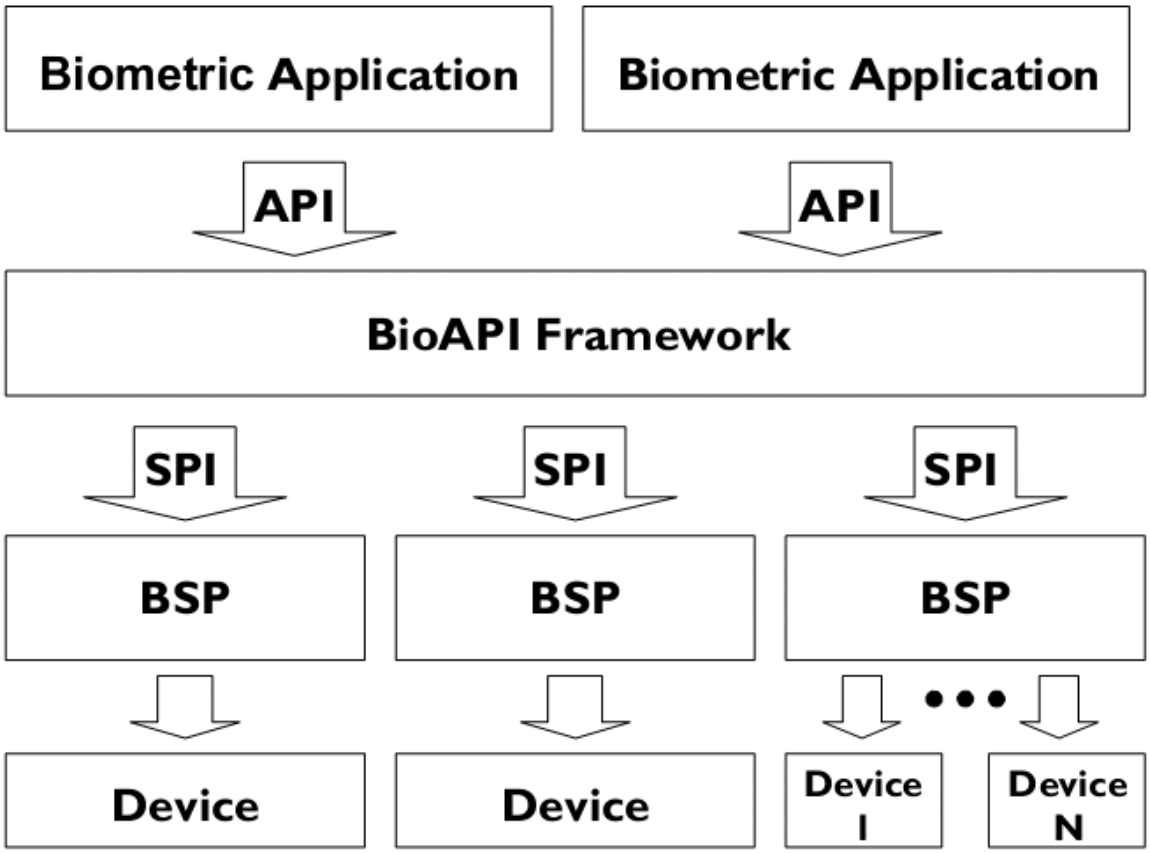
Το BioAPI είναι μια εφαρμογή η οποία προορίζεται να παρέχει ένα μοντέλο υψηλού επιπέδου γενικής βιομετρικής ταυτότητας. Ένα μοντέλο το οποίο καλύπτει τις βασικές λειτουργίες εγγραφής, επαλήθευσης και αναγνώρισης και περιλαμβάνει ένα περιβάλλον βάσης δεδομένων το οποίο επιτρέπει σε έναν παροχέα βιομετρικών υπηρεσιών (Biometric Service Provider – BSP) τη διαχείριση μιας βάσης δεδομένων με κωδικούς κάθε εγγραφής. Αυτό γίνεται για τη βελτιστοποίηση της απόδοσης της λειτουργίας αναγνώρισης για μεγάλους πληθυσμούς και για να παρέχει πρόσβαση σε κωδικούς οι οποίοι μπορούν να αποθηκευτούν σε αυτόνομη συσκευή ανίχνευσης. Παρέχει επίσης αρχέτυπα, πρότυπα, τα οποία δίνουν τη δυνατότητα στην εφαρμογή να διαχειριστεί τη σύλληψη των δειγμάτων για κάθε πελάτη καθώς και την εγγραφή, επαλήθευση και αναγνώριση σε ένα διακομιστή.

Το μοντέλο βιομετρικής ταυτότητας είναι το ίδιο για όλους τους τύπους της βιομετρικής τεχνολογίας. Χρησιμοποιεί συσκευές όπως αναγνώστες δακτυλικών αποτυπωμάτων, κάμερες για την αναγνώριση προσώπου, σαρωτές ίριδας, συσκευές αναγνώρισης υπογραφής, αγγειακά συστήματα απεικόνισης, κλπ προκειμένου να καταγράψει δεδομένα. Το αρχικό πρότυπο κατασκευάζεται με τη συλλογή ενός αριθμού δειγμάτων από μια τέτοια συσκευή. Μπορεί επίσης να παρέχει συσκευές υποστήριξης για την επεξεργασία εικόνας των βιομετρικών δεδομένων και την εξαγωγή χαρακτηριστικών γνωρισμάτων. Τα χαρακτηριστικά γνωρίσματα εξάγονται σε μια συγκεκριμένη μορφή συμπίεσης για μια δεδομένη βιομετρική τεχνολογία και επιτρέπει την άμεση αντιστοίχιση των συμπιεσμένων μορφών - για παράδειγμα, οι σχετικές αποστάσεις στην όψη των ματιών , τη μύτη, το στόμα, ή ο αριθμός των κορυφών μεταξύ κοιλάδων και κορυφογραμμών. Τα αποτελέσματα αυτά συνδυάζονται σε ένα πρότυπο ή πρόκειται να συγκριθούν με κάποιο πρότυπο αργότερα. Για την κατασκευή ενός προτύπου χρησιμοποιούνται μοναδικοί αλγόριθμοι. Στη συνέχεια το πρότυπο αποθηκεύεται από την εφαρμογή και αντιστοιχίζεται με ένα κωδικό πρόσβασης (Biometric Identification Record – BIR).

Οι εφαρμογές του BioAPI στην καθημερινότητά μας βασίζονται στην ικανότητα να μπορεί να διαχειρίζεται αιτήματα που σχετίζονται με προσωπικά στοιχεία αναγνώρισης (π.χ. πιστωτικές κάρτες) ή με πιο συγκεκριμένους τομείς όπως η επαλήθευση της ταυτότητας, οι έλεγχοι για διπλές εγγραφές, διαβατήρια ή φυσικός έλεγχος πρόσβασης σε κάποιο εμπορικό κέντρο ή για την είσοδο των υπαλλήλων σε αεροδρόμια, των ναυτικών του εμπορικού ναυτικού που επιθυμούν να μεταβούν στην ξηρά με την άφιξή τους στο λιμάνι.

4.2 Η βασική δομή του BioAPI

Το βασικό μοντέλο του Bio API απαρτίζεται από τέσσερα (4) βασικά στοιχεία. Τα Applications, το BioAPI Framework, τον Biometric Service Provider – BSP, και τον Biometric Function Provider – BFP. Εκτός από τα βασικά στοιχεία υπάρχουν και interfaces τα οποία διευκολύνουν την μεταξύ τους επικοινωνία. Πρόκειται για τα API και SPI interfaces.

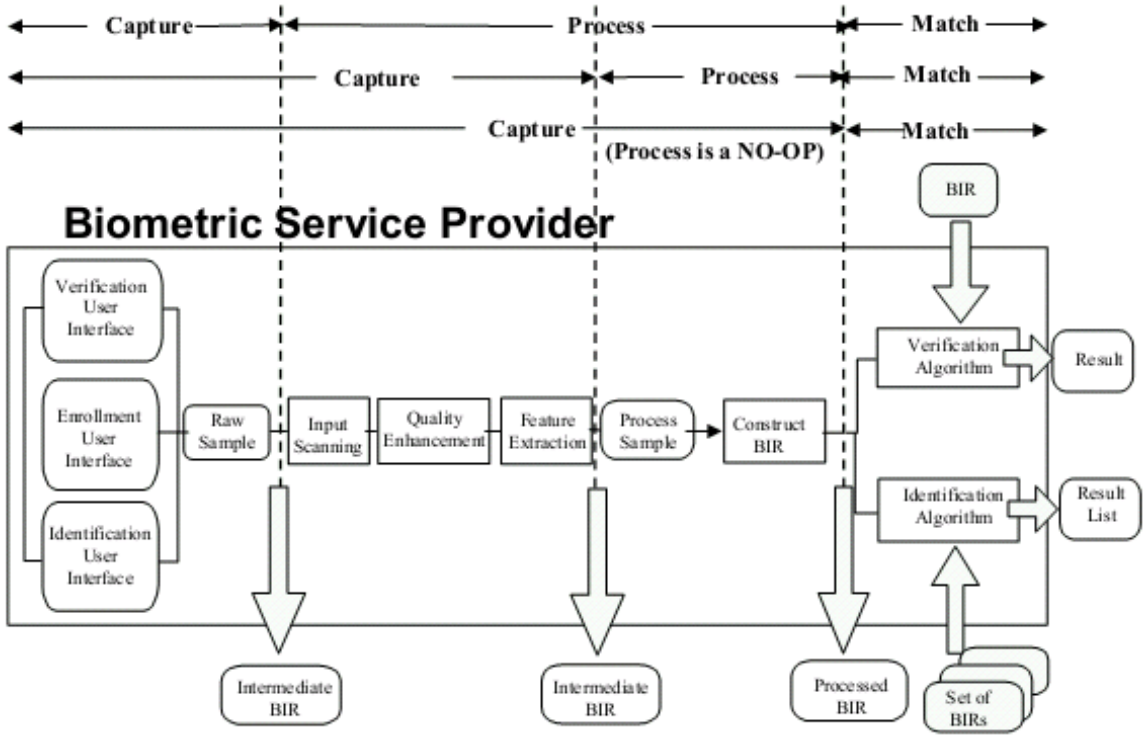


Εικόνα 4.1 Η βασική δομή του BioAPI.

Applications ή εφαρμογές όπως ονομάζονται στα ελληνικά, είναι προγράμματα τα οποία έχουν σχεδιαστεί για να εκτελούν κάποιες λειτουργίες απευθείας για τον χρήστη ή σε κάποιες περιπτώσεις για ένα άλλο πρόγραμμα. Το λογισμικό εφαρμογών μπορεί να χωριστεί σε δυο βασικές κατηγορίες: τα συστήματα λογισμικού και τις εφαρμογές λογισμικού. Τα συστήματα λογισμικού αποτελούνται από χαμηλού επιπέδου προγράμματα που αλληλεπιδρούν με τον υπολογιστή σε ένα βασικό επίπεδο. Αυτό περιλαμβάνει λειτουργικά συστήματα, μεταγλωττιστές καθώς και βοηθητικά προγράμματα για τη διαχείριση των πόρων του υπολογιστή. Αντίθετα οι εφαρμογές λογισμικού περιλαμβάνουν προγράμματα βάσης δεδομένων, επεξεργαστές κειμένου, λογιστικά φύλλα, οι οποίες δεν είναι σε θέση να τρέξουν χωρίς το λειτουργικό σύστημα. Στη δική μας περίπτωση μια τέτοια εφαρμογή μπορεί να αποτελείται από κάποια εξωτερική συσκευή και κάποια εφαρμογή η οποία είναι απαραίτητη για να λειτουργήσει η συσκευή. Τέτοιες συσκευές είναι συσκευές για την λήψη δακτυλικού αποτυπώματος, της ίριδας, του βαδίσματος κ.ο.κ.

Το **BioAPI Framework** αποτελεί την καρδιά του BioAPI διότι φέρνει σε επαφή όλα τα στοιχεία μαζί. Βρίσκεται ανάμεσα στις εφαρμογές και τον BSP. Ενεργοποιεί τις εφαρμογές προκειμένου να ζητήσουν διάφορες βιομετρικές υπηρεσίες και διευθετεί όλη τη διαδικασία “προσφοράς-ζήτησης”. Οι υπηρεσίες αυτές εξετάζονται από το BioAPI Framework για τα πλεονεκτήματα που μπορούνε να προσφέρουν και αν πληρούν τις προϋποθέσεις σύμφωνα πάντα με το πρότυπο του BioAPI τότε δρομολογείται η όλη διαδικασία. Το BioAPI Framework έχει κάποιες ενότητες και κάποιες βασικές λειτουργίες. Είναι υπεύθυνο για τη φόρτωση και την επισύναψη των δεδομένων που εισάγονται, τα διαχειρίζεται, ορίζει την εγγραφή στο σύστημα και διευθετεί τη διέλευση των δεδομένων από και προς τα API και SPI interfaces.

Ο **Biometric Service Provider** είναι ένα από τα βασικά στοιχεία που αποτελούν τη βασική δομή του BioAPI. Αφού το BioAPI Framework έχει επεξεργαστεί τα δεδομένα τα στέλνει στον BSP. Ο BSP παραλαμβάνει τα δεδομένα σε τέτοια μορφή έτσι ώστε να μπορεί να τα συγκρίνει με αποθηκευμένα πρότυπα. Συγκρίνει επομένως τα επεξεργασμένα δείγματα του χρήστη με ένα καθορισμένο σύνολο προτύπων και αποφασίζει ποια ταιριάζουν πιο πολύ.



Εικόνα 4.2 Στο σχήμα απεικονίζονται πιθανές στρατηγικές υλοποίησης της διαδικασίας.

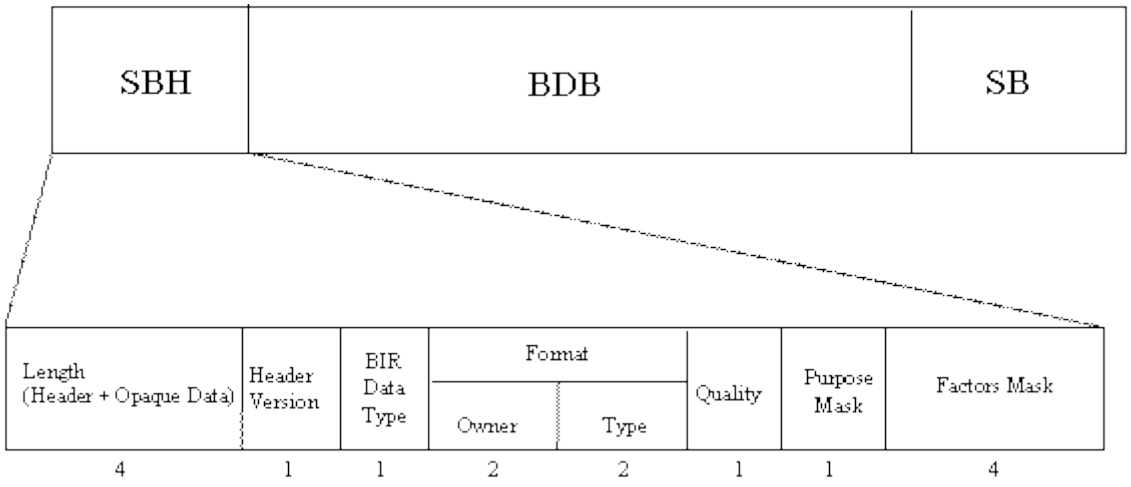
Ο **Biometric Function Provider** προστέθηκε αργότερα στη βασική δομή του μοντέλου BioAPI. Ορίζει ένα επιπλέον χαμηλότερο επίπεδο διεπαφής ανάμεσα στον ίδιο και τον έλεγχο του Biometric Service Provider. Αυτό έχει σαν αποτέλεσμα την ελαχιστοποίηση της ποσότητας λογισμικού που θα πρέπει να αναπτύξει μια συσκευή, επιτρέποντας έτσι σε άλλες συσκευές να κάνουν το μεγαλύτερο μέρος της εργασίας που θα έκανε ο BSP.

Τα **interfaces API** και **SPI** ελέγχουν την επικοινωνία μεταξύ των βασικών στοιχείων που απαρτίζουν τη βασική δομή του BioAPI. Με τη χρήση του API interface προσφέρεται στους χρήστες ένα χρήσιμο εργαλείο ανάπτυξης εφαρμογών το οποίο έχει κατασκευαστεί με βάση τις δικές τους ανάγκες. Εάν δεν υπήρχε αυτό, τότε κάθε χρήστης θα έπρεπε να γνωρίζει και να είναι σε θέση να κατασκευάσει προγραμματιστικά αιτήματα, λειτουργίες δηλαδή σε επίπεδο μηχανής. Το SPI είναι μια διεπαφή που επιτρέπει τη σειριακή ανταλλαγή των δεδομένων μεταξύ δυο συσκευών master-slave. Τα δεδομένα μεταφέρονται ταυτόχρονα και στις δυο κατευθύνσεις. Χρησιμοποιείται σε συστήματα για την επικοινωνία μεταξύ της κεντρικής μονάδας επεξεργασίας CPU και περιφερειακών συσκευών , καθώς επίσης και για τη σύνδεση μεταξύ δυο μικροεπεξεργαστών. Η κύρια δουλειά των δυο αυτών διεπαφών στην προκειμένη περίπτωση είναι να προβλέπουν

γεγονότα όπως τη σύλληψη των βιομετρικών δεδομένων που πρόκειται να μετατραπούν σε BIR κωδικούς, μια μορφή δηλαδή κατάλληλη για την ανταλλαγή ή μεταφορά τους σε άλλα στοιχεία. Προβλέπουν την μεταφορά των BIR κωδικών και την κίνηση μεταξύ του BSP και των εφαρμογών, τον τρόπο που ο BSP λαμβάνει, επεξεργάζεται, αντιστοιχίζει και αρχειοθετεί τα δεδομένα, καθώς επίσης και τα BFP interfaces τα οποία παρέχουν κάποιες συγκεκριμένες λειτουργίες για τον BFP.

4.3 Biometric Identification Record – BIR

Ο κωδικός πρόσβασης ή αλλιώς η βιομετρική εγγραφή αναγνώρισης (Biometric Identification Record – BIR) αναφέρεται σε οποιαδήποτε βιομετρικά δεδομένα τα οποία επιστρέφονται στην εφαρμογή. Περιέχει βιομετρικά δεδομένα συμπεριλαμβανομένων των πρώτων στοιχείων (προ επεξεργασίας) τα ενδιάμεσα στοιχεία και τα επεξεργασμένα στοιχεία, αυτά που είναι έτοιμα για εξακρίβωση ή αναγνώριση, καθώς και δεδομένα εγγραφής. Η βιομετρική εγγραφή αναγνώρισης είναι συστηματικά αποθηκευμένη στην εφαρμογή και δημιουργείται κατά την εγγραφή. Κάθε πρότυπο που υπάρχει στην εφαρμογή χαρακτηρίζεται από ένα τέτοιο κωδικό.



Εικόνα 4.3 Δομή της βιομετρικής εγγραφής αναγνώρισης BIR.

Το SBH (Standard Biometric Header) είναι το πρώτο βασικό μέρος του αρχείου, το οποίο αποτελείται από επιμέρους βασικά πεδία. Το BDB (Biometric Data Block) προσδιορίζει τα δεδομένα που έχουν αναλυθεί σε κάποιο βαθμό. Οι πληροφορίες των δεδομένων που παρέχει μπορεί να ανήκουν σε κάποιο πρότυπο ή δημιουργούνται εκείνη την ώρα κατά την εγγραφή ενός χρήστη, μπορεί να είναι δημοσιευμένα ή αδημοσίευτα, κρυπτογραφημένα ή μη κρυπτογραφημένα. Και τέλος το πεδίο SB (Security Block) περιέχει πληροφορίες για τον αλγόριθμο αναγνώρισης, πληροφορίες για τις παραμέτρους που απαιτούνται για την εκτέλεση της υπογραφής ή την εκτέλεση της συνάρτησης MAC (Message Authentication Code). Η συνάρτηση MAC είναι μια συνάρτηση κατακερματισμού που έχει προσχηματιστεί πάνω στα πεδία SBH και BDB.

4.4 Βασικές συναρτήσεις του μοντέλου API

Σύμφωνα με τις προδιαγραφές της πρώτης έκδοσης του BioAPI Specification Version 1.00 [2000] υπάρχουν τέσσερις πρωτόγονες συναρτήσεις του API οι οποίες αν εκτελεστούν στη σειρά μετατρέπουν τα αρχικά δεδομένα σε τέτοια μορφή ώστε να μπορούν να χρησιμοποιηθούν από την εφαρμογή.

Η συνάρτηση για τη **σύλληψη** των δεδομένων πραγματοποιείται από τον client και απαραίτητη προϋπόθεση γι αυτό είναι να υπάρχει η κατάλληλη βιομετρική συσκευή. Σε αντίθετη περίπτωση επιστρέφεται ένα μήνυμα το οποίο ενημερώνει το χρήστη ότι δεν υποστηρίζεται η λειτουργία. Μετά την καταγραφή των δεδομένων επέρχεται η επεξεργασία τους. Η επεξεργασία αυτή μπορεί να πραγματοποιηθεί είτε στη φάση της καταγραφής, είτε στη φάση της επαλήθευσης ή πιστοποίησης. Αφού ολοκληρωθεί η διαδικασία επεξεργασίας δημιουργείται ο κωδικός BIR. Εάν η επεξεργασία δεν έχει ολοκληρωθεί, ο τύπος του κωδικού BIR παίρνει την τιμή intermediate έτσι ώστε αργότερα να κληθεί ξανά η διαδικασία/συνάρτηση προκειμένου να ολοκληρωθεί η επεξεργασία. Αντίθετα, αν η επεξεργασία έχει ολοκληρωθεί, αυτό καταγράφεται στον τύπο του κωδικού BIR ο οποίος τώρα παίρνει την τιμή processed. Στον processed κωδικό BIR δεν χρειάζεται να κληθεί ξανά η συνάρτηση. Το αν η επεξεργασία των δεδομένων θα ολοκληρωθεί στον server ή στον client καθορίζεται από την εφαρμογή και έτσι δίνεται η ευκαιρία στον BSP να κάνει ειδική επεξεργασία.

Η συνάρτηση της **επεξεργασίας** δεν είναι μια, αλλά πολλές. Υπάρχουν αλγόριθμοι που επεξεργάζονται τα αρχικά δεδομένα και χρησιμοποιούνται είτε από τον server, είτε και από τον client. Στόχος της διαδικασίας αυτής είναι να προετοιμάσει τα δεδομένα για επαλήθευση ή πιστοποίηση και όχι για εγγραφή. Σαν είσοδο παίρνει πάντα έναν κωδικό BIR τύπου intermediate, και με βάση τις πληροφορίες που παρέχει ο κωδικός αυτός, ολοκληρώνει την επεξεργασία των δεδομένων. Εάν ο client είναι αυτός που καλεί τη συνάρτηση, αφού ολοκληρώσει την επεξεργασία των δεδομένων επιστρέφει έναν κωδικό BIR τύπου processed, αλλιώς, εάν δεν έχει ολοκληρωθεί η επεξεργασία, επιστρέφει έναν κωδικό BIR τύπου intermediate, πράγμα που σημαίνει πως η συνάρτηση πρέπει να κληθεί και από τον server. Τώρα, όταν καλείται η συνάρτηση από τον server, η επεξεργασία πάντα ολοκληρώνεται και πάντα επιστρέφεται ένας κωδικός BIR τύπου processed.

Μια άλλη συνάρτηση που καλείται είναι αυτή της **σύγκρισης**. Όταν πρόκειται για την επαλήθευση ενός χρήστη συγκρίνεται ο επεξεργασμένος BIR κωδικός της εγγραφής με ένα πρότυπο που υπάρχει αποθηκευμένο στην εφαρμογή. Στην περίπτωση της πιστοποίησης ενός χρήστη συγκρίνεται ο επεξεργασμένος BIR κωδικός της εγγραφής με μια σειρά από αποθηκευμένα πρότυπα στην εφαρμογή. Οι συναρτήσεις σύγκρισης υποστηρίζονται και είναι πάντα διαθέσιμες στον server αλλά και στον client.

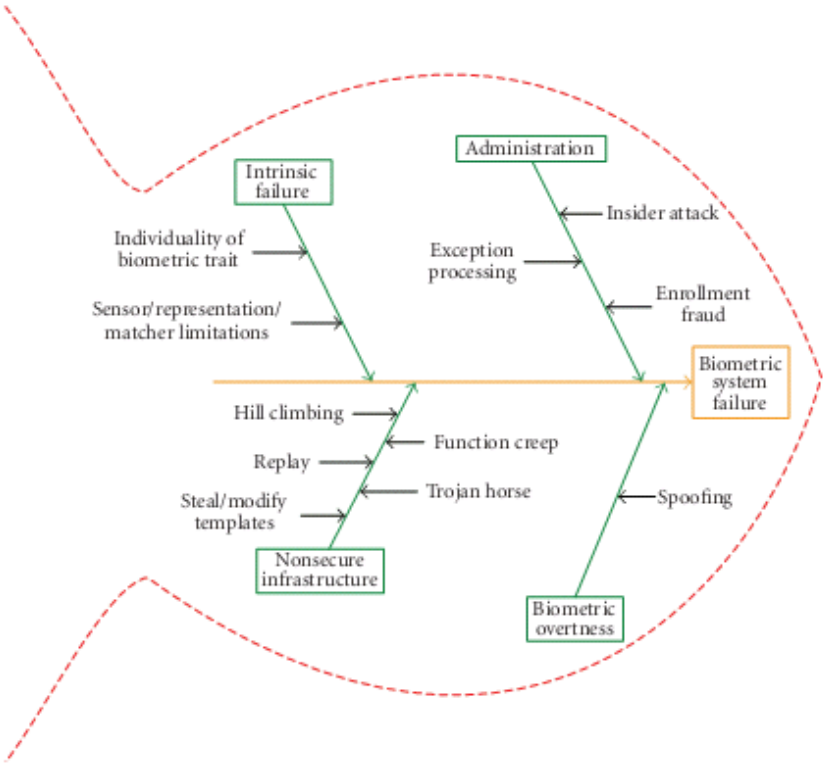
Η **δημιουργία προτύπου** παρέχεται σαν επιλογή από την εφαρμογή έτσι ώστε να κατασκευάζονται κάποια πρότυπα εγγραφής με βάση τα δείγματα που καταγράφονται στο σύστημα. Η συνάρτηση αυτή παίρνει πάντα σαν είσοδο έναν BIR κωδικό τύπου intermediate και κατασκευάζει ένα πρότυπο, αλλάζοντας τον τύπο του κωδικού BIR από intermediate σε processed, και καταγράφει στο αντίστοιχο πεδίο αν πρόκειται για επαλήθευση (enroll_verify) ή για πιστοποίηση (enroll_identify). Εναλλακτικά ένα πρότυπο μπορεί να δημιουργηθεί, αναπροσαρμόζοντας ένα παλιό πρότυπο ενσωματώνοντας τα νέα βιομετρικά δείγματα στον intermediate BIR κωδικό.

Κεφάλαιο 5^{ο} Ασφάλεια βιομετρικών προτύπων και ανάκληση βιομετρικών υπογραφών

Είναι γνωστό ότι η τεχνολογία αναπτύσσεται και διαδίδεται με ραγδαίους ρυθμούς. Τα βιομετρικά συστήματα έχουν εισβάλλει στην καθημερινότητα του ανθρώπου και πλέον τα προσωπικά δεδομένα των χρηστών βρίσκονται σε κίνδυνο από κακόβουλα σχέδια εισβολέων. Στόχος του κεφαλαίου αυτού είναι να γνωστοποιήσει ως ένα βαθμό τους παράγοντες που προκαλούν δυσλειτουργία στο σύστημα και να προσδιοριστούν οι επιθέσεις που μπορεί να προκύψουν σε ένα σύστημα. Τα πρότυπα ασφάλειας για τη δημιουργία βιομετρικών συστημάτων είναι πλέον από τα κρίσιμα ζητήματα γι' αυτό και θα αναφερθούν κάποιες προσεγγίσεις τέτοιων προτύπων. Τέλος θα αναλυθεί την έννοια της ανακλησιμότητας και ο ρόλος της στα βιομετρικά συστήματα καθώς και θα περιγραφεί η διαδικασία της ανάκλησης.

5.1 Ευαισθησία/Ευπάθεια βιομετρικών συστημάτων

Σύμφωνα με τους Anil K.Jail, Karthik Nandakumar and Abhishek Nagar [2007], τα αίτια που κάνουν ένα βιομετρικό σύστημα ευπαθή απεικονίζονται σε ένα μοντέλο γνωστό και ως fish-bone model. Τα αίτια αυτά διακρίνονται σε δυο βασικές κατηγορίες: την εγγενή αδυναμία (intrinsic failure) και την αποτυχία που οφείλεται από επίθεση τρίτου (adversary attack). Προβλήματα σε αισθητήρες, προβλήματα κατά την εξαγωγή χαρακτηριστικών γνωρισμάτων ή προβλήματα κατά την αντιστοιχία των βιομετρικών γνωρισμάτων με τα πρότυπα ανήκουν στη πρώτη κατηγορία. Από την άλλη πλευρά η απόπειρα κάποιου ξένου χρήστη/χάκερ ή ίσως μιας οργανωμένης ομάδας να εισβάλει σε ένα βιομετρικό σύστημα για προσωπικά οφέλη ανήκει στην δεύτερη κατηγορία.



Εικόνα 5.1 Το μοντέλο fish-bone, όπου απεικονίζονται οι αιτίες που κάνουν ένα βιομετρικό σύστημα ευπαθή.

5.1.1 Intrinsic failure

Υπάρχουν σφάλματα τα οποία προκύπτουν από μια λάθος απόφαση του βιομετρικού συστήματος. Τέτοιου είδους σφάλματα ανήκουν σ' αυτή την κατηγορία. Κατά τη διαδικασία λήψης αποφάσεων ενός βιομετρικού συστήματος μπορούν να προκύψουν δυο ειδών σφάλματα τα οποία ονομάζονται **false accept** (λάθος αποδοχή) και **false reject** (λάθος απόρριψη). Υπάρχουν κάποιες διαφορές ανάμεσα στο βιομετρικό πρότυπο του χρήστη και στα χαρακτηριστικά που δημιουργούνται κατά την επαλήθευση. Εξαιτίας των διαφορών αυτών είναι δυνατό να απορριφθεί λανθασμένα κάποιος γνήσιος χρήστης από το βιομετρικό σύστημα και να προκύψει ένα false accept σφάλμα. Αυτές οι διαφορές συνήθως οφείλονται είτε σε λάθος αλληλεπίδραση του χρήστη

με το σύστημα, όπως για παράδειγμα η λάθος τοποθέτηση του δακτύλου του, η διαφορετική πόζα, η διαφορετική έκφραση του προσώπου του κ.α., είτε λόγω του θορύβου που τυχόν υπάρχει στον αισθητήρα όπως για παράδειγμα υπολείμματα που έχουν παραμείνει στην επιφάνειά του. Αντίθετα, ένα false accept σφάλμα συμβαίνει από την έλλειψη της ατομικότητας ή της μοναδικότητας ενός βιομετρικού χαρακτηριστικού. Αυτό μπορεί να έχει σαν αποτέλεσμα τη μεγάλη ομοιότητα ενός συνόλου χαρακτηριστικών με περισσότερους από έναν χρήστη, όπως για παράδειγμα η ομοιότητα των εικόνων προσώπου σε δυο δίδυμα ή σε δυο αδέρφια. Και στις δυο περιπτώσεις μια λανθασμένη απόφαση μπορεί επίσης να προκύψει από τη χρήση ασήμαντων χαρακτηριστικών ή από ανίσχυρους προσαρμογείς (matchers). Κάποιες φορές ένας αισθητήρας μπορεί να μη συλλάβει σωστά το χαρακτηριστικό γνώρισμα γιατί ο χρήστης είτε έχει τοποθετήσει το βιομετρικό χαρακτηριστικό του σε λανθασμένα όρια, είτε το χαρακτηριστικό δεν βρίσκεται υπό τις σωστές συνθήκες, π.χ. ένα ξηρό ή υγρό δάκτυλο. Έτσι μπορεί να προκύψουν δυο ειδών σφάλματα στο σύστημα, η αποτυχία εγγραφής **failure-to-enroll (FTE)** ή η αποτυχία απόκτησης **failure-to-acquire (FTA).**

Αν σε κάποιο βιομετρικό σύστημα οι πιθανότητες να συμβούν false accept και false reject σφάλματα είναι υψηλές τότε είναι πιθανό να προκληθεί σφάλμα ακόμα κι αν κάποιος χάκερ δεν επιθυμεί να εισβάλει στο σύστημα. Τέτοιου είδους δυσλειτουργίες ονομάζονται zero-effort attack, επιθέσεις δηλαδή χωρίς να υπάρχει προσπάθεια για βλάβη του συστήματος. Έτσι στην προσπάθειά του ο άνθρωπος να μειώσει την πιθανότητα τέτοιων σφαλμάτων βελτίωσε αρκετά τα βιομετρικά συστήματα. Σχεδιάστηκαν νέοι αισθητήρες οι οποίοι αποκτούν τα βιομετρικά χαρακτηριστικά ενός ατόμου με πιο αξιόπιστο, άνετο και ασφαλή τρόπο, βελτιώθηκε η αμετάβλητη μορφή των προτύπων, δημιουργήθηκαν ισχυροί και αποτελεσματικότεροι αλγόριθμοι αντιστοίχισης (βιομετρικών χαρακτηριστικών-προτύπων) και ξεκίνησε η χρήση πολλαπλών βιομετρικών χαρακτηριστικών.

5.1.2 Adversary attacks

Κάθε βιομετρικό σύστημα δημιουργείται ανάλογα με τις ανάγκες και τις απαιτήσεις της εφαρμογής όπου και θα ενσωματωθεί και έτσι κάποια συστήματα υπερτερούν ή μειονεκτούν σε κάποια σημεία σε σχέση με άλλα συστήματα. Σύμφωνα με τους Anil K.Jail, Karthik Nandakumar and Abhishek Nagar [2007] με βάση τα κενά που τυχόν υπάρχουν στο σύστημα και τους υπολογιστικούς ή άλλους πόρους που διαθέτει ο εισβολέας, οι επιθέσεις χωρίζονται στις εξής επιμέρους κατηγορίες administration attack, nonsecure infrastructure και biometric overtness.

Administration attack: Η λάθος διαχείριση ενός βιομετρικού συστήματος μπορεί να δημιουργήσει τρωτά σημεία σε αυτό και να κάνει μια επίθεση πολύ πιο εύκολη. Τέτοια λάθη στη διαχείριση του συστήματος δημιουργούνται από την ακεραιότητα της διαδικασίας εγγραφής, την επικοινωνία μεταξύ εισβολέα και συστήματος ή νόμιμου χρήστη και συστήματος και την κατάχρηση των εξαιρέσεων σε μια διαδικασία.

Nonsecure infrastructure: Η υποδομή ενός βιομετρικού συστήματος αποτελείται από hardware, software και τα κανάλια επικοινωνίας μεταξύ των διαφόρων μονάδων. Οι επιθέσεις με βάση την υποδομή του βιομετρικού συστήματος χωρίζονται σε τέσσερις (4) κατηγορίες, attacks at the user interface (input level), attacks at the interfaces between modules, attacks on the modules, και attacks on the template database.

i. **Attacks at the userface**

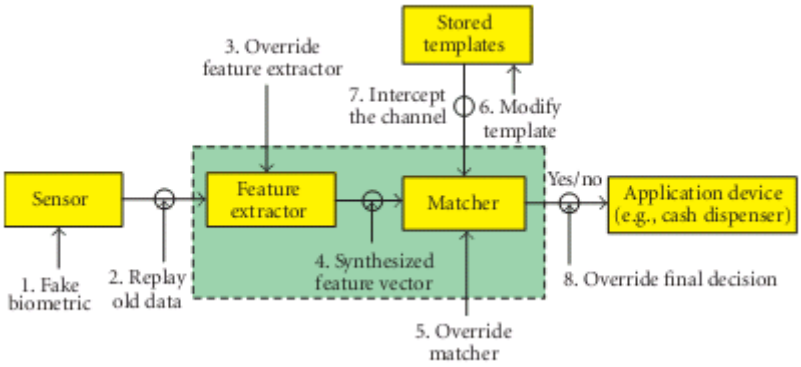
Αυτού του είδους η επίθεση οφείλεται κυρίως σε πλαστά βιομετρικά χαρακτηριστικά τα οποία προσπαθούν να ξεγελάσουν το σύστημα. Αν ο αισθητήρας ή η οποιαδήποτε συσκευή καταγραφής δεν είναι σε θέση να διακρίνει το γνήσιο από το πλαστό βιομετρικό χαρακτηριστικό τότε ο εισβολέας μπορεί να διεισδύσει στο σύστημα παριστάνοντας κάποιον άλλο, έχοντας δηλαδή αποκτήσει μια ψεύτικη ταυτότητα.

ii. **Attacks at the interfaces between modules**

Είναι γνωστό ότι σε ένα βιομετρικό σύστημα εκτός από την επικοινωνία μεταξύ χρήστη και διεπαφής υπάρχει και επικοινωνία μεταξύ διεπαφών όπου μεταφέρονται δεδομένα. Ο εισβολέας μπορεί να σαμποτάρει ή να εισβάλει στις διεπαφές μεταξύ των μονάδων του συστήματος. Εάν το κανάλι επικοινωνίας δεν είναι ασφαλές φυσικά ή κρυπτογραφικά τότε ο εισβολέας μπορεί να παρακολουθήσει, να κλέψει ή και να αλλάξει τα δεδομένα που μεταφέρονται. Για παράδειγμα μπορεί να τοποθετήσει ένα jammer το οποίο θα εμποδίσει την ορθή επικοινωνία του καναλιού. Μια λύση για να αντιμετωπιστεί μια τέτοιου είδους επίθεση είναι η κρυπτογράφηση και κωδικοποίηση των δεδομένων που μεταφέρονται με τη χρήση δημόσιου κλειδιού. Ακόμα και τότε όμως, ο εισβολέας μπορεί να κλέψει τα δεδομένα κλέβοντας τη θέση του γνήσιου χρήστη τη στιγμή που εκείνος πιστοποιεί την ταυτότητά του στο σύστημα. Ένα αντίμετρο γι αυτή την επίθεση είναι η χρήση timestamps και ο μηχανισμός challenge/response.

iii. **Attacks on the modules**

Τα εκτελέσιμα προγράμματα που χρησιμοποιούνται σε μια λειτουργική μονάδα είναι εύκολο να τροποποιηθούν με τέτοιο τρόπο έτσι ώστε να παράγουν αποτελέσματα που είναι επιθυμητά για τον εισβολέα. Τέτοιου είδους επιθέσεις είναι γνωστές και ως Trojan Horse. Για την αποφυγή Trojan horse επιθέσεων θα πρέπει να χρησιμοποιούνται ασφαλείς πρακτικές για την εκτέλεση του κώδικα ή κάποιο εξειδικευμένο υλικό το οποίο θα είναι ικανό να επιβάλλει την ασφαλή εκτέλεση του κώδικα. Επίσης το λογισμικό θα πρέπει να διέπεται από αλγοριθμική ακεραιότητα, να είναι δηλαδή σε θέση το λογισμικό να χειρίζεται οποιαδήποτε είσοδο σύμφωνα με τον επιθυμητό τρόπο. Για παράδειγμα, πρόκειται για αλγοριθμικό ατόπημα, όταν μια μονάδα σύγκρισης δέχεται μια συγκεκριμένη είσοδο Χ και κάθε φορά την αποδέχεται ως γνήσια. Η πράξη αυτή δεν οδηγεί σε κάποιο προγραμματιστικό λάθος, αλλά ένας εισβολέας μπορεί να εκμεταλλευτεί το κενό αυτό και να παραβιάσει την ασφάλεια του συστήματος χωρίς να γίνει αντιληπτός.



Εικόνα 5.2 Στο σχήμα απεικονίζονται τα σημεία όπου μπορεί να παρέμβει ένας χάκερ για να εισβάλει στο σύστημα.

iv. Attacks on the template database

Οι πιο επικίνδυνες επιθέσεις σε ένα βιομετρικό σύστημα είναι αυτές που έχουν σαν στόχο να βλάψουν τα βιομετρικά πρότυπα που είναι αποθηκευμένα στη βάση δεδομένων του συστήματος. Τρείς είναι οι πιθανές ευπάθειες που μπορεί να προκύψουν από μια επίθεση σε ένα πρότυπο.

1) Ένα πρότυπο μπορεί να αντικατασταθεί από το πρότυπο ενός χάκερ και έτσι ο χάκερ να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο σύστημα, αφήνοντας τον γνήσιο χρήστη απ' έξω.
2) Ένα πλαστό βιομετρικό χαρακτηριστικό μπορεί να δημιουργηθεί από το πρότυπο, να χρησιμοποιείται από το χάκερ και να του δίνει πρόσβαση στο σύστημα αλλά και σε άλλα συστήματα που διαθέτουν το ίδιο βιομετρικό χαρακτηριστικό.
3) Ένα κλεμμένο πρότυπο μπορεί να δοθεί από τον χάκερ τη στιγμή πριν τη σύγκριση προτύπου-χαρακτηριστικού που πραγματοποιεί ο προσαρμογέας και έτσι ο χάκερ να αποκτήσει για άλλη μια φορά μη εξουσιοδοτημένη πρόσβαση.

Φυσικά με κλεμμένα πρότυπα ένας χάκερ μπορεί να εισβάλει σε συστήματα που δεν σχετίζονται μεταξύ τους αρκεί να είναι εγγεγραμμένος ο ίδιος χρήστης. Μια λύση σε όλα αυτά μπορεί να δώσει η χρήση συστημάτων γνωστών και ως match-on-card ή system-on-card-technology, όπου ο αισθητήρας, η μονάδα εξαγωγής χαρακτηριστικών, ο προσαρμογέας και τα πρότυπα είναι αποθηκευμένα σε ένα token (βλ. ενότητα 3.6). Το βασικό πλεονέκτημα της τεχνολογίας αυτής είναι ότι οι βιομετρικές πληροφορίες δεν διαγράφονται από το token. Βέβαια σε εφαρμογές μεγάλης κλίμακας η λύση αυτή δεν είναι τόσο πρακτική διότι το κόστος είναι μεγάλο και κάθε χρήστης θα πρέπει να έχει συνέχεια μαζί του το token. Αυτό εγκυμονεί κινδύνους κλοπής, γι αυτό και είναι φρόνιμο να υπάρχουν κωδικοί πρόσβασης και κωδικοί PIN και στα token.

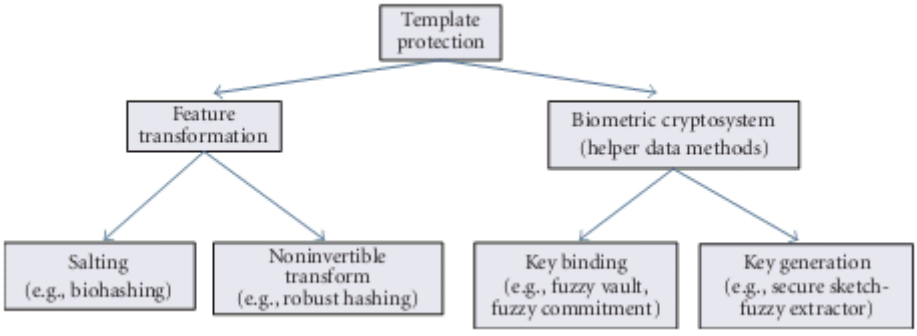
Biometric overtness: Είναι δυνατό ένας χάκερ που θέλει να εισβάλει στο βιομετρικό σύστημα να αποκτήσει κρυφά και παράνομα τα βιομετρικά χαρακτηριστικά του πραγματικού χρήστη. Για παράδειγμα να πάρει τα δακτυλικά του αποτυπώματα από μια επιφάνεια και να δημιουργήσει ένα τεχνητό μέλος (gummy fingers) και να το χρησιμοποιήσει τη στιγμή που το σύστημα θα ζητήσει την εισαγωγή του βιομετρικού χαρακτηριστικού. Εάν το σύστημα δεν είναι

ικανό να ξεχωρίσει ένα φυσικό χαρακτηριστικό από ένα τεχνητό χαρακτηριστικό, το οποίο παρουσιάζεται ως φυσικό, τότε ο χάκερ θα εισέλθει με μεγάλη επιτυχία στο σύστημά μας.

5.2 Βιομετρικά πρότυπα ασφάλειας

Πολλά βιομετρικά συστήματα απέρριπταν τους γνήσιους χρήστες από λάθη κατά την εισαγωγή των βιομετρικών χαρακτηριστικών γιατί η ασφάλεια του συστήματος ήταν πολύ αυστηρή. Εάν ένας χρήστης πραγματοποιούσε πολλές φορές την ίδια διαδικασία επαλήθευσης δεν ήταν σίγουρο ότι θα τον δεχόταν το σύστημα όλες τις φορές, κι αυτό γιατί οι πολλαπλές αποκτήσεις του ίδιου βιομετρικού χαρακτηριστικού δεν οδηγούν στο ίδιο σύνολο χαρακτηριστικών γνωρισμάτων μετά την εξαγωγή χαρακτηριστικών. Έτσι λοιπόν η μεγαλύτερη πρόκληση για το σχεδιασμό ενός βιομετρικού προτύπου ασφαλείας ήταν η ανάγκη να μπορεί το σύστημα να χειρίζεται τη μεταβλητότητα των χαρακτηριστικών των γνήσιων χρηστών. Σύμφωνα με τους Anil K.Jail, Karthik Nandakumar and Abhishek Nagar [2007] ένα ιδανικό βιομετρικό πρότυπο ασφαλείας θα πρέπει να χαρακτηρίζεται από τέσσερις (4) βασικές ιδιότητες την διαφορετικότητα, την δυνατότητα ανάκλησης, την ασφάλεια και την απόδοση.

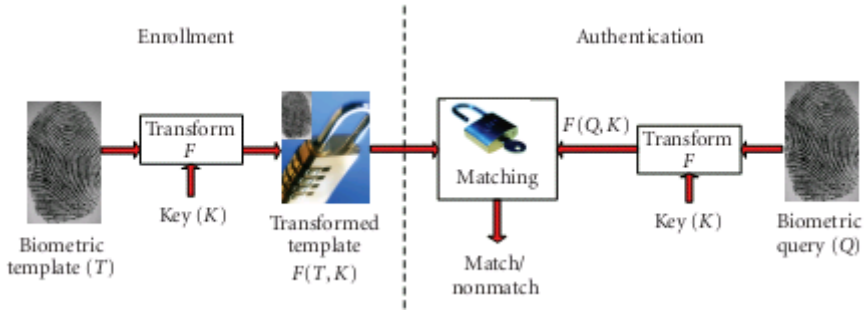
i. **Διαφορετικότητα:** Ένα ασφαλές βιομετρικό πρότυπο δεν θα πρέπει να επιτρέπει τη διασταύρωση των προτύπων μεταξύ δυο ή παραπάνω βάσεων δεδομένων, εξασφαλίζοντας έτσι την προστασία της ιδιωτικότητας του χρήστη.
ii. **Δυνατότητα ανάκλησης:** Θα πρέπει να είναι δυνατή και εύκολη η ανάκληση ενός προτύπου που βρίσκεται σε κίνδυνο και η δημιουργία ενός νέου προτύπου με βάση τα ίδια χαρακτηριστικά.
iii. **Ασφάλεια:** Θα πρέπει υπολογιστικά να είναι δύσκολο να αποκτηθεί το αρχικό βιομετρικό πρότυπο από το ασφαλές πρότυπο έτσι ώστε να μη μπορεί κάποιος χάκερ να ξεγελάσει το σύστημα χρησιμοποιώντας ένα πλαστό βιομετρικό χαρακτηριστικό.
iv. **Απόδοση:** Ένα βιομετρικό πρότυπο ασφάλειας δεν θα πρέπει να υποβαθμίζει την απόδοση αναγνώρισης (FAR και FRR) του βιομετρικού συστήματος.



Εικόνα 5.3 Κατηγοριοποίηση βιομετρικών προτύπων ασφαλείας.

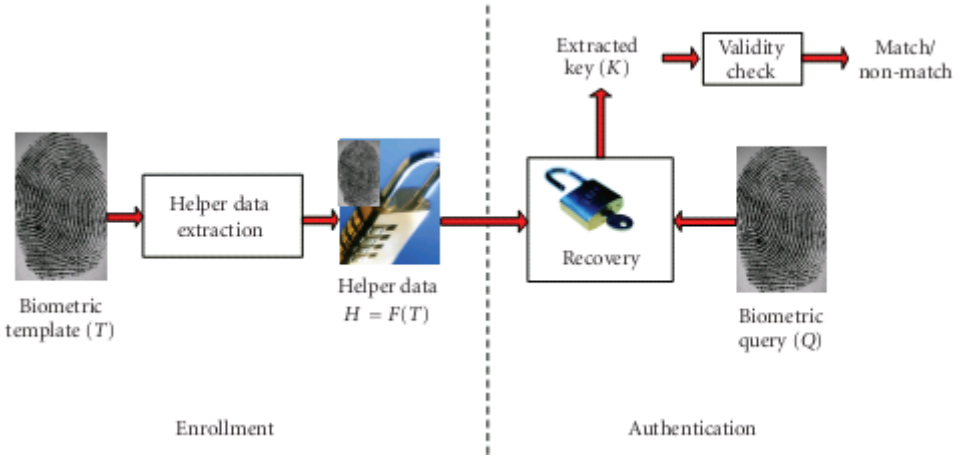
Τα βιομετρικά πρότυπα ασφαλείας που θα αναφερθούν παρακάτω μπορούν να ταξινομηθούν σε δυο βασικές κατηγορίες οι οποίες ονομάζονται feature transformation και biometric cryptosystem. Στην προσέγγιση feature transformation, η βασική διαδικασία που

ακολουθείται είναι η εξής. Μια συνάρτηση μετασχηματισμού εφαρμόζεται στο βιομετρικό πρότυπο και το αποτέλεσμα, δηλαδή το μετασχηματισμένο πρότυπο, αποθηκεύεται στη βάση δεδομένων. Η συνάρτηση μετασχηματισμού παίρνει παραμέτρους που προέρχονται από ένα τυχαίο κλειδί ή από ένα κωδικό. Η ίδια συνάρτηση εφαρμόζεται και στο βιομετρικό χαρακτηριστικό που δίνει ο χρήστης για την επαλήθευση και είσοδό του στο σύστημα. 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 noninvertible transform.



Εικόνα 5.4 Διαδικασία εγγραφής και αυθεντικοποίησης με βάση την προσέγγιση feature transformation.

Η άλλη βασική κατηγορία έχει σαν βασικό χαρακτηριστικό τα βιομετρικά κρυπτοσυστήματα τα οποία μπορούν να ενσωματωθούν σε ένα βιομετρικό σύστημα. Σε ένα βιομετρικό σύστημα κρυπτογράφησης αποθηκεύονται κάποιες δημόσιες πληροφορίες σχετικά με το βιομετρικό πρότυπο, οι οποίες ονομάζονται βοηθητικά δεδομένα. Τα βοηθητικά αυτά δεδομένα δεν αποκαλύπτουν σημαντικές πληροφορίες για το αρχικό βιομετρικό πρότυπο, παρ' όλα αυτά όμως είναι απαραίτητα κατά τη διάρκεια της σύγκρισης για να εξαχθεί ένα κρυπτογραφικό κλειδί από τα βιομετρικά χαρακτηριστικά που δίνει ο χρήστης για την επαλήθευσή του. Η σύγκριση πραγματοποιείται επαληθεύοντας αν το κλειδί αυτό είναι έγκυρο ή όχι. Τα βιομετρικά κρυπτοσυστήματα διακρίνονται κι αυτά με τη σειρά τους σε δυο υποκατηγορίες ανάλογα με το είδος του κλειδιού key-binding και key-generation συστήματα.



Εικόνα 5.5 Διαδικασία εγγραφής και αυθεντικοποίησης με βάση την προσέγγιση biometric cryptosystem.

5.2.1 Salting

Στην salting προσέγγιση χρησιμοποιείται μια συνάρτηση η οποία ορίζεται από έναν κωδικό πρόσβασης ή ένα κλειδί και μετατρέπει τα βιομετρικά χαρακτηριστικά. Η προσέγγιση αυτή χαρακτηρίζεται ως αντιστρέψιμη, πράγμα το οποίο σημαίνει πως όταν κάποιος χάκερ αποκτήσει πρόσβαση στο κλειδί και στο μετασχηματισμένο πρότυπο, τότε μπορεί εύκολα να ανακτήσει το αρχικό βιομετρικό πρότυπο ή έστω μια προσέγγισή του. Επομένως η μυστικότητα του κωδικού πρόσβασης ή του κλειδιού είναι υψίστης σημασίας στην προκειμένη περίπτωση. Το κλειδί θα πρέπει να αποθηκεύεται με ασφάλεια ή να το θυμάται ο χρήστης και να το χρησιμοποιεί κατά τη διάρκεια της επαλήθευσης ταυτότητας. Οι πρόσθετες αυτές πληροφορίες που χρησιμοποιούνται κατά την επαλήθευση ταυτότητας με τη μορφή του κλειδιού, αυξάνουν την εντροπία* του βιομετρικού προτύπου και έτσι ένας χάκερ είναι πιο δύσκολο να αποκτήσει πρόσβαση γιατί θα πρέπει να μαντέψει το πρότυπο.

Πλεονεκτήματα:

- Με τη χρήση του κλειδιού έχουν μειωθεί τα ποσοστά σφαλμάτων false accept, πράγμα το οποίο σημαίνει ότι το σύστημα δεν δέχεται χρήστες οι οποίοι δεν είναι εγγεγραμμένοι στο σύστημα.
- Επειδή κάθε χρήστης έχει ένα δικό του χαρακτηριστικό κλειδί, τα διαφορετικά πρότυπα που ανήκουν στον ίδιο χρήστη μπορούν να έχουν και ξεχωριστό κλειδί. Με τον τρόπο αυτό επιτρέπεται η διαφορετικότητα ανάμεσα στα πρότυπα. Έτσι, σε περίπτωση που ένα πρότυπο από αυτά βρίσκεται σε κίνδυνο δεν κινδυνεύουν και τα υπόλοιπα. Επίσης είναι εύκολο το πρότυπο που βρίσκεται σε κίνδυνο να ανακληθεί και να αντικατασταθεί με ένα καινούριο αλλάζοντας απλώς το κλειδί ή τον κωδικό πρόσβασης.

Μειονεκτήματα:

- Εάν το προσωπικό κλειδί ή ο προσωπικός κωδικός πρόσβασης ενός χρήστη παραβιαστεί τότε ο εισβολέας/χάκερ είναι πολύ πιθανό να ανακτήσει το αρχικό βιομετρικό πρότυπο.
- Από τη στιγμή που η σύγκριση για την επαλήθευση της ταυτότητας πραγματοποιείται σε μετασχηματισμένο πεδίο, ο μηχανισμός salting θα πρέπει να σχεδιαστεί με τέτοιο τρόπο έτσι ώστε η απόδοση αναγνώρισης να μην υποβαθμίζεται.

Σημ.: ***Εντροπία:** Ένα μέτρο, που ορίζει τον αριθμό των διαφορετικών ταυτοτήτων που διακρίνονται από ένα βιομετρικό σύστημα.

5.2.2 Noninvertible transform

Σε μια τέτοιου είδους προσέγγιση εφαρμόζεται στο πρότυπο μια μονόδρομη συνάρτηση η οποία είναι υπολογιστικά δύσκολο να αντιστρέψει ένα μετασχηματισμένο πρότυπο ακόμα κι αν το κλειδί είναι γνωστό. Δίνοντας δηλαδή μια παράμετρο στη συνάρτηση είναι εύκολο να παραχθεί το αποτέλεσμά της αλλά αν αντιστρέψουμε τη συνάρτηση είναι δύσκολο να πάρουμε την ίδια παράμετρο. Η παράμετρος αυτή ή οι παράμετροι της συνάρτησης μετασχηματισμού ορίζονται από ένα κλειδί το οποίο θα πρέπει να υποβάλει ο χρήστης κατά τη διαδικασία επαλήθευσης ταυτότητας για να μετασχηματίσει το βιομετρικό χαρακτηριστικό που επίσης υποβάλλει εκείνη τη στιγμή. Κύριο χαρακτηριστικό της προσέγγισης αυτής είναι ότι ακόμα κι αν το κλειδί ή το

μετασχηματισμένο πρότυπο είναι γνωστό από κάποιο χάκερ είναι πολύ δύσκολο να αποκτήσει το αρχικό βιομετρικό πρότυπο.
Πλεονεκτήματα:

- Το γεγονός ότι ακόμα κι αν ο χάκερ γνωρίζει το κλειδί είναι δύσκολο να ανακτήσει το αρχικό βιομετρικό πρότυπο, καθιστά την προσέγγιση αυτή ασφαλέστερη σε σύγκριση με την salting προσέγγιση.
- Χρησιμοποιώντας συγκεκριμένες εφαρμογές και συγκεκριμένες συναρτήσεις μετασχηματισμού για κάθε χρήστη είναι δυνατό να επιτευχθεί αντίστοιχα η διαφορετικότητα και η δυνατότητα ανάκλησης των προτύπων.

Μειονεκτήματα:

- Το βασικό μειονέκτημα εδώ είναι ότι η συνάρτηση της προσέγγισης αυτής θα πρέπει να χαρακτηρίζεται τόσο για τη διάκριση μεταξύ των προτύπων, όσο και για τη μη αντιστρεψιμότητά τους και είναι δύσκολο να σχεδιαστεί μια τέτοια συνάρτηση. Χαρακτηριστικά του ιδίου χρήστη θα πρέπει να έχουν υψηλή ομοιότητα πριν και μετά το μετασχηματισμό, ενώ αντίθετα χαρακτηριστικά διαφορετικών χρηστών του συστήματος θα πρέπει να διαφέρουν κατά πολύ μετά το μετασχηματισμό. Επίσης ο μετασχηματισμός θα πρέπει να είναι μη αντιστρέψιμος για να είναι δύσκολο να ανακτήσει κάποιος τρίτος το αρχικό πρότυπο.

5.2.3 Key-binding biometric cryptosystem

Εδώ η ασφάλεια του βιομετρικού προτύπου προέρχεται από μία αποκλειστική σύνδεσή του με ένα κλειδί κρυπτογράφησης. Χρησιμοποιούνται και εδώ βοηθητικά δεδομένα σε μορφή μιας οντότητας (π.χ. token) στην οποία ενσωματώνονται το κλειδί κρυπτογράφησης αλλά και το πρότυπο που είναι αποθηκευμένο στη βάση δεδομένων του συστήματος. Τα βοηθητικά αυτά δεδομένα δεν αποκαλύπτουν σημαντικές πληροφορίες για το πρότυπο ή το κλειδί κρυπτογράφησης, αλλά αποτελούν ένα σύνδεσμο με τον κώδικα διόρθωσης σφαλμάτων για το βιομετρικό πρότυπο. Κατά την επαλήθευση ταυτότητας, όταν το χαρακτηριστικό που δίνει ο χρήστης διαφέρει από το αρχικό πρότυπο σε ανεκτικά όρια, υπάρχει μια κωδική λέξη που σχετίζεται με το αντίστοιχο ποσοστό σφάλματος η οποία ανακτάται, αποκωδικοποιείται και χρησιμοποιείται για την απόκτηση του κλειδιού και έτσι μπορεί να πραγματοποιηθεί ξανά η σύγκριση για την ταυτοποίηση.
Πλεονεκτήματα:

- Βασικό πλεονέκτημα της προσέγγισης αυτής είναι ότι ανέχεται, ως ένα βαθμό, λάθη σε δεδομένα που δίνουν γνήσιοι χρήστες κατά την επαλήθευσή τους. Η ανοχή αυτή προσδιορίζεται από τη δυνατότητα διόρθωσης σφαλμάτων με μια συσχετιζόμενη λέξη κλειδί.

Μειονεκτήματα:

- Η σύγκριση προτύπου-χαρακτηριστικού πρέπει να γίνεται πάντα χρησιμοποιώντας τη διόρθωση λαθών που τυχόν προκύπτουν. Έτσι αποκλείονται καινούριοι και εξελιγμένοι προσαρμογείς και είναι πιθανό να μειωθεί η ακρίβεια στη σύγκριση.
- Αν και τα βιομετρικά κρυπτοσυστήματα δεν έχουν σχεδιαστεί για να προσφέρουν διαφορετικότητα στα πρότυπα και δυνατότητες ανάκλησης, γίνονται προσπάθειες να παρέχονται και οι δυο αυτές ιδιότητες χρησιμοποιώντας τη συγκεκριμένη προσέγγιση σε συνδυασμό με κάποια άλλη.

- Τα βοηθητικά δεδομένα θα πρέπει να έχουν δημιουργηθεί λαμβάνοντας υπόψη τιςιδιαιτερότητες των βιομετρικών χαρακτηριστικών και τις φυσικές παραλλαγές που μπορεί να πάρει το χαρακτηριστικό αυτό.

5.2.4 Key generating biometric generation

Μια ενδιαφέρουσα προσέγγιση βιομετρικού προτύπου ασφάλειας είναι αυτή όπου από τα βιομετρικά χαρακτηριστικά δημιουργείται απευθείας ένα κλειδί κρυπτογράφησης, αλλά η εφαρμογή της είναι δύσκολη λόγω της μεταβλητότητας των γνήσιων χρηστών. Σύμφωνα με το άρθρο Biometric Template Security τα πρώτα συστήματα με αυτή την προσέγγιση χρησιμοποιήθηκαν σε ειδικευμένα για κάθε χρήστη σχήματα κβαντοποίησης όπου σε κάποιο token αποθηκεύονταν πληροφορίες σχετικές με τα όρια ποσοτικοποίησης, ως βοηθητικά δεδομένα και το χρησιμοποιούσαν οι χρήστες κατά την επαλήθευση ταυτότητας. Αργότερα σύμφωνα με το άρθρο Biometric Template Security (p. 10), ο Dodis εισήγαγε την έννοια του ασφαλούς σκίτσου και του ασαφή εξαγωγέα (secure sketch an fuzzy extractor), πληροφορίες που προέρχονται από βιομετρικά στοιχεία. Όσον αφορά το ασφαλές σκίτσο, πρόκειται για βοηθητικά δεδομένα τα οποία παρέχουν πληροφορίες σχετικές με το πρότυπο , διευκολύνει την ακριβή ανακατασκευή του προτύπου όταν ο χρήστης δώσει το χαρακτηριστικό που του ζητηθεί κατά την επαλήθευση ταυτότητας. Από την άλλη πλευρά, ο ασαφές εξαγωγέας είναι ένα κρυπτογραφικό σύστημα το οποίο δημιουργεί ένα κρυπτογραφικό κλειδί από τα βιομετρικά χαρακτηριστικά. Η σταθερότητα του κλειδιού και η τιμή της εντροπίας του κλειδιού δεν ευνοούν για τη διάκριση μεταξύ των προτύπων. Η σταθερότητα του κλειδιού αναφέρεται στο αν το κλειδί θα είναι επαναλήψιμο ή όχι, ενώ η τιμή της εντροπίας σχετίζεται με τον αριθμό των κλειδιών που δημιουργούνται. Για παράδειγμα αν ένα σύστημα παράγει το ίδιο κλειδί για πολλά πρότυπα, τότε έχει μεγάλη σταθερότητα αλλά μηδενική εντροπία. Αντίθετα, αν το σύστημα παράγει διαφορετικά κλειδιά για διαφορετικά πρότυπα ενός χρήστη τότε έχει υψηλή εντροπία και μηδενική σταθερότητα. Και οι δυο περιπτώσεις οδηγούν σε σφάλματα false accept και false reject αντίστοιχα, γι' αυτό και γίνονται προσπάθειες για την επίτευξη και των δυο μέτρων ταυτόχρονα.
Πλεονεκτήματα:

- Η προσέγγιση αυτή μπορεί να φανεί πολύ χρήσιμη και για κρυπτογραφικές εφαρμογές.

Μειονεκτήματα:

- Το κλειδί που δημιουργείται είναι δύσκολο να διαθέτει υψηλή σταθερότητα και υψηλή εντροπία ταυτόχρονα.

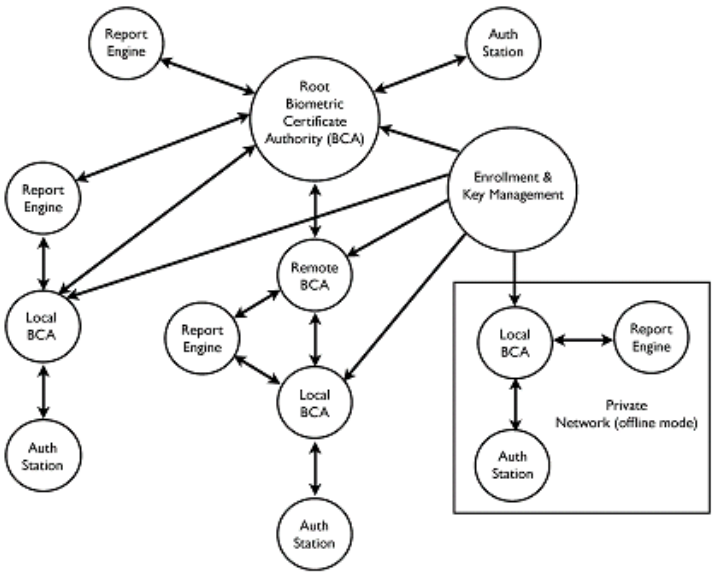
5.3 Ανάκληση βιομετρικής υπογραφής

Ένα από τα πρώτα ερωτήματα που γεννιέται στο μυαλό των ανθρώπων όταν διαβάζουν για την ανάκληση μιας βιομετρικής υπογραφής είναι "Τι είναι η ανάκληση" "Γιατί να ανακαλέσουμε ένα βιομετρικό πρότυπο" και "Πώς γίνεται η ανάκληση ενός προτύπου". Έχοντας αναφέρει πιο πάνω τις ευαισθησίες ενός βιομετρικού συστήματος μπορεί να παρατηρήσει κανείς ότι η πρόσβαση ενός ξένου χρήστη στο σύστημα δεν είναι ακατόρθωτη. Αντιθέτως μάλιστα, με το πέρας του χρόνου γίνεται όλο και πιο εύκολο, καθώς οι χάκερ ψάχνουν συνέχεια να βρούνε τρόπους για να το παραβιάσουν. Η ανάγκη των ανθρώπων να προστατευτούν τα προσωπικά δεδομένα τόσων χρηστών οδήγησε στη δημιουργία της ανάκλησης της βιομετρικής υπογραφής. Όταν κάποιος

χρήστης ανακαλύψει ότι κάποιος άλλος χειρίζεται το λογαριασμό του στο σύστημα, τότε του δίνεται η δυνατότητα να αλλάξει τη βιομετρική του ταυτότητα. Υπό άλλες συνθήκες θα ήταν απαραίτητο να πραγματοποιήσει ξανά τη διαδικασία εγγραφής του στο σύστημα έτσι ώστε να δημιουργηθεί από την αρχή το αρχικό βιομετρικό του πρότυπο και τα νέα βιομετρικά χαρακτηριστικά που το απαρτίζουν. Με την ανάκληση του προτύπου όμως αυτό δεν είναι απαραίτητο. Εάν ο χρήστης δεν επιθυμεί την επανεγγραφή του στο σύστημα, τότε τα βιομετρικά χαρακτηριστικά που απαρτίζουν το τρέχον πρότυπο, διαγράφονται και δημιουργούνται νέα με βάση το αρχικό βιομετρικό πρότυπο που κατέγραψε το σύστημα κατά την εγγραφή του χρήστη. Αναλυτικά η διαδικασία ανάκλησης μιας βιομετρικής υπογραφής θα παρουσιαστεί παρακάτω.

5.3.1 Biocryptographic Key Infrastructure

Η περιγραφή της ανάκλησης βιομετρικής υπογραφής που θα περιγραφεί παρακάτω, σύμφωνα με τους W.J. Scheirer, W. Bishop and T.E. Boult [2010], σχετίζεται με το Biocryptographic Key Infrastructure. Πρόκειται για μια υποδομή η οποία πιστοποιεί τα βιομετρικά χαρακτηριστικά ενός χρήστη. Απαρτίζεται από πολλές οντότητες, απαραίτητες για τη δημιουργία ενός βιομετρικού πιστοποιητικού (BCAs – Biometric Certificate Authorities). Τα πιστοποιητικό αυτό υποστηρίζει το δημόσιο κλειδί που χρησιμοποιείται αλλά και το ανακληθέν βιομετρικό πρότυπο. Στην υποδομή αυτή υπάρχει μια κεντρική ρίζα η οποία εγκρίνει όλα τα πιστοποιητικά, την εγγραφή, τη διαχείριση των κλειδιών και ότι σχετίζεται με αυτά. Υπάρχουν Auth Stations όπως ονομάζονται, και είναι συσκευές στις οποίες οι χρήστες υποβάλλουν τα βιομετρικά δείγματα για τη δημιουργία των προτύπων, report engines, μηχανές οι οποίες χρησιμοποιούνται για να γίνει γνωστή μια εγγραφή και γενικά για να διαδοθούν αναφορές σχετικές με εγγραφές και συναλλαγές. Το πιστοποιητικό του Biocryptographic Key Infrastructure είναι στη ουσία το πιστοποιητικό x.509 v3 που χρησιμοποιείται για την επικοινωνία ατόμων στο διαδίκτυο με τη χρήση δημόσιου κλειδιού (PKI – Public Key Infrastructure), προσθέτοντας κάποια επιπλέον πεδία.



Εικόνα 5.6 Απεικόνιση της υποδομής BKI.

Όταν ένας χρήστης επιθυμεί να αποκτήσει ένα νέο πιστοποιητικό τότε στέλνει ένα μήνυμα CSR – Certificate Signing Request στη ρίζα της υποδομής για να πάρει την έγκριση. Εάν πάρει την έγκριση τότε στο πιστοποιητικό προστίθενται κάποια επιπλέον πεδία τα οποία παρέχουν πληροφορίες σχετικές με την εγγραφή. Η αίτηση αυτή φτάνει μέχρι τη ρίζα της υποδομής, περνώντας από όλους τους ενδιάμεσους σταθμούς. Με τη χρήση του κλειδιού της ρίζας της υποδομής ελέγχεται αν ο χρήστης είναι αυτός που ισχυρίζεται, η όχι, και αντίστοιχα επισημαίνεται, ή όχι, ως κακόβουλος χρήστης.

5.3.2 Ανάκληση και επανέκδοση

Το μοντέλο ανάκλησης που θα αναλύσουμε σήμερα σχετίζεται με το BKI πρωτόκολλο. Για να πραγματοποιηθεί μια επανέκδοση δεν αρκεί μόνο να ανακληθεί ένα πιστοποιητικό, να δημιουργηθεί ένα νέο κλειδί και να επανεκδοθεί το πρότυπο, θα πρέπει επίσης να πραγματοποιηθεί και η επανέκδοση των βιομετρικών χαρακτηριστικών. Σε πολλά συστήματα η ανάκληση περιγράφεται ως μια ιδιότητα σε ένα πρότυπο, εδώ όμως θα δούμε περιγραφικά τη διαδικασία. Παρακάτω θα περιγραφούν τρία σενάρια ανάκλησης για το πρωτόκολλο BKI.

Certificate Signing Request

Common Name
Organization
Organizational Unit
City/Locality
State/County/Region
Country
Email Address
Signing Representative
Signing Representative's Email Address
Public Key
Biotoken Type
Enrollment Biotoken
Keyring* for Biotoken (optional)
Re-issue Flag

Εικόνα 5.7 Απεικόνιση του μηνύματος CSR.

Certificate Re-issue Notification

Serial Number
New Serial Number
Biotoken Re-issued Flag
Key-pair Re-issued Flag
Biotoken and Key-pair Revoked Flag
*Keyring for Biotoken (Optional)
Biotoken Type (Optional)
Biotoken (Optional)
Signature

Εικόνα 5.8 Απεικόνιση του μηνύματος CRN.

1. Χειροκίνητη επανέκδοση

Όπως αναφέρθηκε και παραπάνω μια μονάδα BCA (Biometric Certificate Authority) εκδίδει πιστοποιητικά, και είναι απαραίτητο να διαθέτει μια λίστα ανάκλησης πιστοποιητικών για να μπορεί να γνωρίζει ποια πιστοποιητικά έχουν εκδοθεί ή πρόκειται να εκδοθούν. Η λίστα αυτή Certificate Revocation List – CRL, όπως ονομάζεται περιέχει μόνο όσα πιστοποιητικά έχουν ανακληθεί καθώς και πιστοποιητικά τα οποία δεν έχουν λήξει ακόμη. Εάν έχει παραβιαστεί κάποιο κλειδί ή κάποιο βιομετρικό χαρακτηριστικό τότε το πιστοποιητικό αυτό μπορεί να ανακληθεί. Σ'

αυτό το σενάριο η μονάδα BCA δεν έχει κρατήσει πληροφορίες που χρειάζονται για την ανάκληση ενός πιστοποιητικού.

Για να ξεκινήσει η διαδικασία ανάκλησης, η μονάδα BCA στέλνει το συγκεκριμένο πιστοποιητικό στη λίστα ανάκλησης πιστοποιητικών CRL, και ειδοποιεί τον χρήστη για την έναρξη της διαδικασίας με ένα μήνυμα CRN (Certificate Re-issue Notification)μέσω των πληροφοριών επικοινωνίας που παρέχονται από το CSR (Certificate Signing Request). Εάν ο χρήστης επιτρέπει την επανέκδοση, τότε μια μονάδα Auth Station δημιουργεί ένα ζευγάρι κλειδιών (δημόσιο και ιδιωτικό) και ένα νέο πρότυπο. Όλες αυτές οι πληροφορίες στέλνονται πίσω στη μονάδα BCA με τη μορφή μιας νέας αίτησης CSR για εγγραφή. Αν η αίτηση αυτή γίνει δεκτή, πραγματοποιείται η επανεγγραφή του χρήστη και ένα νέο πιστοποιητικό εκδίδεται.

Η επανέκδοση ενός πιστοποιητικού μπορεί να πραγματοποιηθεί και χωρίς την εγγραφή του χρήστη από την αρχή, αρκεί στη μονάδα BCA να έχει αποθηκευτεί το αρχικό βιομετρικό πρότυπο χωρίς να υποστεί κάποιο μετασχηματισμό. Για να ξεκινήσει η διαδικασία αυτή, η μονάδα BCA στέλνει το ανάλογο πιστοποιητικό στη λίστα ανάκλησης πιστοποιητικών CRL και ειδοποιεί το χρήστη με ένα μήνυμα CRN. Το συγκεκριμένο CRN μήνυμα περιλαμβάνει το αρχικό βιομετρικό πρότυπο του ιδιοκτήτη. Ο χρήστης θα δημιουργήσει ένα νέο ζεύγος κλειδιών, τα οποία θα χρησιμοποιηθούν για να δημιουργηθεί το νέο κωδικοποιημένο βιομετρικό πρότυπο. Τέλος, το νέο κωδικοποιημένο βιομετρικό πρότυπο και προαιρετικά ένα νέο δημόσιο κλειδί αποστέλλονται πίσω στη μονάδα BCA με τη μορφή μιας νέας αίτησης εγγραφής CSR.

Αν έχει παραβιαστεί το δημόσιο κλειδί ή το βιομετρικό πρότυπο ή το κλειδί της μονάδας BCA τότε είναι απαραίτητο να πραγματοποιηθεί ανάκληση με την επανεγγραφή του χρήστη διότι τα δεδομένα που είναι αποθηκευμένα δεν μπορούν να χαρακτηριστούν αξιόπιστα. Ανάκληση χωρίς επανεγγραφή του χρήστη μπορεί να χρησιμοποιείται όταν η τακτική του χρήστη είναι να αλλάζει συνεχώς το πρότυπο για την ασφαλή χρήση του.

2. Αυτόματη επανέκδοση προτύπου

Όταν μια μονάδα BCA ανακαλύπτει ότι ένα πρότυπο έχει παραβιαστεί θα ήταν σκόπιμο να μπορεί να ανακαλέσει το πρότυπο με κάποιο αυτοματοποιημένο τρόπο. Για να πραγματοποιηθεί αυτό, η μονάδα BCA θα πρέπει να διαθέτει κλειδιά ώστε να μπορεί να αντιστρέφει τις πληροφορίες που υπάρχουν σε ένα token και να δημιουργεί ένα νέο πρότυπο βασιζόμενο στις πληροφορίες του. Οι αποθηκευμένες πληροφορίες δεν είναι ανάγκη να είναι τα αρχικά βιομετρικά χαρακτηριστικά. Το κατάλληλο κλειδί για να αντιστραφούν οι πληροφορίες ανήκει στη ρίζα, επομένως μόνο η μονάδα BCA που αποτελεί τη ρίζα της υποδομής μπορεί να αντιστρέψει τις πληροφορίες, οι υπόλοιπες μονάδες BCA δεν μπορούν.

Στην περίπτωση αυτοματοποιημένης ανάκλησης, στην διαδικασία εγγραφής το μήνυμα CSR περιλαμβάνει ακόμη ένα πεδίο το οποίο περιλαμβάνει όλα τα απαραίτητα κλειδιά, κωδικούς ή αναγνωριστικά που θα χρειαστούν για να κωδικοποιηθεί το αρχικό βιομετρικό πρότυπο, κατά τη διάρκεια του μετασχηματισμού. Το πεδίο αυτό, του μηνύματος CSR, θα κωδικοποιηθεί με το κλειδί της μονάδας BCA, και θα αποθηκευτεί στη μονάδα BCA, για μελλοντική χρήση σε περίπτωση που κριθεί αναγκαία η ανάκληση του προτύπου. Η αυτόματη διαδικασία ανάκλησης ξεκινά με τη μονάδα BCA να στέλνει το αντίστοιχο πιστοποιητικό στην λίστα ανάκλησης πιστοποιητικών CRL, και να ειδοποιεί τον χρήστη για την έναρξη της διαδικασίας. Αν ο κάτοχος επιτρέπει την επανέκδοση, τότε η μονάδα BCA αναλαμβάνει να αντιστρέψει το πρότυπο που βρίσκεται ένα επίπεδο πιο πίσω, να δημιουργήσει ένα νέο σύνολο πληροφοριών μετασχηματισμού και να κωδικοποιήσει ξανά το πρότυπο. Έτσι δημιουργείται ένα νέο πιστοποιητικό με βάση το νέο πρότυπο και το αρχικό δημόσιο κλειδί. Η μονάδα BCA στέλνει στο χρήστη ένα CRN μήνυμα που

δείχνει τον αύξοντα αριθμό του πιστοποιητικού που ανακλήθηκε, τον αύξοντα αριθμό του νέου πιστοποιητικού που δημιουργήθηκε και το πεδίο με τα απαραίτητα κλειδιά για το νέο βιομετρικό πρότυπο. Το μήνυμα αυτό υπογράφεται από τη μονάδα BCA, πράγμα το οποίο σημαίνει πως το νέο πιστοποιητικό είναι πλέον έγκυρο.

3. Αυτόματη επανέκδοση ζεύγους κλειδιών

Με το ίδιο σκεπτικό όπως και στο προηγούμενο σενάριο, θα ήταν σκόπιμο να πραγματοποιείται αυτόματη επανέκδοση ενός πιστοποιητικού όταν ένα ζεύγος κλειδιών βρίσκεται σε κίνδυνο. Για να μπορέσει να πραγματοποιηθεί κάτι τέτοιο, η μονάδα BCA πρέπει να δημιουργήσει ένα διμερές πρότυπο και να το στείλει στον χρήστη. Το διμερές αυτό πρότυπο αποτελείται από δυο μέρη, το αρχικό βιομετρικό πρότυπο του χρήστη που είναι αποθηκευμένο στο πιστοποιητικό του και ένα μυστικό που θέλει να μεταφέρει στο χρήστη. Η διαδικασία ανάκλησης ξεκινά με την μονάδα BCA να στέλνει το αντίστοιχο πιστοποιητικό στη λίστα ανάκλησης πιστοποιητικών CRL και να ειδοποιεί τον κάτοχο του πιστοποιητικού για την έναρξη της διαδικασίας. Αν ο κάτοχος επιτρέπει την επανέκδοση, η μονάδα BCA αναλαμβάνει να δημιουργήσει ένα νέο ζεύγος κλειδιών (δημόσιο-ιδιωτικό). Έτσι, με το νέο δημόσιο κλειδί και το αρχικό βιομετρικό πρότυπο δημιουργείται το καινούριο πρότυπο. Η μονάδα BCA δημιουργεί ένα διμερές πρότυπο που αποτελείται από το ιδιωτικό κλειδί και το αρχικό βιομετρικό πρότυπο. Στη συνέχεια στέλνει στον χρήστη ένα CRN μήνυμα με το οποίο του γνωστοποιεί τον αύξοντα αριθμό του ανακληθέντος πιστοποιητικού, τον αύξοντα αριθμό του νέου πιστοποιητικού και το διμερές πρότυπο το οποίο περιέχει και το ιδιωτικό κλειδί. Το μήνυμα αυτό υπογράφεται από τη μονάδα BCA, πράγμα το οποίο σημαίνει πως το νέο πιστοποιητικό είναι πλέον έγκυρο.

Στη διαδικασία αυτόματης επανέκδοσης θα χρειαστεί να παρέμβει ο χρήστης και να υποβάλλει σε μια μονάδα Auth Station τα βιομετρικά του χαρακτηριστικά προκειμένου να απελευθερώσει το νέο ιδιωτικό κλειδί από το διμερές πρότυπο στο CRN.

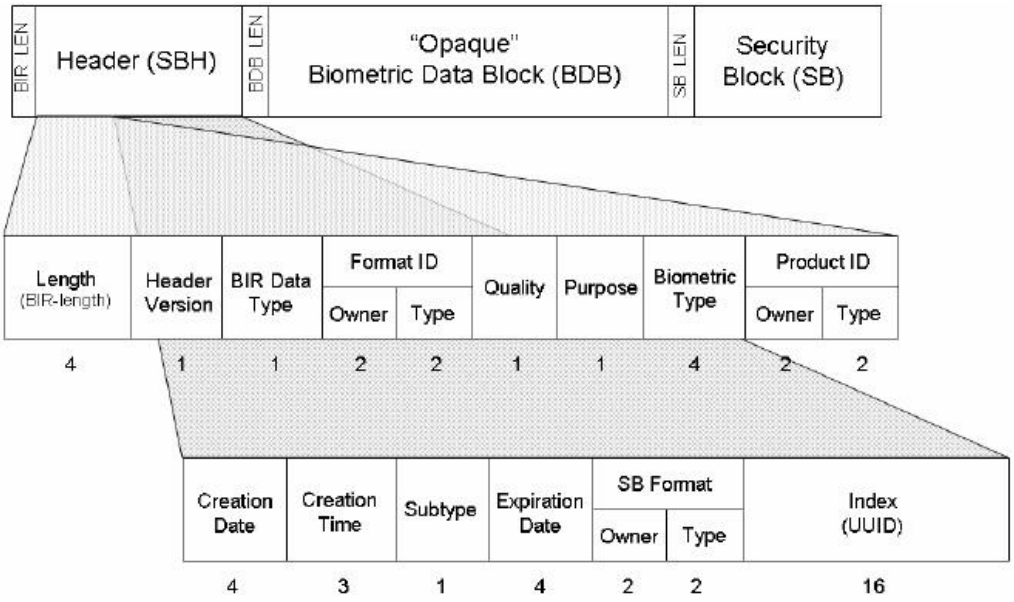
Κεφάλαιο 6ο Μελέτη περίπτωσης

Έχοντας μελετήσει όλα τα παραπάνω καταλήξαμε στο συμπέρασμα πως η καρδιά μιας βιομετρικής υπογραφής είναι η εγγραφή ενός ή πολλών χαρακτηριστικών στη βάση δεδομένων. Στο κεφάλαιο αυτό αρχικά θα αναλυθεί εκτενέστερα η βιομετρική εγγραφή αναγνώρισης, αναλύοντας το περιεχόμενο και τη λειτουργία όλων των πεδίων που διαθέτει καθώς επίσης και τύπους και συναρτήσεις που εμπεριέχονται σε ένα αρχείο bioAPI. Στη συνέχεια θα δοθεί ένα παράδειγμα μιας πολύτροπης βιομετρικής υπογραφής. Μια υπογραφή, δηλαδή, η οποία θα περιλαμβάνει πληροφορίες για περισσότερα από ένα χαρακτηριστικά του ανθρώπινου σώματος.

6.1 Ανάλυση της βιομετρικής εγγραφής αναγνώρισης (BIR)

Πρόκειται για μια δομή δεδομένων, η οποία διασχίζει τα interfaces API και SPI, και αποθηκεύεται στη μνήμη χρησιμοποιώντας δείκτες σε διάφορα στοιχεία. Αυτή η δομή δεδομένων, η βιομετρική εγγραφή αναγνώρισης όπως ονομάζεται ή κωδικός BIR, δημιουργείται από τον Biometric Service Provider (BSP) και, όπως αναφέρθηκε και στο 4^{ο} κεφάλαιο, απαρτίζεται από 3 βασικά πεδία, τα Standard Biometric Header (SBH), Biometric Data Block (BDB) και Signature Block ή Security Block (SB). Κάθε φορά που δημιουργείται ένας κωδικός BIR από τον BSP, επιστρέφεται μια "λαβή" (handle) και με βάση αυτή μπορεί ο κωδικός BIR να αποθηκευτεί σε μια βάση δεδομένων ή να αποσταλεί σε κάποιο server για ταυτοποίηση ή επαλήθευση. Οι περισσότερες τοπικές λειτουργίες μπορούν να εκτελεστούν χωρίς να μετακινηθεί ο κωδικός BIR από τον BSP. Ωστόσο όμως, αν κάποια εφαρμογή χρειάζεται τον κωδικό αυτό ως είσοδο σε κάποια συνάρτηση, τότε μπορεί να τον χρησιμοποιήσει με έναν από τους παρακάτω τρεις τρόπους:

- με αναφορά στη "λαβή" (handle) του BIR
- με αναφορά στο πρωτεύον κλειδί μιας βάσης δεδομένων όπου είναι αποθηκευμένος
- με τη χρήση του ίδιου του κωδικού BIR.



Εικόνα 6.1 Αναλυτική αναπαράσταση κωδικού BIR

6.1.1 Standard Biometric Header

Σύμφωνα με το ISO/IEC 19784-1 [2006] το πεδίο Standard Biometric Header απαρτίζεται από επιμέρους πεδία όπως φαίνονται στην εικόνα 6.1. τα οποία και θα αναλυθούν παρακάτω. Η μορφή των πεδίων αυτών έχει καθοριστεί με βάση το Common Biometric Exchange Format (CBEEF).

- **BioAPI_BIR_LENGTH**
  Στο πεδίο αυτό αποθηκεύεται το συνολικό μήκος της βιομετρικής υπογραφής το οποίο περιλαμβάνει την επικεφαλίδα (HEADER) και το βιομετρικό μπλοκ δεδομένων (Opaque BDB).

- **BioAPI_BIR_HEADER_VERSION**
  Στο πεδίο αυτό αναγράφεται η έκδοση της επικεφαλίδας.

```
typedef  uint8  BioAPI_BIR_VERSION, *BioAPI_BIR_VERSION_PTR;
```

- **BioAPI_BIR_DATA_TYPE**
  Το πεδίο αυτό χρησιμοποιείται για τρεις διαφορετικούς σκοπούς. Προσδιορίζει τον τύπο του βιομετρικού δείγματος, αν δηλαδή τα δεδομένα είναι επεξεργασμένα, μερικώς επεξεργασμένα ή καθόλου επεξεργασμένα (flag: raw, intermediate or processed). Σε κάποιες περιπτώσεις οι κωδικοί BIR δεν δημιουργούνται από τον BSP αλλά προκύπτουν από άλλες μορφές δεδομένων και συνήθως τότε δεν ορίζεται κάποια σημαία για το πεδίο αυτό. Αν δεν έχει οριστεί ή έχουν οριστεί παραπάνω από μια σημαίες και περάσει ο κωδικός BIR στο BioAPI Framework τότε θα προκληθεί σίγουρα σφάλμα. Η δεύτερη χρησιμότητα του πεδίου αυτού είναι να προσδιορίζει αν ο κωδικός BIR είναι κρυπτογραφημένος, υπογεγραμμένος ή όχι (flag: encrypted or signed). Σ΄αυτή την περίπτωση αν υπάρχει μια από τις δύο, και οι δύο ή καμία σημαία, τότε ισχύουν και οι αντίστοιχες ιδιότητες για τον κωδικό BIR. Τέλος στο πεδίο αυτό μπορεί να οριστεί αν στο τμήμα της επικεφαλίδας BIR περιλαμβάνεται κάποια τιμή δείκτη.

```
typedef uint8_t BioAPI_BIR_DATA_TYPE;

    #define BioAPI_BIR_DATA_TYPE_RAW              (0x01)
    #define BioAPI_BIR_DATA_TYPE_INTERMEDIATE     (0x02)
    #define BioAPI_BIR_DATA_TYPE_PROCESSED        (0x04)
    #define BioAPI_BIR_DATA_TYPE_ENCRYPTED        (0x10)
    #define BioAPI_BIR_DATA_TYPE_SIGNED           (0x20)
    #defineBioAPI_BIR_INDEX_PRESENT               (0x80)
```

- **BioAPI_BIR_FORMAT_ID**
  Το πεδίο αυτό περιλαμβάνει πληροφορίες οι οποίες προσδιορίζουν το περιεχόμενο του πεδίου Opaque Biometric Data Block. Πληροφορίες όπως ο ιδιοκτήτης του συγκεκριμένου βιομετρικού χαρακτηριστικού και πληροφορίες σχετικές με τον τύπο του συγκεκριμένου βιομετρικού χαρακτηριστικού, όπως για παράδειγμα μικρολεπτομέρειες ενός δακτυλικού αποτυπώματος.

```
typedef struct bioapi_bir_biometric_data_format {
    uint16_t FormatOwner;
    uint16_t FormatType;
} BioAPI_BIR_BIOMETRIC_DATA_FORMAT;
```

- **BioAPI_BIR_QUALITY**
  Το πεδίο αυτό προσδιορίζει την ποιότητα των δεδομένων καθώς επίσης και σε εξειδικευμένες περιπτώσεις το αν η παράμετρος αυτή δεν έχει οριστεί ή αν δεν υποστηρίζεται καθόλου από τον BSP. Η ποιότητα των δεδομένων εξαρτάται και από το σκοπό για τον οποίο πρόκειται να χρησιμοποιηθούν. (π.χ. για εγγραφή στο σύστημα,

αναγνώριση κλπ.) Ο σκοπός ύπαρξης αυτής της παραμέτρου είναι ότι ο BSP θα πρέπει να ενημερώνει την εφαρμογή για την κατάσταση των δεδομένων καθώς επίσης και για το αν οι τρέχουσες παρατηρήσεις είναι καλύτερες από τις προηγούμενες ή όχι. Το εύρος της τιμής που μπορεί να πάρει το πεδίο αυτό είναι μεταξύ 0-100.

Πίνακας 2: Πίνακας εύρους τιμών ποιότητας δεδομένων

Εύρος τιμών	Ονομασία	Επεξήγηση
-2	-	Η παράμετρος δεν υποστηρίζεται από τον BSP.
-1	-	Η παράμετρος δεν έχει οριστεί από τον BSP.
0-25	UNACCEPTABLE	Η ποιότητα των βιομετρικών δεδομένων δεν αρκεί για να πραγματοποιηθεί ο αντίστοιχος στόχος και θα πρέπει να αντικατασταθούν.
2-50	MARGINAL	Η ποιότητα των βιομετρικών δεδομένων είναι φτωχή και οριακή για το στόχο που έχει καθορίσει η εφαρμογή. Επομένως θα πρέπει να αντικατασταθούν.
51-75	ADEQUATE	Η ποιότητα των δεδομένων είναι αρκετά ικανοποιητική για τις περισσότερες εφαρμογές σύμφωνα με τον στόχο που έχει καθοριστεί. Σε περίπτωση όμως που ο σχεδιαστής έχει θέσει μεγαλύτερες απαιτήσεις θα γίνει προσπάθεια να επιτευχθεί καλύτερη ποιότητα.
76-100	EXCELLENT	Η ποιότητα των δεδομένων είναι σε άριστη κατάσταση και ικανοποιεί πλήρως τον στόχο που έχει καθοριστεί.

- **BioAPI_BIR_PURPOSE**

  Το πεδίο αυτό παίρνει μια τιμή η οποία καθορίζει το σκοπό για τον οποίο προορίζεται ο κωδικός BIR όταν χρησιμοποιείται σαν είσοδος σε κάποια συνάρτηση ή αν είναι κατάλληλο όταν χρησιμοποιείται σαν έξοδος από μια συνάρτηση ή βρίσκεται σε μια κεφαλίδα BIR. Όταν χρησιμοποιείται σαν είσοδος σε μια συνάρτηση ο BSP θα πρέπει να γνωρίζει τον σκοπό για να εκτελέσει την κατάλληλη λήψη ή/και επεξεργασία των δεδομένων. Μπορεί για παράδειγμα να χρησιμοποιηθεί για πιστοποίηση, ταυτοποίηση, εγγραφή κλπ. Αν πρόκειται να χρησιμοποιηθεί για την κεφαλίδα ενός BIR κωδικού, τότε θα πρέπει να έχει οριστεί ο σκοπός και η κεφαλίδα να δείξει στην εφαρμογή για ποιο σκοπό προορίζεται, πιστοποίηση ή επαλήθευση.

```
typedef uint8_t BioAPI_BIR_PURPOSE;

    #define BioAPI_PURPOSE_VERIFY                              (1)
    #define BioAPI_PURPOSE_IDENTIFY                            (2)
    #define BioAPI_PURPOSE_ENROLL                              (3)
    #define BioAPI_PURPOSE_ENROLL_FOR_VERIFICATION_ONLY        (4)
    #define BioAPI_PURPOSE_ENROLL_FOR_IDENTIFICATION_ONLY      (5)
    #define BioAPI_PURPOSE_AUDIT                               (6)
    #define BioAPI_NO_PURPOSE_AVAILABLE                        (0)
```

  Η τιμή *NO_PURPOSE_AVAILABLE* χρησιμοποιείται για τους κωδικούς BIR οι οποίοι δεν παράγονται από τον BSP αλλά προκύπτουν από άλλες πηγές και έχουν μετατραπεί σε ένα BioApi BIR. Ο BSP δεν μπορεί να ορίσει τιμή *NO_PURPOSE_AVAILABLE* για έναν κωδικό που δημιουργεί.

- **BioAPI_BIR_BIOMETRIC_TYPE**
  Η τιμή του πεδίου αυτού προσδιορίζει τον τύπο του βιομετρικού χαρακτηριστικού στο οποίο ανήκει αυτός ο κωδικός. Παρακάτω φαίνονται οι τιμές που μπορεί να πάρει το συγκεκριμένο πεδίο.

```
typedef uint32_t BioAPI_BIR_BIOMETRIC_TYPE;

    #define BioAPI_NO_TYPE_AVAILABLE          (0x00000000)
    #define BioAPI_TYPE_MULTIPLE              (0x00000001)
    #define BioAPI_TYPE_FACIAL_FEATURES       (0x00000002)
    #define BioAPI_TYPE_VOICE                 (0x00000004)
    #define BioAPI_TYPE_FINGERPRINT           (0x00000008)
    #define BioAPI_TYPE_IRIS                  (0x00000010)
    #define BioAPI_TYPE_RETINA                (0x00000020)
    #define BioAPI_TYPE_HAND_GEOMETRY         (0x00000040)
    #define BioAPI_TYPE_SIGNATURE_DYNAMICS    (0x00000080)
    #define BioAPI_TYPE_KEYSTOKE_DYNAMICS     (0x00000100)
    #define BioAPI_TYPE_LIP_MOVEMENT          (0x00000200)
    #define BioAPI_TYPE_THERMAL_FACE_IMAGE    (0x00000400)
    #define BioAPI_TYPE_THERMAL_HAND_IMAGE    (0x00000800)
    #define BioAPI_TYPE_GAIT                  (0x00001000)
    #define BioAPI_TYPE_OTHER                 (0x40000000)
    #define BioAPI_TYPE_PASSWORD              (0x80000000)
```

  Εκτός από τις προφανείς τιμές υπάρχουν και κάποιες ειδικές τιμές όπως οι *MULTIPLE* και *OTHER*. Στην πρώτη περίπτωση το είδος της υπογραφής είναι σύνθετο και αποτελείται από παραπάνω από ένα γνωστά βιομετρικά χαρακτηριστικά. Στη δεύτερη περίπτωση πρόκειται για ένα κωδικό BIR που δεν έχει δημιουργηθεί από τον BSP. Το είδος της υπογραφής δεν είναι κάποιο από τα γνωστά χαρακτηριστικά και δεν είναι διαθέσιμο στην αρχική πηγή εγγραφής.

- **BioAPI_BIR_PRODUCT_ID**
  Η τιμή της παραμέτρου αυτής προσδιορίζει ένα αναγνωριστικό της οντότητας που δημιούργησε τα βιομετρικά δεδομένα που είναι αποθηκευμένα στο πεδίο BDB του κωδικού BIR. Αυτή η οντότητα μπορεί για παράδειγμα να είναι ο BSP ή μια εφαρμογή η οποία δημιούργησε ή μετασχημάτισε τα δεδομένα αυτά. Χαρακτηρίζεται από δυο επιμέρους παραμέτρους, τις *ProductOwner* και *ProductType*.

```
typedef struct bioapi_bir_biometric_product_ID {
    uint16_t ProductOwner;
    uint16_t ProductType;
} BioAPI_BIR_BIOMETRIC_PRODUCT_ID;

    #define BioAPI_NO_PRODUCT_OWNER_AVAILABLE       (0x0000)
    #define BioAPI_NO_PRODUCT_TYPE_AVAILABLE        (0x0000)
```

  Η τιμή *NO_PRODUCT_TYPE_AVAILABLE* χρησιμοποιείται στις περιπτώσει όπου ο κωδικός BIR δεν έχει δημιουργηθεί από τον BSP.

- **BioAPI_BIR_CREATION_DAY**
  Στο πεδίο αυτό προσδιορίζεται η ημέρα που δημιουργήθηκαν τα βιομετρικά δεδομένα με την εξής μορφή YYYYMMDD (π.χ. 20120822, δηλαδή 22 Αυγούστου 2012)

- **BioAPI_BIR_CREATION_TIME**
  Η τιμή του πεδίου αυτού προσδιορίζει την ώρα δημιουργίας των βιομετρικών δεδομένων, έχοντας τη μορφή hhmmss (π.χ. 054020Z, δηλαδή στις 5 και 40 λεπτά και 20 δευτερόλεπτα.)

- **BioAPI_BIR_SUBTYPE**
  Το περιεχόμενο του πεδίου αυτού προσδιορίζει περαιτέρω τον τύπο του βιομετρικού χαρακτηριστικού του BDB πεδίου και δίνει περισσότερες πληροφορίες γι' αυτό. Εκτός του ότι αποτελεί πεδίο στον κωδικό BIR, μπορεί να χρησιμοποιηθεί και σαν είσοδος σε κάποια συνάρτηση. Οι τιμές που μπορεί να πάρει ποικίλουν ανάλογα με το βιομετρικό χαρακτηριστικό. Μπορεί να έχει τις τιμές "δεξί" ή "αριστερό" όταν πρόκειται π.χ. για το μάτι, το χέρι ή τη γεωμετρία χεριού κλπ ή μπορεί να παίρνει τιμές οι οποίες προσδιορίζουν ένα από τα 5 δάκτυλα του χεριού από το οποίο έχει καταγραφεί του αποτύπωμα.

```
typedef uint8_t BioAPI_BIR_SUBTYPE;

    #define BioAPI_BIR_SUBTYPE_LEFT              (0x01)
    #define BioAPI_BIR_SUBTYPE_RIGHT             (0x02)
    #define BioAPI_BIR_SUBTYPE_THUMB             (0x04)
    #define BioAPI_BIR_SUBTYPE_POINTERFINGER     (0x08)
    #define BioAPI_BIR_SUBTYPE_MIDDLEFINGER      (0x10)
    #define BioAPI_BIR_SUBTYPE_RINGFINGER        (0x20)
    #define BioAPI_BIR_SUBTYPE_LITTLEFINGER      (0x40)
    #define BioAPI_BIR_SUBTYPE_MULTIPLE          (0x80)

    #define BioAPI_NO_SUBTYPE_AVAILABLE          (0x00)
```

  Η τιμή *NO_SUBTYPE_AVAILABLE* χαρακτηρίζει τους κωδικούς BIR που δεν έχουν δημιουργηθεί από τον BSP αλλά από μια άλλη μορφή δεδομένων. Επίσης όταν μια εφαρμογή θέλει να ορίζει ο BSP τον υποτύπο του χαρακτηριστικού, τότε δίνει στο πεδίο αυτό την τιμή 0.

- **BioAPI_BIR_EXPIRATION_DATE**
  Η τιμή του πεδίου αυτού προσδιορίζει την ημέρα που παύει να ισχύει ο συγκεκριμένος κωδικός BIR έχοντας την ίδια μορφή με την BioAPI_BIR_CREATION_DATE, YYYYMMDD (π.χ. 20120822, δηλαδή 22 Αυγούστου 2012)

- **BioAPI_BIR_SB_FORMAT**
  Το πεδίο αυτό καθορίζει τη μορφή των δεδομένων που περιέχονται στο πεδίο Security Block του BioAPI. Περιλαμβάνει δυο επιπλέον ιδιότητες *FormatOwner* και *Format*Type. Το SB πεδίο μπορεί να περιέχει μια ψηφιακή υπογραφή ή κάποιο κωδικοποιημένο μήνυμα ταυτότητας και το πεδίο SB_FORMAT περιλαμβάνει πληροφορίες γι αυτά.

```
typedef struct bioapi_bir_security_block_format {
    uint16_t SecurityFormatOwner;
    uint16_t SecurityFormatType;
} BioAPI_BIR_SECURITY_BLOCK_FORMAT;
```

- **BioAPI_BIR_INDEX**
  Το πεδίο αυτό είναι ένα παγκοσμίως μοναδικό αναγνωριστικό που χρησιμοποιείται για να προσδιορίζει και να βρίσκει στοιχεία όπως τον BSP, μονάδες του BioAPI, το Framework που χρησιμοποιείται, τη βάση δεδομένων του συστήματος, καθώς επίσης χρησιμοποιείται και ως δείκτης της βάσης δεδομένων για τον BSP.

```
typedef  uint8_t  BioAPI_UUID[16];
```

Πίνακας 3: Πίνακας τιμών των BioAPI δεδομένων

BioAPI field name, BioAPI reference and patron format field name	**Length (bytes)**	**Abstract Values**	**Encoding**
BIRLenght	4	Length in bytes of the entire BIR encoding, with the exception of this length field	integer
BioAPI_VERSION	1	Major=2 Minor=1	'20'
BioAPI_BIR_DATA_TYPE	1	NOT ENCRYPTED ENCRYPTED	'0_' '1_'
		NOT SIGNED SIGNED	'0_' '2_'
		NO VALUE AVAILABLE RAW INTERMEDIATE PROCESSED	'_1' '_2' '_3' '_4'
(index flag)		INDEX PRESENT	'8_'
BioAPI_BIR_BIOMETRIC_DATA_FORMAT	4	FormatOwner FormatType	Integer Integer
BioAPI_QUALITY	1	NOT SUPPORTED NOT SET (NO VALUE AVAILABLE) VALUE	-2 -1 0-100
BioAPI_BIR_PURPOSE	1	NO VALUE AVAILABLE VERIFY IDENTITY ENROLL ENROLL_FOR_VERIFICATION_ONLY ENROLL _FOR_IDENTIFICATION_ONLY AUDIT	0 1 2 3 4 5 6
BioAPI_BIR_BIOMETRIC_TYPE	4	NO VALUE AVAILABLE MULTIPLE FACIAL FEATURES VOICE FINGERPRINT IRIS RETINA HAND GEOMETRY SIGNATURE DYNAMICS KEYSTROKE DYNAMICS LIP MOVEMENT THERMAL FACE IMAGE	'00 00 00 00' '00 00 00 01' '00 00 00 02' '00 00 00 04' '00 00 00 08' '00 00 00 10' '00 00 00 20' '00 00 00 40' '00 00 00 80' '00 00 01 00' '00 00 02 00' '00 00 04 00'

		THERMAL HAND GEOMETRY GAIT OTHER PASSWORD	’00 00 08 00’ ’00 00 10 00’ ’40 00 00 00’ ’80 00 00 00’
BioAPI_BIR_BIOMETRIC_PRODUCT_ID	4	ProductOwner ProductType NO VALUE AVAILABLE	Non-zero Integer Non-zero Integer ’00 00 00 00’
BioAPI_DATE (creation date)	4	NO VALUE AVAILABLE Year, Month, Day	’00 00 00 00’ Integers, not all zero
BioAPI_Time (creation time)	4	NO VALUE AVAILABLE Hour, Minute, Second	’99 99 99; integers
BioAPI_BIR_SUBTYPE	1	NO VALUE AVAILABLE LEFT RIGHT THUMB POINTFINGER MILDLEFINGER RINGFINGER LITTLEFINGER MULTIPLE	‘00’ ‘01’ ’02’ ’04’ ‘08’ ‘10’ ‘20’ ‘40’ ‘80’
BioAPI_DATE (expiration date)	4	NO VALUE AVAILABLE Year, Month, Day	’00 00 00 00’ Integers, not all zero
BioAPI_BIR_SECURITY_BLOCK_FORMAT	4	SecurityFormatOwner SecurityFormatType NO VALUE AVAILABLE	Non-zero Integer Non-zero Integer ’00 00 00 00’
BioAPI_UUID (index)	16	BIR database index	Integer
BDB Length	4	Length in bytes of BDB	Integer
BioAPI_DATA (BiometricData)	Variable	BiometricData	
SB Length	4	Length in bytes of SB	Integer
BioAPI_DATA (SecurityBlock)	Variable	SecurityBlock	

6.1.2 Opaque Biometric Data Block

Το συγκεκριμένο κομμάτι της βιομετρικής εγγραφής αναγνώρισης περιλαμβάνει ένα βιομετρικό πρότυπο το οποίο καθορίζει τα βιομετρικά δεδομένα του χαρακτηριστικού που υποβάλει ο χρήστης. Μπορεί να είναι σε μια μη τυπική μορφή ή μια μορφή αρχείου που έχει δημιουργηθεί ή εγκριθεί από τα πρότυπα σώματος, τη Βιομετρική Κοινοπραξία ή από μια ομάδα ατόμων που έχουν ορίσει τα χαρακτηριστικά ενός προτύπου. Τις φορές που το περιεχόμενο δεν είναι κάποιο βιομετρικό πρότυπο, είναι επιμέρους πληροφορίες, παράμετροι και δεδομένα που καθορίζουν τη μορφή του προτύπου. Από τις πληροφορίες αυτές εξαρτάται και το μέγεθος του πεδίου το οποίο δεν είναι προκαθορισμένο. Επίσης, ανάλογα με τη μορφή του προτύπου που έχει οριστεί για τις ψηφιακές υπογραφές του κάθε συστήματος, τα δεδομένα αυτά μπορεί να είναι κωδικοποιημένα ή όχι.

6.1.3 Security Block

Το τρίτο μέρος της βιομετρικής εγγραφής αναγνώρισης δεν υφίσταται απαραίτητα σε κάθε εγγραφή. Η ύπαρξή του εξαρτάται από το είδος ασφάλειας που καθορίζεται για τη συγκεκριμένη εγγραφή. Στο πεδίο αυτό αποθηκεύεται η υπογραφή ή το μήνυμα αυθεντικοποίησης των δεδομένων. Μπορεί επίσης να περιέχει πληροφορίες που θα χρησιμοποιηθούν στον αλγόριθμο αναγνώρισης ή και τις παραμέτρους που απαιτούνται για την εκτέλεση της υπογραφής ή τη λειτουργία του μηνύματος MAC. Το μέγεθος του πεδίου αυτού δεν είναι προκαθορισμένο αλλά εξαρτάται από το πλήθος των δεδομένων που είναι αποθηκευμένα σ' αυτό.

6.2 Λοιπές πληροφορίες που περιέχει ένα BioAPI αρχείο

Εκτός από τον κωδικό BIR ένα αρχείο BioAPI περιλαμβάνει κι άλλες πληροφορίες για τη σωστή λειτουργία και τη σωστή εκτέλεση διεργασιών σε ένα βιομετρικό σύστημα. Πιο αναλυτικά, θα πρέπει να διευθετηθεί η επικοινωνία του BSP με τη βάση δεδομένων και το Graphical User Interface (GUI). Παρακάτω παρουσιάζονται αναφορικά κάποιες από τις διεργασίες και τις μεταβλητές που περιλαμβάνονται στο αρχείο αυτό.

Για τη βάση δεδομένων:

- BioAPI_DB_ACCESS_TYPE //ορίζει το επίπεδο πρόσβασης της εφαρμογής στη βάση δεδομένων του BSP
- BioAPI_DB_MARKER_HANDLE // είναι ένας δείκτης, ο οποίος δείχνει σε μια εγγραφή της βάσης δεομένων
- BioAPI_DB_HANDLE // δείχνει σε μια βάση δεδομένων και η εφαρμογή το χρησιμοποίει για να δείξει μια εγγραφή της βάσης δεδομένων
- BioAPI_DBBIR_ID // μια δομή η οποία δείχνει σε μια βάση δεδομένων που ελέγχεται από τον BSP και έτσι η εφαρμογή μπορεί να χρησιμοποιήσει δεδομένα της συγκεκριμένης βάσης.
- BioAPI_DbOpen //συνάρτηση που ανοίγει μια βάση δεδομένων στον BSP, και δημιουργεί τον marker για την πρώτη εγγραφή.
- BioAPI_DbClose // συνάρτηση που κλείνει μια βάση δεδομένων καθώς όλοι οι markers έχουν αντιστοιχισθεί με κάποια εγγραφή
- BioAPI_DbCreate //συνάρτηση που δημιουργεί έναν νέο κωδικό BIR για την επόμενη εγγραφή στη βάση δεδομένων
- BioAPI_DbDelete // συνάρτηση που διαγράφει όλες τις εγγραφές από τη συγκεκριμένη βάση δεδομένων και αφαιρεί όλες τις πληροφορίες που σχετίζονται με αυτή.
- BioAPI_DbSetMarker //συνάρτηση που ρυθμίζει τον δείκτη MARKER_HANDLE ώστε να δείχνει ένα κωδικό BIR της βάσης δεδομένων.
- BioAPI_DbFreeMarker //συνάρτηση που ελευθερώνει τη μνήμη και τους πόρους που σχετίζονται με το συγκεκριμένο δείκτη ακυρώνει τη τιμή της μεταβλητής MARKER_HANDLE
- BioAPI_DbStoreBIR //συνάρτηση που αποθηκεύει στη βάση ένα συγκεκριμένο κωδικό BIR.

- BioAPI_DbGetBIR //συνάρτηση που αποθηκεύει τον κωδικό BIR σε ένα προσωρινό μέρος του BSP ώστε να μπορεί να τον χρησιμοποιήσει σε κάποια μετέπειτα διεργασία.
- BioAPI_DbGetNextBIR // συνάρτηση που αποθηκεύει τον επόμενο κωδικό BIR σε ένα προσωρινό μέρος του BSP ώστε να μπορεί να τον χρησιμοποιήσει σε κάποια μετέπειτα διεργασία
- BioAPI_DbDeleteBIR //συνάρτηση που διαγράφει ένα κωδικό BIR αι επομένως μια βιομετρική ταυτότητα

Για τη διεπαφή χρήστη (GUI):

- BioAPI_GUI_BITMAP //ορίζει τη γραφική εικόνα της εφαρμογής
- BioAPI_GUI_MESSAGE // μήνυμα της εφαρμογής
- BioAPI_GUI_PROGRESS //απεικονίζει τη πρόοδο ολοκλήρωσης της εισόδου του BSP στην εφαρμογή
- BioAPI_GUI_RESPONSE //η εφαρμογή επιστρέφει μια τιμή κατά τη διάρκεια μιας λειτουργίας
- BioAPI_GUI_STATE // δείχνει την κατάσταση της διεπαφής αλλά και ενημερώνει το χρήστη για τυχόν παραμέτρους που χρειάζονται.
- BioAPI_GUI_STATE_CALLBACK // ενημερώνει την εφαρμογή αν ο BSP μπορεί να της παρέχει πληροφορίες.
- BioAPI_GUI_STREAMING_CALLBACK // μια συνάρτηση η οποία επιτρέπει στον BSP να στείλει πληροφορίες, με τη μορφή μιας σειράς bit, στην εφαρμογή.

Για τον BSP:

- BioAPI_BSPLoad //ορίζει την εκκίνηση του BSP και ενεργοποιεί τα γεγονότα που πρέπει να εκτελεστούν
- BioAPI_BSPUnload // σταματά τη λειτουργία του BSP, να καταγράφει δηλαδή τα αποτελέσματα των γεγονότων που εκτελούνται.
- BioAPI_BSPAttach //προσπαθεί να φέρει σε επαφή BSP και εφαρμογή και ελέγχει τη συμβατότητά τους.
- BioAPI_BSPDettach //σταματά την επαφή μεταξύ BSP και εφαρμογής, αποσυνδέει τον BSP από την εφαρμογή

Για τη λειτουργία της εφαρμογής:

- BioAPI_Capture //συνάρτηση που καταγράφει δείγματα και επιστρέφει είτε ένα ενδιάμεσο ή ένα επεξεργασμένο τύπο BIR
- BioAPI_CreateTemplate // συνάρτηση η οποία δημιουργεί ένα νέο πρότυπο εγγραφής.
- BioAPI_Process // συνάρτηση που επεξεργάζεται τα ενδιάμεσα δεδομένα για επαλήθευση ή αναγνώριση
- BioAPI_ProcessWithAuxBIR // συνάρτηση που επεξεργάζεται τα ενδιάμεσα δεδομένα μαζί με βοηθητικά δεδομένα για μεταγενέστερη επαλήθευση ή αναγνώριση
- BioAPI_Enroll //συνάρτηση που συλλαμβάνει τα βιομετρικά δεδομένα από έναν αισθητήρα για τη δημιουργία μιας εγγραφής
- BioAPI_Verify // συνάρτηση που εκτελεί μια ένα-προς-πολλά επαλήθευση ανάμεσα σε κωδικούς BIR
- BioAPI_VerifyMatch //συνάρτηση που εκτελεί μια ένα-προς-ένα επαλήθευση ανάμεσα σε δυο κωδικούς BIR

- BioAPI_Identity //συνάρτηση που συλλαμβάνει βιομετρικά δεδομένα από μια συσκευή π.χ. αισθητήρα και συγκρίνει τα δεδομένα με κάποιο πρότυπο.
- BioAPI_IdentityMatch // συνάρτηση που συλλαμβάνει βιομετρικά δεδομένα από μια συσκευή π.χ. αισθητήρα και συγκρίνει τα δεδομένα με ένα σύνολο προτύπων.

6.3 Παράδειγμα πολύτροπης βιομετρικής υπογραφής

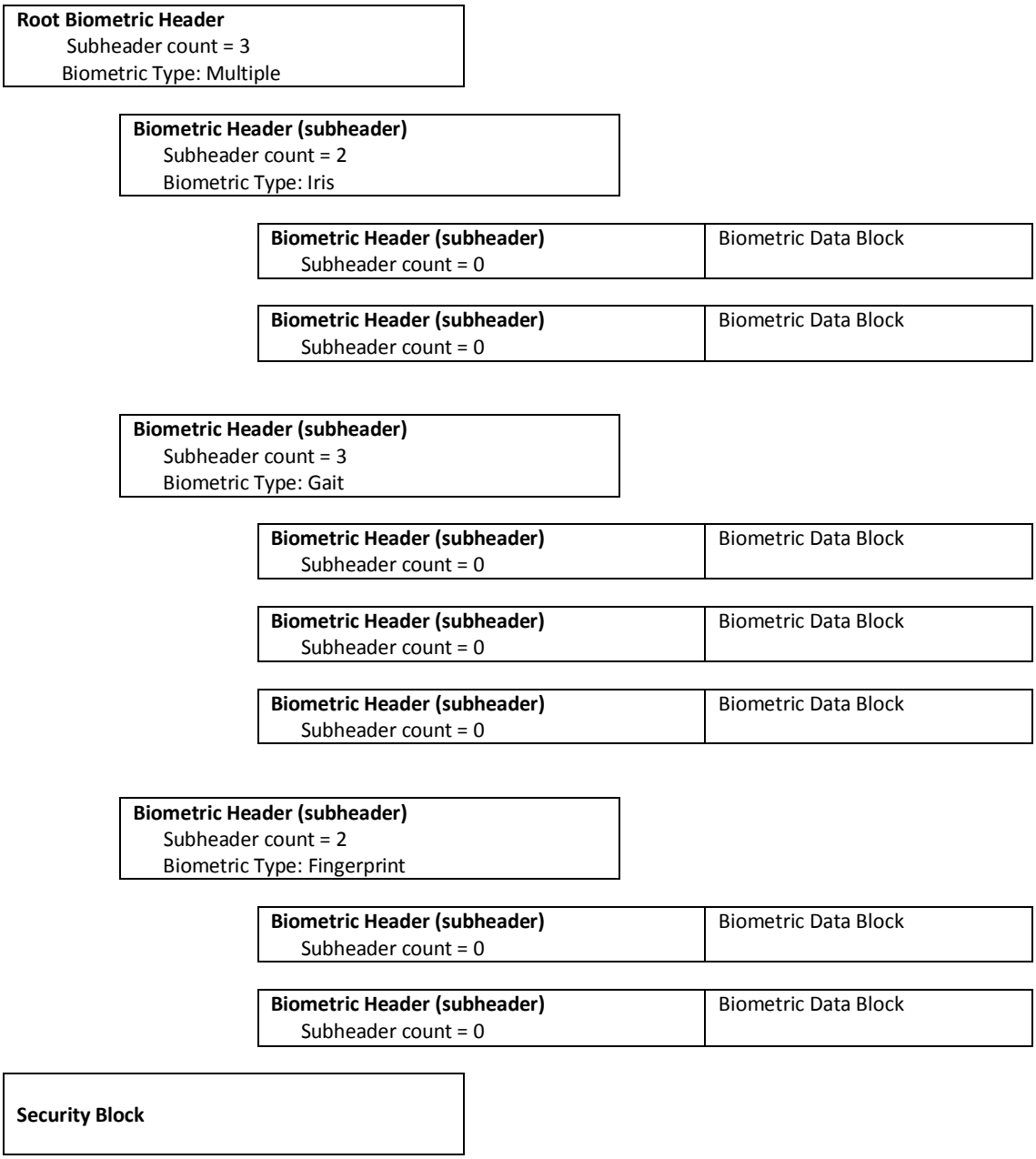
Έχοντας μελετήσει τη δομή μιας βιομετρικής υπογραφής, τη χρήση και τις ιδιαιτερότητές της, μια πολύτροπη βιομετρική υπογραφή είναι καλό να αποτελείται από 3 χαρακτηριστικά του ανθρώπινου σώματος. Αυτός ο αριθμός χαρακτηριστικών δεν είναι πολύ μικρός ώστε να είναι αρκετά ευπαθής σε επιθέσεις, αλλά ούτε και πολύ μεγάλος ώστε να κουράζει το χρήστη κατά τη διαδικασία εισαγωγής του στο σύστημα. Τα βιομετρικά χαρακτηριστικά που αποτελούν τη σύνθετη βιομετρική υπογραφή του παραδείγματός μας είναι το πρόσωπο, η ίριδα και το αποτύπωμα. Κάθε ένα από αυτά αποτελεί και ένα πρότυπο. Κάθε πρότυπο διακρίνεται από επιμέρους χαρακτηριστικά τα οποία και θα αναφέρουμε.

Χαρακτηριστικά ίριδας:
- Οριοθέτηση ίριδας (εύρεση εξωτερικών σημείων)
- Κέντρο ίριδας
- Φυσιολογία της ίριδας (κρύπτες, χρωστικές κουκίδες, αυλάκια)
- IrisCode

Χαρακτηριστικά βηματισμού:
- Απόσταση ποδιών
- Σιλουέτα
- Σκελετικές διαστάσεις και μάζα (έδαφος, τραυματισμοί, ενδυνάμωση μυών, κόπωση κλπ)
- Συχνότητα διοχέτευσης
- Κλείδωμα φάσης
- Σωματική αξιοπιστία

Χαρακτηριστικά δακτυλικού αποτυπώματος:
- Σημεία Galton (τελείωμα διακλαδώσεων και κορυφογραμμών)
- Minutiae (Arch , loop, whorl)

Δεν είναι απαραίτητο μια τελική υπογραφή να αποτελείται από όλα τα παραπάνω χαρακτηριστικά, μερικά από αυτά είναι αρκετά, αρκεί φυσικά το σύνολό τους να αποτελεί συνδυασμό των τριών βασικών χαρακτηριστικών (ίριδα, βηματισμός, δακτυλικό αποτύπωμα).



Σχήμα 6.1: Κωδικός BIR πολύτροπης βιομετρικής υπογραφής

Στο παραπάνω σχήμα απεικονίζεται η μορφή του κωδικού BIR μιας πολύτροπης βιομετρικής υπογραφής και όπως φαίνεται αποτελείται από τρία επίπεδα. Στο πρώτο επίπεδο (από έξω προς τα μέσα) βλέπουμε ότι υπάρχουν η κεφαλίδα και το security block της υπογραφής αυτής. Το BDB μιας υπογραφής, όπως αναφέρθηκε παραπάνω στην ενότητα 6.1.2 περιέχει το πρότυπο ή επιμέρους πληροφορίες, παραμέτρους και δεδομένα που καθορίζουν τη μορφή του προτύπου. Στο παράδειγμά μας το BDB πεδίο απεικονίζεται στο σχήμα από το δεύτερο και τρίτο επίπεδο. Στο δεύτερο επίπεδο υπάρχουν οι κεφαλίδες, μία για κάθε χαρακτηριστικό του ανθρώπινου σώματος (ίριδα, βηματισμός, δακτυλικό αποτύπωμα) οι οποίες μας λένε ποια βιομετρικά χαρακτηριστικά αποτελούν την πολύτροπη βιομετρική υπογραφή (BiometricType) και πόσα επιμέρους χαρακτηριστικά (Subheader count) διακρίνουν την κάθε μία. Στο τρίτο επίπεδο απεικονίζονται όλα τα επιμέρους χαρακτηριστικά γνωρίσματα (features) τα οποία διακρίνουν

κάθε βιομετρικό χαρακτηριστικό. Για παράδειγμα παρατηρούμε ότι για την ίριδα υπάρχουν δυο επιμέρους χαρακτηριστικά π.χ. φυσιολογία ίριδας και iriscode, για το βάδισμα τρία επιμέρους χαρακτηριστικά π.χ. σιλουέτα, σκελετικές διαστάσεις και κλείδωμα φάσης, για το δακτυλικό αποτύπωμα δύο επιμέρους χαρακτηριστικά π.χ. σημεία Galton και οι μικρολεπτομέρειες minutiae.

Κεφάλαιο 7ο Συμπεράσματα - Επεκτάσεις

7.1 Συμπεράσματα

Όπως η εξέλιξη στη ζωή του ανθρώπου έτσι και η εξέλιξη στην τεχνολογία προχωρά με ταχύτατους ρυθμούς. Τα συστήματα έχουν εισέλθει στη καθημερινότητά μας εδώ και πολλά χρόνια και εμείς καλούμαστε να τα ακολουθήσουμε και να τα εξελίξουμε ακόμη περισσότερο. Η ασφαλής χρήση τους και οι αξιόπιστοι χρήστες είναι θέματα που απασχόλησαν πολύ τον άνθρωπο. Στην αρχή, η χρήση κωδικών ασφαλείας έδωσε λύση στο πρόβλημα. Αργότερα όμως οι κωδικοί αυτοί δεν αποτελούσαν πια εμπόδιο στα σχέδια των εισβολέων. Έτσι στη συνέχεια, ξεκίνησαν να χρησιμοποιούν ως κωδικούς πρόσβασης σημεία του ανθρώπινου σώματος, τα λεγόμενα βιομετρικά χαρακτηριστικά, τα οποία είναι πολύ πιο δύσκολο να κλαπούν.

Τα βιομετρικά χαρακτηριστικά παρουσιάστηκαν ένα-ένα στην εργασία αυτή και μελετώντας τα φτάσαμε στο συμπέρασμα πως η δομή των αγγείων, και επομένως η σάρωση του

αμφιβληστροειδή, είναι το πιο αξιόπιστο βιομετρικό χαρακτηριστικό. Μπορεί να προσφέρει υψηλή ασφάλεια σε ένα σύστημα αλλά υπάρχει ο κίνδυνος να απορρίψει μεγάλο ποσοστό μη εξουσιοδοτημένων χρηστών εάν οι χρήστες δεν είναι συγκεντρωμένοι κατά τη διαδικασία επαλήθευσης ή ταυτοποίησης. Επομένως, η αξιοπιστία ενός συστήματος, όσον αφορά την επιλογή του βιομετρικού χαρακτηριστικού, εξαρτάται από τις απαιτήσεις της εφαρμογής. Υψηλή ασφάλεια ή φιλικότητα προς το χρήστη? Είναι λεπτή η ισορροπία των δυο αυτών παραγόντων. Συνεπώς, ανάλογα με τις απαιτήσεις συστήματος και χρηστών επιλέγεται το καταλληλότερο βιομετρικό χαρακτηριστικό ή ο συνδυασμός διαφόρων βιομετρικών χαρακτηριστικών ο οποίος καθιστά το σύστημα πιο ασφαλές. Συμπεραίνουμε λοιπόν πως ιδανικό σύστημα δεν υπάρχει. Σε κάθε σύστημα παρουσιάζονται ευαισθησίες και "κενά" τα οποία μπορεί να εκμεταλλευτεί ο εισβολέας για να κάνει την κίνησή του. Αναλύοντας τα μοντέλα εφαρμογής για την υλοποίηση της αρχιτεκτονικής και τις ευπάθειες ενός συστήματος διαπιστώσαμε πως πάντα θα υπάρχουν σημεία στα οποία, ένα σύστημα, θα υπερέχει και άλλα στα οποία θα υστερεί. Φυσικά σε όλο αυτό, παίζουν σημαντικό ρόλο και τα πρότυπα ασφαλείας που δημιουργήθηκαν καθώς και η δυνατότητα ανάκλησης μιας βιομετρικής υπογραφής. Η ανάκληση της υπογραφής αποδείχτηκε μεγάλο εξελικτικό βήμα διότι έχει συμβάλει κατά πολύ στην πρόληψη της κλοπής μιας ταυτότητας. Επίσης, ένας από τους στόχους της εργασίας αυτής ήταν η παρουσίαση της πολύτροπης βιομετρικής υπογραφής ο οποίος υλοποιήθηκε στο $6^{ο}$ κεφάλαιο. Μια σύνθετη υπογραφή δεν διαφέρει πολύ από μια απλή. Στην ουσία πρόκειται για εμφωλευμένες απλές υπογραφές, πράγμα το οποίο μας οδηγεί στο συμπέρασμα πως η υλοποίηση των δυο αντίστοιχων υπογραφών είναι πάνω κάτω η ίδια.

Όλα τα παραπάνω συμβάλλουν για τη δημιουργία ενός αξιόπιστου και ακριβή βιομετρικού συστήματος, το οποίο στις μέρες θα έλεγε κανείς ότι είναι απαραίτητο. Τα βιομετρικά συστήματα δημιουργήθηκαν από τον άνθρωπο, εκείνος είναι αυτός που μπορεί να τα καθορίσει, αλλά και να τα εξελίξει. Η εγκληματικότητα αυξάνεται με ταχύτατους ρυθμούς, η απληστία και η ανάγκη του ανθρώπου για εξουσία μπορεί εύκολα να τον οδηγήσει σε κλοπές και παρανομίες. Γι αυτό και η σωστή διαχείριση της τεχνολογίας είναι απαραίτητη.

7.2 Επεκτάσεις

Η πολύτροπη βιομετρία είναι θα λέγαμε στην αρχή της ανάπτυξής της. Έχουμε δει ένα μικρό ποσοστό των δυνατοτήτων που μπορεί να προσφέρει και μέσα στα επόμενα χρόνια αναμένεται η εξέλιξή της. Πολλοί είναι εκείνοι που πιστεύουν πως σε μια πολυδιάστατη υπογραφή είναι καλύτερο να υπάρχει φυσιολογικό αλλά και συμπεριφοριστικό χαρακτηριστικό διότι ο συνδυασμός και των δυο δεν είναι ευπαθής σε απόπειρες εισβολής. Εμείς δεν είμαστε σίγουροι γι αυτή την άποψη. Πιστεύουμε πως ο συνδυασμός n φυσιολογικών χαρακτηριστικών είναι πιο ισχυρός από έναν συνδυασμό n φυσιολογικών και συμπεριφοριστικών χαρακτηριστικών. Θεωρούμε λοιπόν καλό να πραγματοποιηθεί μια έρευνα ή και μια υλοποίηση δυο συστημάτων έτσι ώστε να δούμε τη διαφορά στην απόδοσή τους. Η βιομετρική υπογραφή του ενός συστήματος θα μπορούσε να απαρτίζεται από 4 φυσιολογικά χαρακτηριστικά, το δακτυλικό αποτύπωμα, τη σάρωση του αμφιβληστροειδή, τη σάρωση της ίριδας και την αναγνώριση του αυτιού. Η βιομετρική υπογραφή του άλλου συστήματος θα μπορούσε να απαρτίζεται από 2 φυσιολογικά και 2 συμπεριφοριστικά χαρακτηριστικά, τη σάρωση της ίριδας, το δακτυλικό αποτύπωμα, την αναγνώριση φωνής και το βάδισμα. Όσον αφορά την αρχιτεκτονική πλευρά των δυο συστημάτων θα πρέπει φυσικά να σχεδιαστούν και τα δυο με βάση το ίδιο μοντέλο

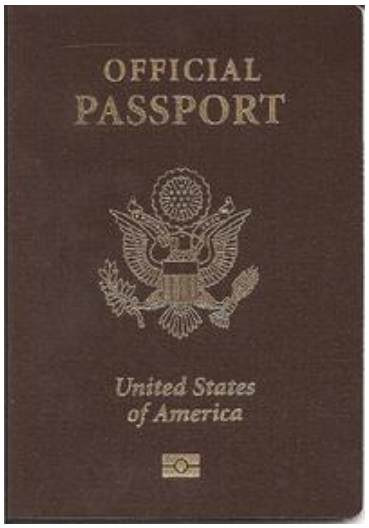
αρχιτεκτονικής χωρίς να παίζει σημαντικό ρόλο ποιο από τα 8 θα είναι. Εδώ δεν μας ενδιαφέρει τόσο η αρχιτεκτονική όσο η επιλογή των βιομετρικών χαρακτηριστικών. Στη συνέχεια, ένας αριθμός ατόμων (π.χ. 500) θα εγγραφούν και στα δυο συστήματα και έπειτα θα πραγματοποιήσουν τη διαδικασία πιστοποίησης. Τέλος, θα καταγραφούν και θα μελετηθούν στατιστικά οι παράγοντες FAR (false accept rate) και FRR (false reject rate) και έτσι θα οδηγηθούμε σε μια πιο εμπεριστατωμένη άποψη.

Ένα από τα σημαντικά προβλήματα των τελευταίων χρόνων αφορά σε κλοπές ταυτοτήτων. Έχουν ακουστεί πάρα πολλά για πλαστά διαβατήρια και για την αντικατάστασή τους με ηλεκτρονικά διαβατήρια. Αποτελεί λοιπόν ένα επίκαιρο και ενδιαφέρον θέμα. Θα ήταν σκόπιμο επομένως να πραγματοποιηθεί μια υλοποίηση ενός ηλεκτρονικού διαβατηρίου. Με μια πρώτη σκέψη καλό θα ήταν να γίνεται η χρήση όχι ενός βιομετρικού χαρακτηριστικού για την αυθεντικοποίηση του χρήστη. Η χρήση τριών βιομετρικών χαρακτηριστικών θα αποτελούσε για μένα ιδανική λύση, αλλά είναι πολύ πιθανό να κουράσει το χρήστη κατά την διαδικασία αυθεντικοποίησης. Για να αποφύγουμε αυτό το πρόβλημα θα πρότεινα τα εξής τρία χαρακτηριστικά, τη γεωμετρία χεριού, το δακτυλικό αποτύπωμα του δείκτη, και τη σάρωση αμφιβληστροειδή του χρήστη. Για τα δυο πρώτα χαρακτηριστικά ο χρήστης δεν θα χρειάζεται να υποβάλλει το χέρι του δυο φορές. Η συσκευή σάρωσης θα σαρώνει την επιφάνεια του χεριού και τα βιομετρικά χαρακτηριστικά θα εξάγονται από την ίδια εικόνα σε επόμενη φάση. Έτσι, το σύστημα θα ζητά από το χρήστη να υποβάλλει το χέρι του σε μια αντίστοιχη συσκευή και το μάτι του σε μια άλλη, προκειμένου να πραγματοποιηθεί και η σάρωση αμφιβληστροειδή. Μέχρι σήμερα στα ηλεκτρονικά διαβατήρια χρησιμοποιούνταν μόνο ένα χαρακτηριστικό και αυτό ήταν είτε το πρόσωπο, είτε το δακτυλικό αποτύπωμα, είτε η ίριδα. Η χρήση όμως μιας πολύτροπης βιομετρικής υπογραφής θα εξασφαλίσει μεγαλύτερη αξιοπιστία για την αυθεντικοποίηση του χρήστη διότι καθιστά την κλοπή μιας ταυτότητας πιο δύσκολη. Επίσης η επιλογή του αμφιβληστροειδή ως βιομετρικό χαρακτηριστικό έγινε διότι τα αγγεία του αποτελούν ένα σύνθετο σχέδιο το οποίο διαφέρει σε μεγάλο βαθμό ακόμα και στην περίπτωση των πανομοιότυπων διδύμων. Πρόκειται για ένα χαρακτηριστικό που δεν αλλάζει κατά τη διάρκεια της ζωής του ανθρώπου, εκτός από εξεζητημένες περιπτώσεις, και είναι ένα μέρος του σώματος που προστατεύεται από ατυχήματα με φυσικό τρόπο λόγω της ανατομίας του σώματος. Πολλοί χρήστες ισχυρίζονται πως η σάρωση του αμφιβληστροειδή δεν είναι εύκολη στη χρήση διότι πρέπει να τοποθετήσουν τα μάτια τους πολύ κοντά στη συσκευή και αισθάνονται φόβο και δυσφορία. Έχοντας όμως όλοι επισκεφτεί κάποια στιγμή στη ζωή μας έναν οφθαλμίατρο έχουμε διαπιστώσει ότι δεν πρόκειται για κάτι τόσο τρομακτικό. Παρ' όλα αυτά αν εξακολουθούν οι χρήστες να έχουν την ίδια άποψη, ένα εναλλακτικό χαρακτηριστικό που θα μπορούσε να χρησιμοποιηθεί είναι η ίριδα.

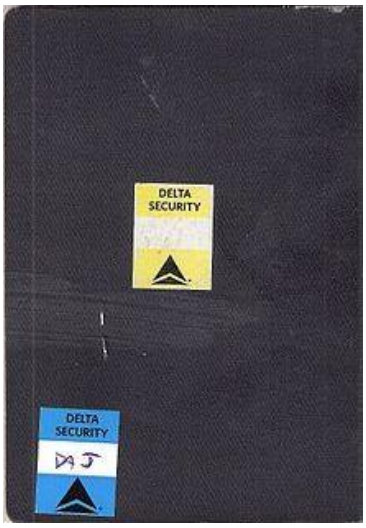
Βλέποντας την πρόταση αυτή από τεχνικής πλευράς, πρέπει να βρεθεί και το κατάλληλο μοντέλο αρχιτεκτονικής για την υλοποίηση του συστήματος. Το ηλεκτρονικό διαβατήριο εκτός από τις βασικές πληροφορίες που θα παρέχει για το χρήστη σε έντυπη μορφή θα χρησιμοποιείται και σαν ένα token για την παροχή ηλεκτρονικών πληροφοριών που θα αφορούν το χρήστη. Θα ενσωματωθεί λοιπόν ένα μικροτσίπ στο ηλεκτρονικό διαβατήριο όπου θα είναι αποθηκευμένο το βιομετρικό πρότυπο της πολύτροπης υπογραφής του χρήστη. Κατά τη δημιουργία του ηλεκτρονικού διαβατηρίου θα πρέπει να δημιουργηθεί το βιομετρικό πρότυπο, η εγγραφή δηλαδή του χρήστη στο σύστημα. Κατά την εγγραφή, το σύστημα ζητά από το χρήστη να υποβάλλει το χέρι και το μάτι του στις αντίστοιχες συσκευές σάρωσης. Οι σαρωτές δημιουργούν φωτογραφίες οι οποίες επεξεργάζονται στο στάδιο εξαγωγής χαρακτηριστικών. Από τη φωτογραφία που αντιστοιχεί στο χέρι θα εξαχθούν δυο από τα τρία βιομετρικά χαρακτηριστικά, η γεωμετρία του χεριού και το δακτυλικό αποτύπωμα, και από τη φωτογραφία που αντιστοιχεί στο μάτι θα εξαχθεί

η αγγειακή δομή του αμφιβληστροειδή. Η υποβολή των χαρακτηριστικών επαναλαμβάνεται για 7 φορές έτσι ώστε να μη δημιουργηθεί μια ψευδή ταυτότητα. Από τις 7 φορές, οι 5 τουλάχιστον θα πρέπει να είναι ίδιες κατά ένα ποσοστό 90% για να συνεχιστεί η διαδικασία εγγραφής. Στη συνέχεια, με βάση τα χαρακτηριστικά που έχουν εξαχθεί, δημιουργείται η βιομετρική υπογραφή του χρήστη. Αυτή η πρώτη υπογραφή που έχει δημιουργηθεί αποτελεί και το πρότυπο βιομετρικής του υπογραφής το οποίο θα αποθηκευτεί σε μια βάση δεδομένων του συστήματος, αλλά και στο token που θα ενσωματωθεί στο ηλεκτρονικό διαβατήριο.

Ένα ηλεκτρονικό διαβατήριο θα παρέχει και μη βιομετρικές πληροφορίες του χρήστη, όπως το όνομα, το επίθετο, την ημερομηνία και τον τόπο γέννησης του χρήστη, το φύλο του χρήστη, μια φωτογραφία του προσώπου του, έναν αριθμό διαβατηρίου (αύξοντας αριθμός για τα διαβατήρια που έχουν εκδοθεί), ένας κωδικός που να υποδεικνύει τη χώρα έκδοσης του διαβατηρίου, την ημερομηνία έκδοσης και λήξης του διαβατηρίου καθώς και την έντυπη υπογραφή του χρήστη. Η πιστοποίηση του χρήστη σύμφωνα με αυτή την αρχιτεκτονική μπορεί να πραγματοποιηθεί με δυο τρόπους. Ο ένας τρόπος είναι κατά τη διαδικασία της πιστοποίησης το σύστημα να ζητά από τον χρήστη μόνο την υποβολή του διαβατηρίου. Στη συνέχεια θα πραγματοποιείται ένας έλεγχος ταύτισης του βιομετρικού προτύπου που είναι αποθηκευμένο στο διαβατήριο και του βιομετρικού προτύπου που είναι αποθηκευμένο στη βάση του συστήματος. Αν τα δυο πρότυπα συμπίπτουν σε ένα ποσοστό πάνω από 80% τότε η πιστοποίηση θα είναι επιτυχής, αν το ποσοστό είναι μικρότερο από 80%, τότε η πιστοποίηση θα είναι ανεπιτυχής. Σε περίπτωση όμως που δεν υπάρχει και ανθρώπινος παράγοντας ώστε να ελέγξει αν το πρόσωπο στη φωτογραφία του διαβατηρίου είναι το ίδιο με αυτό που κρατά το διαβατήριο, τότε εγκυμονεί ο κίνδυνος πλαστοπροσωπίας.



Εικόνα 7.1: Μπροστά όψη διαβατηρίου



Εικόνα 7.2: Πίσω όψη διαβατηρίου

Εικόνα 7.3: Περιεχόμενο διαβατηρίου και κάρτα-διαβατήριο

Ο δεύτερος τρόπος είναι κατά τη διαδικασία πιστοποίησης του χρήστη, το σύστημα να του ζητά να υποβάλλει το χέρι και το μάτι του σε αντίστοιχους σαρωτές, καθώς και το διαβατήριό του. Οι σαρωτές θα δημιουργήσουν δυο φωτογραφίες οι οποίες θα επεξεργαστούν στη συνέχεια προκειμένου να εξαχθούν τα βιομετρικά χαρακτηριστικά της γεωμετρίας του χεριού, του δακτυλικού αποτυπώματος του δείκτη και της αγγειακής δομής του αμφιβληστροειδή. Με βάση

αυτές τις πληροφορίες θα δημιουργείται η βιομετρική υπογραφή του χρήστη. Στη συνέχεια, θα πραγματοποιηθούνε δυο έλεγχοι. Η βιομετρική υπογραφή του χρήστη θα ελεγχθεί αν ταιριάζει με το βιομετρικό πρότυπο που είναι αποθηκευμένο στο διαβατήριο αλλά και με το βιομετρικό πρότυπο που είναι αποθηκευμένο στη βάση δεδομένων του συστήματος. Με αυτό τον τρόπο παρέχεται μια πιο έγκυρη και αξιόπιστη πιστοποίηση αφού η βιομετρική ταυτότητα είναι αποθηκευμένη σε δυο διαφορετικούς χώρους. Επίσης ακόμη και στην περίπτωση μη ύπαρξης ανθρώπινου παράγοντα δεν υπάρχει κίνδυνος πλαστοπροσωπίας διότι ελέγχονται βιομετρικά χαρακτηριστικά του χρήστη.

Ένα από τα βασικά χαρακτηριστικά του συστήματος αυτού θα πρέπει επίσης να είναι και η δυνατότητα ανάκλησης του βιομετρικού προτύπου για την αποφυγή πλαστοπροσωπίας. Ο χρήστης θα πρέπει να έχει τη δυνατότητα να αλλάξει τη βιομετρική του υπογραφή είτε αλλάζοντας και τα τρία χαρακτηριστικά είτε κάποια από αυτά. Στη διαδικασία ανάκλησης της υπογραφής ο χρήστης προαιρετικά θα περάσει ξανά από τη διαδικασία εγγραφής έτσι ώστε να εξαχθούν νέα χαρακτηριστικά γνωρίσματα και να δημιουργηθεί ένα νέο βιομετρικό πρότυπο. Στην περίπτωση που ο χρήστης επιλέξει να περάσει ξανά τη διαδικασία εγγραφής, υποβάλλει το χέρι ή το μάτι του ή και τα δυο, στις αντίστοιχες συσκευές σάρωσης και μετέπειτα οι φωτογραφίες επεξεργάζονται και εξάγονται νέα χαρακτηριστικά γνωρίσματα. Στην περίπτωση που ο χρήστης επιλέξει να μην υποβληθεί ξανά στη διαδικασία εγγραφής, τότε ανακτάται η πρώτη φωτογραφία που είχε δημιουργηθεί κατά τη διαδικασία εγγραφής κάθε χαρακτηριστικού και υποβάλλεται σε επεξεργασία προκειμένου να εξαχθούν νέα χαρακτηριστικά γνωρίσματα. Στη συνέχεια δημιουργείται το νέο πρότυπο βιομετρικής υπογραφής και ενημερώνεται η βάση δεδομένων του συστήματος και φυσικά το μικροσύστημα που είναι ενσωματωμένο στο διαβατήριο.

Κεφάλαιο 8ο Βιβλιογραφία

- Frost & Sullivan, “A Best Practices Guide to Fingerprint Biometrics Ensuring a Successful Biometrics Implementation” (www.frost.com), Αποθηκεύτηκε 12/5/2012.
- SANS Institute InfoSec Reading Room, “An Exploration of Voice Biometrics”, 2004.
- Anil K. Jain, Arun Ross, Salil Prabhakar, “An Introduction to Biometric Recognition”, 2004.
- Dr. Richard Guest, “An Introduction to Biometric Standards”, University of Kent, UK.
- Davrondzhon Gafurov, “A Survey of Biometric Gait Recognition: Approaches, Security and Challenges”, 2007.
- Catherine Tilton, “BioAPI”, March 2009.
- BioAPI Consortium, “BioAPI Specification Version 1.00”, March 2000.
- Alessandro Triglia, “BioAPI 2.0 and the Biometric Interworking Protocol”, June 2005.
- Jeffrey E. Boyd and James J. Little, “Biometric Gait Recognition”, 2005.

- C. Vielhauer, R. Steinmetz, and A. Mayerhofer, “Biometric hash based on statistical features of online signatures,” in Proceedings of the International Conference on Pattern Recognition, vol. 1, pp. 123–126, Quebec, QC, Canada, August 2002.
- Ping Yan and Kevin W. Bowyer, “Biometric Recognition Using 3D Ear Shape”, 2007.
- SANS Institute InfoSec Reading Room, “Biometric Scanning Technoligies: Finger, Facial, and Retinal Scanning”, 2003.
- Anil K.Jail, Karthik Nandakumar and Abhishek Nagar, “Biometric Template Security”, December 2007
- Y.J. Chang, W. Zhang, and T. Chen, “Biometrics-based cryptographic key generation,” in Proceeding of the IEEE International Conference on Multimedia and Expo(ICME ’04), vol. 3, pp. 2203–2206, Taipei, Taiwan, June 2004.
- Bertenthal , B.I., Pinto, J.: “Complementary processes in the perception and production of human movements”. In Smith, L.B., Thelen E eds : “A Dynamic Systems Approach to Development: Applications”. MIT Press, Cambridge, MA (1993) p.209-239.
- National Science and Technology Council (NSTC), “Dynamic Signature”, 2006.
- Xyzmo SIGNificant, “Dynamic Signature Verification White Paper” (http://www.xyzmo.com/en/products/Pages/Signature-Verification.aspx).
- Gail G. Gordon, “Face Recognition Based on Depth and Carvature Features”.
- FingerTec, “FACE RECOGNITION TECHNOLOGY WHITE PAPER”, 2009.
- John M. Butler, Genetics and Genomics of Core STR Loci Used in Human Identity Testing”, 2006.
- Arun Ross, Anil Jain, “Information fusion in Biometrics”, 2003.
- BS ISO/IEC 19784-1:2006, “Information technology – Biometric application programming interface”, 2006.
- ISO/IEC JTC 1/SC 27, “Information technology – Security techniques”, 2010.
- National Science and Technology Council (NSTC), “Iris Recognition”, 2006.
- Richard P. Wildes, “Iris Recognition: An Emerging Biometric Technology”, 1997.
- SANS Institute InfoSec Reading Room, “Iris Recognition Technology for Improved Authentication”, 2002.
- Computer Science and Engineering Discipline, Khulna University, Bangladesh, “Person Identification Using Ear Biometrics”, May-August 2007.
- Rajiv Mahajan, Teenum Gupta, Sakshi Mahajan and Navneet Bawa, “Retina as Authentication Tool for Convert Channel Problem”, 2009.
- Neil Muller, Lourenco Magaia, B. M. Herbst, “Singular Value Decomposition, Eigenfaces, and 3D Reconstractions”, 2004.
- D.J. Hurley, B. Arbab-Zavar and M.S.Nixon, University of Southampton, “THE EAR AS A BIOMETRIC”, 2007.
- M.Burge and W.Burger, “Using Ear Biometrics for Passive Identification”, Austria 1998.
- Mark Burge and Wilhelm Burger, Johannes Kepler University, “13 EAR BIOMETRICS”, Austria.
- Norah Rudin, Keith Inman, Gustavo Stolovitzky, Isidore Rigoustos, “14 DNA BASED IDENTIFICATION”.
- Asker M. Bazen, “Βιομετρική απεικόνιση”.
- Μαρία Κοροδήμου, Δέσποινα Χιωτίδου, “Οπτική Ανίχνευση Εκφράσεων Προσώπου”.
- Σπυρίδων Σιάτρας, “Σύστημα Αυθεντικοποίησης Μέσω Αναγνώρισης Τρόπου Πληκτρολόγησης”, 2004.

- Χαιρέτη Όλγα, “Υλοποίηση Γραφικής Διεπαφής σε περιβάλλον MATLAB για επεξεργασία ψηφιακής εικόνας τομογραφίας ανθρώπινου δακτύλου”, 2009.
- http://www.bioapi.org/history.asp
- http://en.wikipedia.org/wiki/BioAPI
- http://en.wikipedia.org/wiki/United_States_passport