



ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ
Τμήμα Στρατιωτικών Επιστημών

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΔΙΔΡΥΜΑΤΙΚΟ ΔΙΑΤΜΗΜΑΤΙΚΟ
ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΑΚΑΔΗΜΑΪΚΟΥ ΕΤΟΥΣ 2016-17

ΣΧΕΔΙΑΣΗ & ΕΠΕΞΕΡΓΑΣΙΑ ΣΥΣΤΗΜΑΤΩΝ (SYSTEMS ENGINEERING)

(ΠΔ 96 / 2015 / ΦΕΚ 163Α' / 20.08.2014)



ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
Σχολή Μηχανικών Παραγωγής &
Διοίκησης

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

ΒΙΟΜΕΤΡΙΚΟ ΣΥΣΤΗΜΑ ΠΡΟΣΒΑΣΗΣ (BIOMETRIC ACCESS SYSTEM)

Διατριβή που υπεβλήθη για την μερική ικανοποίηση των απαιτήσεων
για την απόκτηση Μεταπτυχιακού Διπλώματος Ειδίκευσης

Υπό:

ΕΥΑΓΓΕΛΙΑ Γ. ΑΛΕΞΟΠΟΥΛΟΥ

A.M.: 2015018001

ΝΟΕΜΒΡΙΟΣ 2017

Η Μεταπτυχιακή Διατριβή της Ευαγγελίας Γ. Αλεξοπούλου εγκρίνεται:

ΤΡΙΜΕΛΗΣ ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ

Αν. Καθηγήτρια Δρ. Καρανάσιου Ειρήνη (Επιβλέπουσα) ,.....

Καθηγητής Δρ. Δάρας Νικόλαος ,.....

Καθηγητής Δρ. Κλάδης Γεώργιος ,.....

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

© Copyright υπό Ευαγγελία Γ. Αλεξοπούλου
Έτος 2017

Στην μνήμη των γονιών μου και
στο σύζυγο μου

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω την Αν. Καθηγήτρια Δρ. Καρανάσιου Ειρήνη για την εμπιστοσύνη και την υποστήριξη που έδειξε, ώστε να φέρουμε εις πέρας αυτή την εργασία, καθώς και για την άμεση ανταπόκριση σε οποιαδήποτε πρόκληση αντιμετώπισα.

Επίσης θα ήθελα να ευχαριστήσω το σύζυγο μου για την ψυχολογική υποστήριξη και την αμέτρητη κατανόηση που έδειξε όλο αυτό το χρονικό διάστημα.

ΣΕΛΙΔΑ ΣΚΟΠΙΜΑ ΚΕΝΗ

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΕΡΙΛΗΨΗ	Σελ.	1
ΕΙΣΑΓΩΓΗ		
§1. Εισαγωγικό Σημείωμα	Σελ.	2
§2. Στόχοι Εργασίας	Σελ.	2
§3. Δομή Εργασίας	Σελ.	3
ΚΕΦΑΛΑΙΟ 1		
Βιομετρία και Βιομετρικά Συστήματα		
§1. Γενικά	Σελ.	4
§2. Ιστορική Αναδρομή	Σελ.	4
§3. Ορισμοί	Σελ.	8
3.1. Τι είναι Βιομετρία	Σελ.	8
3.2. Τι είναι Ταυτοποίηση και Αυθεντικοποίηση	Σελ.	9
3.3. Πώς ορίζονται τα Βιομετρικά Χαρακτηριστικά	Σελ.	10
3.4. Τι είναι Βιομετρικό Σύστημα	Σελ.	10
ΚΕΦΑΛΑΙΟ 2		
Βιομετρικά Συστήματα και Ασφάλεια		
§1. Είδη Βιομετρικών Συστημάτων	Σελ.	11
§2. Χαρακτηριστικά Βιομετρικών Συστημάτων	Σελ.	13
2.1. Ακρίβεια	Σελ.	13
2.2. Ταχύτητα	Σελ.	14
2.3. Αξιοπιστία	Σελ.	14
2.4. Αποθήκευση Δεδομένων και Επεξεργασία	Σελ.	14
2.5. Διαδικασία Καταχώρησης	Σελ.	14
2.6. Μοναδικότητα	Σελ.	15
2.7. Παραποίηση Στοιχείων	Σελ.	15
2.8. Αποδοχή Χρήστη	Σελ.	15
§3. Πλεονεκτήματα και Μειονεκτήματα Βιομετρικών Συστημάτων	Σελ.	15
3.1. Πλεονεκτήματα	Σελ.	16
3.2. Μειονεκτήματα	Σελ.	16
§4. Μέτρηση Απόδοσης	Σελ.	17
ΚΕΦΑΛΑΙΟ 3		
Βιομετρική Αναγνώριση και Αυθεντικοποίηση		
§1. Γενικά	Σελ.	18
§2. Στάδια Βιομετρικής Αναγνώρισης ή Αυθεντικοποίησης	Σελ.	18
2.1. Εγγραφή	Σελ.	18
2.2. Ψηφιακή Αναπαράσταση	Σελ.	19
2.3. Σύγκριση	Σελ.	19
2.3.1. Πρότυπο	Σελ.	21

ΚΕΦΑΛΑΙΟ 4

Κατασκευή Βιομετρικού Συστήματος Πρόσβασης

§1. Περί ARDUINO	Σελ.	22
§2. Χρησιμοποιούμενοι Αισθητήρες	Σελ.	22
2.1. Fingerprint (Δακτυλικό Αποτύπωμα)	Σελ.	22
2.1.1. Γενικά	Σελ.	22
2.1.2. Τρόπος Λειτουργίας	Σελ.	24
2.2. Temperature Sensor (Αισθητήρας Θερμοκρασίας)	Σελ.	24
2.2.1. Γενικά	Σελ.	24
2.2.2. Τρόπος Λειτουργίας	Σελ.	25
2.3. Galvanic Skin Response (Γαλβανική Απόκριση Δέρματος)	Σελ.	25
2.3.1. Γενικά	Σελ.	25
2.3.2. Τρόπος Λειτουργίας	Σελ.	26
2.4. Heartbeat Pulse Sensor (Αισθητήρας Καρδιακού Παλμού)	Σελ.	26
2.4.1. Γενικά	Σελ.	26
2.4.2. Τρόπος Λειτουργίας	Σελ.	27
§3. Συνδεσμολογία	Σελ.	29

ΚΕΦΑΛΑΙΟ 5

Προοπτικές για το μέλλον

§1. Μελλοντική Εξέλιξη της Εργασίας	Σελ.	30
-------------------------------------	------	----

ΒΙΒΛΙΟΓΡΑΦΙΑ

	Σελ.	31
--	------	----

ΠΑΡΑΡΤΗΜΑ- ΚΩΔΙΚΕΣ

A	“Μηδενικός” Κώδικας Καταχώρησης Δακτυλικών Αποτυπωμάτων	Σελ.	34
B	Κώδικας Ταυτοποίησης Δακτυλικού Αποτυπώματος και Τοπικής Οθόνης Πληροφοριών	Σελ.	35
Γ	Κώδικας των Αισθητήρων Galvanic Skin Response, Heartbeat Pulse και Temperature	Σελ.	38
Δ	Σκαρίφημα Συνδεσμολογίας Αισθητήρων Galvanic Skin Response, Heartbeat Pulse και IR Temperature sensor	Σελ.	45
E	Σκαρίφημα Συνδεσμολογίας Αισθητήρα Fingerprint και Τοπικής Οθόνης Πληροφοριών	Σελ.	46

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διατριβή έχει ως στόχο τη δημιουργία ενός Βιομετρικού Συστήματος Πρόσβασης χρησιμοποιώντας έναν αριθμό παραμέτρων ώστε η πρόσβαση να μην επιτρέπεται εύκολα, ακόμα και από το προσωπικό που έχει καταχωρηθεί ήδη στην βάση δεδομένων. Με τις παραμέτρους που έχουμε ορίσει, ακόμη και όταν το προσωπικό κρίνεται ότι δεν είναι σε θέση να λάβει ορθές αποφάσεις, ή για κάποιο λόγο έχουν αλλάξει οι συνήθειες προθέσεις του, δεν θα δύναται να εισέλθει στον χώρο. Μια τέτοια περίπτωση αποτελεί ο πυρετός. Από μια θερμοκρασία και άνω δεν θα δύναται να εισέλθει δεδομένου ότι δημιουργούνται ακόμη και παραισθήσεις, καθώς και από μια θερμοκρασία και κάτω, που δείχνει ότι το άτομο δεν είναι εν ζωή. Άλλες παράμετροι είναι ο καρδιακός παλμός και η εφίδρωση που αποτελούν στοιχεία άγχους και εκνευρισμού.

Πιο συγκεκριμένα σκοπός μας είναι η δημιουργία ενός συστήματος ασφαλείας θυρών που να επιτρέπει όσο το δυνατόν πιο δύσκολα σε κάποιον να εισέλθει σε διαβαθμισμένο χώρο. Το σύστημα που αναπτύχθηκε περιέχει αισθητήρες όπως, Fingerprint (Δακτυλικό Αποτύπωμα), Heartbeat Pulse Sensor (Αισθητήρας Καρδιακού Παλμού), Galvanic Skin Response (Αισθητήρας Γαλβανικής Απόκρισης Δέρματος) και Temperature Sensor (Αισθητήρας Θερμοκρασίας). Η τεχνολογία στην οποία βασίστηκε η υλοποίηση είναι η πλατφόρμα ανοιχτού κώδικα ARDUINO. Οι παράμετροι που έχουμε θέσει έχουν αφενός ως σκοπό να επιβεβαιωθεί η ζωτικότητα της παλάμης από την οποία παίρνουμε μετρήσεις, λαμβάνοντας την θερμοκρασία τον καρδιακό παλμό και μετρώντας τις μικρομεταβολές στην εφίδρωση και στη συνέχεια αναζητούμε το δακτυλικό αποτύπωμα από τη βάση δεδομένων. Προς αποφυγή της χρήσης ακρωτηριασμένου δακτύλου στον αισθητήρα δακτυλικού αποτυπώματος, έχουμε τοποθετήσει τον αισθητήρα της θερμοκρασίας ακριβώς επάνω από αυτόν. Έτσι αν το δάκτυλο φέρει διαφορετική θερμοκρασία από την επιτρεπόμενη δεν τροφοδοτείται ο αισθητήρας του δακτυλικού αποτυπώματος και άρα δεν επιτρέπεται η πρόσβαση. Ο λόγος εξέτασης της κάθε μιας παραμέτρου είναι να αποφευχθεί η είσοδος ατόμου που δεν βρίσκεται σε πλήρη διαύγεια είτε λόγω αυξημένης σωματικής θερμοκρασίας είτε λόγω παράγοντα που του προκαλεί άγχος. Εκτός από την πρόσβαση μπορούμε να έχουμε εικόνα για το πόσες φορές έχει εισέλθει σε έναν χώρο ένα άτομο, καθώς και για τις ενδείξεις των μετρήσεων του για περαιτέρω επεξεργασία. Τέλος μέσα από τις μετρήσεις μπορεί να προκύψει και η φυσική κατάσταση του εισερχόμενου προσωπικού λαμβάνοντας υπόψη τον καρδιακό παλμό. Έτσι αν ο χώρος που χρησιμοποιείται απαιτεί και καλή φυσική κατάσταση μπορεί να παρατηρηθεί η μεταβολή αυτής και να ζητηθεί αντίστοιχα η λήψη μέτρων διατροφής και άσκησης.

ΕΙΣΑΓΩΓΗ

§1. ΕΙΣΑΓΩΓΙΚΟ ΣΗΜΕΙΩΜΑ

Η εξέλιξη της τεχνολογίας σε συνδυασμό με την διασφάλιση κάποιου μυστικού ή κάποιας εφευρεθείσας τεχνολογίας μας έχει οδηγήσει σε σημείο να κάνουμε κάποια μέρη πιο δύσκολα προσβάσιμα. Για να το επιτύχουμε αυτό, έχουμε αρχίσει και αναζητούμε αδιάβλητους τρόπους πιστοποίησης. Αναζητούμε λοιπόν χαρακτηριστικά τα οποία είναι μοναδικά και σε συνδυασμό με άλλες παραμέτρους [7], μας προκύπτει η εκπλήρωση συνθηκών εισόδου ή μη. Ένα αντίστοιχο μέσο πρόσβασης είναι το Βιομετρικό Σύστημα Πρόσβασης που συνδυάζει ένα αμετάβλητο στοιχείο, το δακτυλικό αποτύπωμα και άλλες παραμέτρους όπως θερμοκρασία, καρδιακό παλμό και μικρομεταβολές στην εφίδρωση.

§2. ΣΤΟΧΟΙ ΤΗΣ ΕΡΓΑΣΙΑΣ

Σε μια εποχή που τα μέτρα ασφαλείας κρίνονται απαραίτητα, ανακαλύπτονται νέοι τρόποι, κατά το δυνατόν αδιάβλητοι, προκειμένου σε κάθε χώρο να εισέρχονται αυτοί που πραγματικά επιτρέπεται και όχι αυτοί που κατάφεραν να εξαπατήσουν είτε άτομα είτε συστήματα για να εισέλθουν. Στην παρούσα εργασία σκοπός είναι η παρουσίαση ενός Βιομετρικού Συστήματος Πρόσβασης σε διαβαθμισμένο χώρο, το οποίο θα λαμβάνει ενδείξεις από θερμοκρασία, καρδιακούς παλμούς και εφίδρωση, τα οποία σε συνδυασμό με το δακτυλικό αποτύπωμα να μας δίνουν ή όχι πρόσβαση. Για να γίνει η χρήση του δακτυλικού αποτυπώματος, θα πρέπει να πληρούνται οι προϋποθέσεις της κατάλληλης θερμοκρασίας, των φυσιολογικών καρδιακών παλμών και της εφίδρωσης. Εάν μια από αυτές τις παραμέτρους δεν είναι σωστή δεν προχωράει το σύστημα στον έλεγχο του δακτυλικού αποτυπώματος. Επομένως το σύστημα αυτό δεν λαμβάνει υπόψη ένα μοναδικό δακτυλικό αποτύπωμα, αλλά και βιολογικά γνωρίσματα και φυσιολογικές μετρήσεις μέσα από τα οποία μπορούμε να αντιληφθούμε εάν το άτομο είναι σε απόλυτη ηρεμία και υγιές ή είναι αγχωμένο ή άρρωστο. Επίσης μπορούμε να ελέγξουμε πόσες φορές ένα άτομο έχει εισέλθει στο χώρο, καθώς και μπορεί να διαπιστωθεί και φυσική του κατάσταση μέσα από τις ενδείξεις του καρδιακού παλμού.

§3. ΔΟΜΗ ΤΗΣ ΕΡΓΑΣΙΑΣ

Σε αυτό το σημείο παρουσιάζονται συνολικά τα περιεχόμενα της παρούσας εργασίας, ξεκινώντας από βασικές γνώσεις για την κατανόηση των όσων αναφέρονται, και ως τελικό στάδιο την υλοποίηση του Βιομετρικού συστήματος. Αναλυτικά το περιεχόμενο κάθε κεφαλαίου παρουσιάζεται παρακάτω.

Στο πρώτο κεφάλαιο γίνεται μια εισαγωγή και ανασκόπηση της εξέλιξης των βιομετρικών συστημάτων ξεκινώντας από την αρχαία Αίγυπτο, όπου τα χρησιμοποιούσαν ως απόδειξη ότι κάποιος πληρώθηκε, και συνεχίστηκε με την χρήση των δακτυλικών αποτυπωμάτων για την εξιχνίαση εγκλημάτων. Στην συνέχεια παρουσιάζονται οι ορισμοί της βιομετρίας, της αυθεντικοποίησης και της ταυτοποίησης, των βιομετρικών χαρακτηριστικών και τέλος τα βασικά χαρακτηριστικά ενός βιομετρικού συστήματος.

Στο δεύτερο κεφάλαιο γίνεται εμβάθυνση στα βιομετρικά συστήματα και την ασφάλεια, παραθέτοντας τα είδη των βιομετρικών συστημάτων αναφορικά, τα χαρακτηριστικά τους, τα πλεονεκτήματα και μειονεκτήματα αυτών, καθώς και τον τρόπο με τον οποίο μετράται η απόδοση των συστημάτων αυτών.

Το τρίτο κεφάλαιο αναφέρεται στην ταυτοποίηση και αυθεντικοποίηση κάνοντας μια γενική εισαγωγή και στη συνέχεια γίνεται εμβάθυνση στα στάδια και στις κατηγορίες τους.

Στο τελευταίο κεφάλαιο γίνεται παρουσίαση του βιομετρικού συστήματος που αναπτύχθηκε. Περιγράφονται οι αισθητήρες που χρησιμοποιούνται, αναφέροντας κάποια γενικά στοιχεία για αυτούς, καθώς και ο τρόπος λειτουργίας και η συνδεσμολογία με τους μικροεπεξεργαστές.

Τέλος στο Παράρτημα υπάρχουν οι κώδικες που χρησιμοποιήθηκαν για την λειτουργία του Βιομετρικού Συστήματος.

ΚΕΦΑΛΑΙΟ 1

Βιομετρία και Βιομετρικά Συστήματα

§1. Γενικά

Η χρήση της Βιομετρίας ξεκινάει από τους αρχαίους χρόνους όταν χρησιμοποιήθηκε ως μέσο ταυτοποίησης των ατόμων για την μη εξαπάτηση του συστήματος πληρωμής. Με την πάροδο των χρόνων άρχισε να χρησιμοποιείται ως μέσο ταυτοποίησης αποτυπωμάτων ως τρόπο εξιχνίασης εγκλημάτων. Μέσα από αυτή τους την ανακάλυψη έγινε αντιληπτή και η μοναδικότητα αυτών των αποτυπωμάτων. Όσο άρχισε να διευρύνεται η χρήση των Βιομετρικών Συστημάτων τόσο βελτιώνονταν και οι χρησιμοποιούμενες τακτικές, όπως η ταυτοποίηση χαρακτηριστικών του προσώπου και η αναγνώριση ίριδας.

Σε αυτό το κεφάλαιο θα γίνει μια εκτενής ιστορική αναδρομή της εξέλιξης των Βιομετρικών Συστημάτων, καθώς και θα δοθούν και ορισμοί για την καλύτερη κατανόηση.

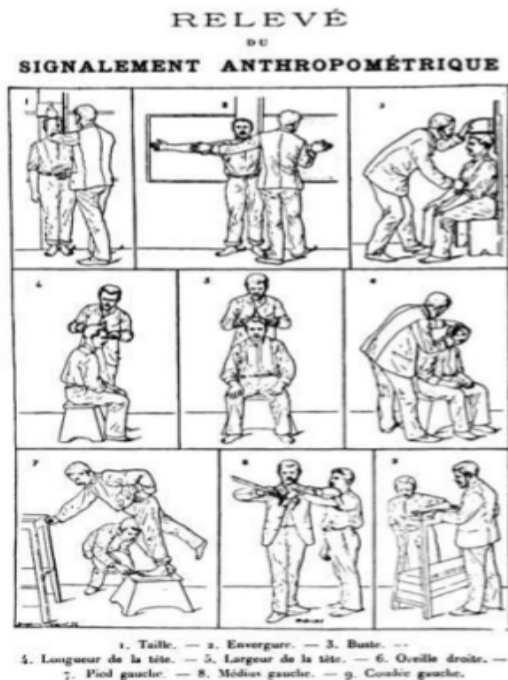
§2. Ιστορική Αναδρομή

Ένας από τους παλαιότερους και καταγεγραμμένους τρόπους αξιοποίησης των βιομετρικών χαρακτηριστικών εμφανίστηκε στην αρχαία Αίγυπτο [1], κατά τη διάρκεια κατασκευής της πυραμίδας Khufu. Οι βιομετρικές πληροφορίες που συλλέγονταν όπως ύψος, βάρος, σημάδια, παραμορφώσεις, καθώς και τα στοιχεία του χαρακτήρα όπως αγενής και οξύθυμος ήταν αυτά που εξασφάλιζαν τη μη εξαπάτηση του συστήματος πληρωμής.

Η χρήση των δακτυλικών αποτυπωμάτων ως βιομετρική ταυτοποίηση εμφανίστηκε στα τέλη του 19ου αιώνα. Η πρώτη συστηματική μελέτη στην ταυτοποίηση αποτυπωμάτων έγινε το 1893 από τον ανθρωπολόγο Francis Galton, ο οποίος απέδειξε ακόμη και τα αποτυπώματα δύο μονογενών διδύμων δεν είναι ίδια [3].

Η σωματομετρική μέτρηση των ανθρώπων με σκοπό την ταυτοποίηση έγινε το 1870 από τον Alphonse Bertillon. Μέχρι την δεκαετία του '20 χρησιμοποιούνταν για τον προσδιορισμό των φυλακισμένων με μετρήσεις από το σώμα τους, όπως τη διάμετρο του κρανίου και το μήκος βραχίονα και ποδιών, όπως φαίνεται στη Εικόνα 1. Αργότερα, ο ίδιος

ο Alphonse Bertillon [2], ως προϊστάμενος του Αστυνομικού Τμήματος στο Παρίσι, χρησιμοποίησε ένα αριθμό μετρήσεων για τον προσδιορισμό των εγκληματιών το 1883, δηλαδή επινόησε ένα ανθρωπομετρικό σύστημα, το γνωστό και ως Bertillonage. Όμως λόγω της σημαντικής ανακάλυψης του Francis Galton η ανακάλυψη του επισκιάστηκε.



Bertillonage metrics

1. Height
2. Stretch: Length of body from left shoulder to right middle finger when arm is raised
3. Bust: Length of torso from head to seat, taken when seated
4. Length of head: Crown to forehead
5. Width of head: Temple to temple
6. Length of right ear
7. Length of left foot
8. Length of left middle finger
9. Length of left cubit: Elbow to tip of middle finger
10. Width of cheeks

Εικόνα 1. Μέθοδος Bertillonage [8]

Μέσα σε 150 χρόνια η εξέλιξη των βιομετρικών συστημάτων είναι η ακόλουθη [1, 2]:

- 1858: Πρώτη συστηματική διαδικασία αναγνώρισης ατόμου μέσω του χεριού του.
- 1870: Ανάπτυξη νέας μεθόδου από τον Bertillon για αναγνώριση ατόμων μέσω ανθρωπομετρικών χαρακτηριστικών.
- 1892: Ανάπτυξη ενός νέου συστήματος κατηγοριοποίησης των δακτυλικών αποτυπωμάτων από τον Galton.
- 1894: Έκδοση ενός μυθιστορήματος του Mark Twain ("The Tragedy of Pudd'nhead Wilson"), στο οποίο αναφέρεται ένα περιστατικό, κατά το οποίο ένας κατηγορούμενος προτείνει στο δικαστήριο τη σύγκριση των δακτυλικών του αποτυπωμάτων με τα αντίστοιχα που είχαν βρεθεί στον τόπο του εγκλήματος, με σκοπό να αποδείξει την αθωότητά του.
- 1896: Ανάπτυξη νέας μεθόδου κατηγοριοποίησης των δακτυλικών αποτυπωμάτων από τον Henry.

- 1903: Ενσωμάτωση της μεθόδου των δακτυλικών αποτυπωμάτων στις φυλακές της πολιτείας της Νέας Υόρκης. Κατάρρευση της θεωρίας του Bertillon. Το λόγο για την κατάρρευση αυτή αποτελεί η εύρεση διδύμων με ίδια ανθρωπομετρικά χαρακτηριστικά.
- 1936: Πρόταση από τον οφθαλμολόγο Frank Burch για αναγνώριση ατόμου μέσω του σχεδίου της ίριδας.
- 1960: Ημι-αυτοματοποίηση της αναγνώρισης προσώπου. Δημιουργία του πρώτου μοντέλου acoustic speech (αναγνώρισης φωνής).
- 1963: Δημοσίευση μιας έρευνας του Hughes για την αυτοματοποίηση της μεθόδου των δακτυλικών αποτυπωμάτων.
- 1965: Εκκίνηση ερευνών για αναγνώριση ατόμων μέσω αναγνώρισης της υπογραφής [9].
- 1969: Άσκηση πιέσεων από το FBI, ώστε να υιοθετηθεί η μέθοδος της αναγνώρισης των ατόμων μέσω δακτυλικών αποτυπωμάτων, ως μία αυτοματοποιημένη διαδικασία.
- 1970: Προώθηση της αυτοματοποίησης της διαδικασίας της αναγνώρισης προσώπου. Μοντελοποίηση των συμπεριφορικών χαρακτηριστικών της ομιλίας.
- 1974: Διάθεση των πρώτων συστημάτων αναγνώρισης ατόμων μέσω της γεωμετρίας του χεριού, για εμπορική χρήση.
- 1975: Χρηματοδότηση από το FBI για την ανάπτυξη αισθητήρων και για την προώθηση τεχνολογιών για την εξαγωγή των χαρακτηριστικών ενδιαφέροντος των δακτυλικών αποτυπωμάτων.
- 1976: Ανάπτυξη του πρώτου πρωτότυπου συστήματος για αναγνώριση ομιλίας.
- 1977: Κατοχύρωση πατέντας για δυναμική λήψη πληροφορίας από υπογραφή.
- 1980: Ίδρυση της ομάδας για την αναγνώριση ομιλίας στο Ινστιτούτο NIST (National Institute of Standards and Technology).
- 1985: Παρουσίαση της ιδέας της μοναδικότητας της ίριδας, από τους οφθαλμολόγους Leonard Flom, Aran Safir. Κατοχύρωση πατέντας για την αναγνώριση ατόμου μέσω της γεωμετρίας της παλάμης (David Sidlauskas).
- 1986: Δημοσίευση ενός προτύπου που αφορούσε στην ανταλλαγή δεδομένων ως προς τα δακτυλικά αποτυπώματα. Κατοχύρωση πατέντας για τη χρήση της ίριδας στη διαδικασία ταυτοποίησης ατόμου (Leonard Flom, Aran Safir).
- 1988: Ανάπτυξη του πρώτου ημι-αυτοματοποιημένου μοντέλου για την αναγνώριση ατόμου μέσω του προσώπου Ανάπτυξη της τεχνικής eigenface στη μέθοδο αναγνώρισης προσώπου (L.Sirovich, M.Kirby)[10].
- 1991: Εντοπισμός του προσώπου μέσα σε μία φωτογραφία, γεγονός που καθιστά την αναγνώριση προσώπου εφικτή σε πραγματικό χρόνο (M.A. Turk, A.P. Pentland)[11].
- 1992: Ίδρυση της "Βιομετρικής Κοινοπραξίας" στους κόλπους της κυβέρνησης των Ηνωμένων Πολιτειών της Αμερικής.
- 1993: Έναρξη ερευνητικών προγραμμάτων για την καθιέρωση ενός προτύπου στο πεδίο της αναγνώρισης της ίριδας. Έναρξη του προγράμματος FERET (FacE Recognition

Technology), μέσω του οποίου κατασκευάστηκαν και τα πρώτα συστήματα αναγνώρισης προσώπου για εμπορική χρήση.

- 1994: Κατοχύρωση της πατέντας για την αναγνώριση ίριδας (Dr. John Daugman). Υιοθέτηση του INSPASS (Immigration and Naturalization Service Passenger Accelerated Service System) σε επιλεγμένα αεροδρόμια στις Ηνωμένες Πολιτείες της Αμερικής, το οποίο έκανε χρήση του βιομετρικού χαρακτηριστικού της γεωμετρίας της παλάμης.
- 1995: Διάθεση εμπορικών προϊόντων για αναγνώριση ίριδας. Εφαρμογή ετήσιας αξιολόγησης στο τμήμα αναγνώρισης ομιλίας στο NIST (National Institute of Standards and Technology).
- 1998: Υιοθέτηση από το FBI [5] της μεθόδου ταυτοποίησης ατόμου μέσω DNA για περιπτώσεις που εμπίπτουν στον τομέα της Εγκληματολογίας.
- 2000: Πραγματοποίηση ελέγχου της μεθόδου αναγνώρισης προσώπου σε ευρείας κλίμακας βάσεις δεδομένων Δημοσίευση της πρώτης επιστημονικής έρευνας με θέμα τη χρήση της κατανομής των αιμοφόρων αγγείων για ταυτοποίηση ατόμου Ίδρυση σχολής Βιομετρίας στο Πανεπιστήμιο της West Virginia.
- 2001: Χρήση της μεθόδου αναγνώρισης προσώπου σε αθλητική διοργάνωση (“Super Bowl”) στην πόλη Tampa της Florida.
- 2002: Ίδρυση της επιτροπής ISO/IEC standards για τον καθορισμό προτύπων στις βιομετρικές τεχνολογίες. Υποβολή έρευνας για την αναγνώριση ατόμου μέσω του αποτυπώματος της παλάμης του, στην Επιτροπή Υπηρεσιών Αναγνώρισης.
- 2003: Έναρξη του επίσημου συντονισμού των βιομετρικών δραστηριοτήτων στη κυβέρνηση των Ηνωμένων Πολιτειών της Αμερικής. Ενσωμάτωση των κυανοτυπιών στα ταξιδιωτικά έγγραφα από το διεθνή οργανισμό ICAO (International Civil Aviation Organization). Ίδρυση του ευρωπαϊκού οργανισμού EBF (European Biometrics Forum).
- 2004: Υιοθέτηση από το Υπουργείο Άμυνας των Ηνωμένων Πολιτειών του συστήματος ABIS (Automated Biometric Identification System). Έκδοση Προεδρικής Οδηγίας (από τον πρόεδρο G. Bush) για υποχρεωτική χρήση καρτών με σκοπό την ταυτοποίηση ατόμων μέσω βιομετρικών χαρακτηριστικών. Η Προεδρική αυτή απόφαση αφορούσε στα άτομα, τα οποία είχαν πρόσβαση σε κυβερνητικά κτίρια και συστήματα. Ευρεία χρήση στις Ηνωμένες Πολιτείες βάσεων δεδομένων με χαρακτηριστικά που αφορούν στα αποτυπώματα παλάμης. Χρηματοδότηση από την κυβέρνηση των Ηνωμένων Πολιτειών ενός θεσμού, μέσω του οποίου προωθείται η ανάπτυξη βέλτιστων αλγορίθμων για αναγνώριση προσώπου.
- 2005: Λήξη της (αμερικανικής) πατέντας για την αναγνώριση ίριδας. Ανακοίνωση των αποτελεσμάτων της έρευνας με θέμα: «ίριδα εν κινήσει» («Iris On The Move») στο συνέδριο Biometrics Consortium Conference.

§3. Ορισμοί

Σε αυτό το σημείο αναλύονται κάποιοι από τους σημαντικότερους ορισμούς που θα βοηθήσουν στην κατανόηση της εργασίας.

3.1. Τι είναι Βιομετρία

Η βιομετρία είναι μια σύνθετη λέξη που προέρχεται από την λέξη βίος και μετρώ, που σημαίνει “υπολογίζω τη ζωή”. Η επιστήμη της βιομετρίας μελετά τα βιολογικά στοιχεία ενός ατόμου μέσα από στατιστικές και μαθηματικές μεθόδους. Κάθε άτομο διαθέτει ιδιαίτερα και μοναδικά φυσικά ή βιολογικά χαρακτηριστικά. Ο κύριος στόχος της βιομετρίας είναι η ανάπτυξη μεθόδων και συνθημάτων που να πιστοποιούν την ταυτότητα του ατόμου. Ο λόγος της δημιουργίας αυτών των συστημάτων οφείλεται στο γεγονός ότι οι παραδοσιακές μέθοδοι ταυτοποίησης δεν ήταν πια επαρκείς.

Η φυσική βιομετρία μετρά και εξάγει δεδομένα από την μέτρηση μελών του σώματος όπως από ένα δάκτυλο ή ακόμη και ολόκληρη την παλάμη, την ίριδα, τον αμφιβληστροειδή χιτώνα του ματιού καθώς και το πρόσωπο.

Υπάρχουν όμως και τα βιολογικά χαρακτηριστικά όπως είναι η φωνή, η υπογραφή ακόμη και η εφίδρωση τα οποία έχουν αποτυπωθεί και ενσωματωθεί σε βιομετρικά συστήματα.

Στο αντικείμενο της Ασφάλειας, ο όρος αναφέρεται στη συλλογή και στην ανάλυση ενός ή και συνδυασμό εξωτερικών χαρακτηριστικών ενός ατόμου, καθώς και από σημάδια συμπεριφοράς. Η συλλογή και η ανάλυση αυτών των χαρακτηριστικών οδηγεί στην δημιουργία της ταυτότητας ενός ατόμου.

3.2. Τι είναι Ταυτοποίηση και Αυθεντικοποίηση

Με τον όρο ταυτοποίηση εννοούμε τη συσχέτιση ενός ατόμου με μια ταυτότητα και την επιβεβαίωση ή μη, ότι αυτή η ταυτότητα είναι αυθεντική [12].

Με τον όρο αυθεντικοποίηση εννοούμε τη διαδικασία επιβεβαίωσης της ταυτότητας ενός χρήστη [12].

Για να γίνει η ταυτοποίηση και αυθεντικοποίηση του ατόμου χρησιμοποιούνται οι ακόλουθες παραδοσιακές τεχνικές, οι οποίες είτε αποτελούν κάποιο αντικείμενο, είτε κάποιο κωδικό είτε κάποιο συγκεκριμένο χαρακτηριστικό γνώρισμα. Αυτές διακρίνονται σε [1]:

α. Κάτι που κατέχουμε: Αναφέρεται σε κάποιο φυσικό αντικείμενο, το οποίο μπορεί να είναι ένα διαβατήριο, στο οποίο η ταυτοποίηση δεν γίνεται αυτόματα και απαιτείται η ανθρώπινη παρέμβαση, ή μια μαγνητική κάρτα, με την οποία γίνεται αυτόματη ταυτοποίηση μέσω ενός συστήματος/ υπολογιστή. Η προσέγγιση αυτή είναι γνωστή ως παράγων κατοχής (possession factor).

β. Κάτι που είμαστε: Αναφέρεται στην μέτρηση ενός ή περισσότερων βιολογικών χαρακτηριστικών, όπως στα δακτυλικά αποτυπώματα και την υπογραφή. Η προσέγγιση αυτή είναι γνωστή και ως παράγων ύπαρξης (being factor).

γ. Κάτι που γνωρίζουμε: Αναφέρεται σε κάποιο “μυστικό”, το οποίο για κάθε άτομο να είναι συγκεκριμένο, όπως ένας κωδικός (PIN). Η προσέγγιση αυτή είναι γνωστή ως παράγων γνώσης (knowledge factor).

Συγκρίνοντας αυτές τις τρεις τεχνικές διαπιστώνουμε ότι οι δύο τεχνικές έχουν τρωτά σημεία. Η επιλογή ενός κωδικού ή η χρήση μιας κάρτας εισόδου εύκολα μπορεί να χαθεί, να ξεχαστεί και να αποσπαστεί. Το ίδιο όμως δεν μπορεί να γίνει στα βιομετρικά χαρακτηριστικά, διότι δεν μπορούν να πλαστογραφηθούν. Μπορούν όμως να αλλοιωθούν κάτι που μειώνει την δυνατότητα αναγνώρισης από το σύστημα.

3.3. Πώς ορίζονται τα Βιομετρικά Χαρακτηριστικά

Ως βιομετρικά χαρακτηριστικά ορίζονται όλα τα φυσικά χαρακτηριστικά ενός ατόμου, τα προσωπικά γνώρισμα, η συμπεριφορά ή οι επαναλαμβανόμενες κινήσεις που χαρακτηρίζουν ένα άτομο και μέσα από αυτά μπορούμε να το αναγνωρίσουμε [1]. Τα γνώρισμα και οι συμπεριφορές αυτές είναι μοναδικές για το καθένα άτομο και πρόκειται για χαρακτηριστικά που δεν μεταβάλλονται και μέσω αυτών είναι δυνατή η ταυτοποίηση. Τέτοια χαρακτηριστικά είναι τα γενετικά δεδομένα (DNA), τα σωματικά χαρακτηριστικά (δακτυλικά αποτυπώματα, ίριδα, γεωμετρία προσώπου) ή και στοιχεία συμπεριφοράς (βάδισμα, υπογραφή, φωνή) [2]. Παράδειγμα όμως συμπεριφοράς αποτελεί και ο τρόπος που θα πιεστεί το δάκτυλο μας πάνω στον αισθητήρα αναγνώρισης δακτυλικού αποτυπώματος [4].

3.4. Τι είναι Βιομετρικό Σύστημα

Τα Βιομετρικά Συστήματα είναι αυτά που προσδιορίζουν ή επαληθεύουν την ταυτότητα ενός ατόμου με βάση τα ανατομικά και συμπεριφοριστικά του χαρακτηριστικά [3, 6, 13]. Τα χαρακτηριστικά αυτά δεν μπορούν να μεταβληθούν, να πλαστογραφηθούν, να μοιραστούν ή να ξεχαστούν, αλλά είναι μόνιμα συνδεδεμένα με την ταυτότητα ενός ατόμου. Τα συστήματα αυτά έχουν ως προϋπόθεση την στιγμή της επαλήθευσης- ταυτοποίησης το άτομο να είναι παρόν για να απορρίψει τις ψευδείς προσβάσεις [2].

Επίσης, μόνο τα συστήματα αυτά μπορούν να αναγνωρίσουν αν ένα άτομο είναι πράγματι εγγεγραμμένο. Αν δεν αναγνωριστεί από την πλατφόρμα δεν του επιτρέπεται η πρόσβαση.

ΚΕΦΑΛΑΙΟ 2

Βιομετρικά Συστήματα και Ασφάλεια

§1. Είδη Βιομετρικών Συστημάτων

Τα Βιομετρικά Συστήματα μπορούν να χωριστούν σε δύο κατηγορίες, όπως φαίνεται και στην Εικόνα 4, που απεικονίζονται τα πιο διαδεδομένα: σε αυτά που υπακούουν στους κανόνες της φυσιολογίας και είναι μοναδικά και σε αυτά που σχετίζονται με τους ψυχολογικούς παράγοντες.

Τα μεν πρώτα είναι [1]:

- Αναγνώριση δακτυλικών αποτυπωμάτων (fingerprint verification). Εστιάζει στο δακτυλικό αποτύπωμα, το οποίο είναι μοναδικό για κάθε άτομο, ακόμη και στα μονοζυγωτικά δίδυμα και δεν αλλοιώνεται με την πάροδο του χρόνου με εξαίρεση ειδικών περιπτώσεων, όπως τα εγκαύματα ή οι δερματικές ασθένειες.
- Αναγνώριση αποτυπωμάτων παλάμης (palm print recognition). Σε αυτή τη μέθοδο γίνεται ανάλυση της υψής, των πτυχώσεων και της επιφάνειας της παλάμης, όπως φαίνεται στην Εικόνα 3.
- Αναγνώριση γεωμετρίας του χεριού (hand geometry analysis) [15]. Σε αυτή τη διαδικασία μετράται το ύψος των δακτύλων, η απόσταση μεταξύ των κλειδώσεων και το σχήμα των αρθρώσεων.
- Αναγνώριση προσώπου (facial recognition). Η διαδικασία αυτή εστιάζει στα χαρακτηριστικά του προσώπου όπως σχήμα ματιών και μέγεθος μύτης.
- Σάρωση του αμφιβληστροειδούς (retinal scan). Η μέθοδος αυτή μετά από την ίριδα αποτελεί την πιο αξιόπιστη. Επίσης είναι και η πιο παλαιά χρησιμοποιούμενη αλλά και η πιο δύσκολη. Στην σάρωση του αμφιβληστροειδούς ελέγχεται η μορφή των αγγείων, που είναι μοναδική στο καθένα άτομο.

- Αναγνώριση της ιριδας (iris recognition), όπως φαίνεται στη Εικόνα 2. Αποτελεί μια από τις πιο αξιόπιστες μεθόδους αναγνώρισης λόγω της μοναδικότητας της μορφολογίας.
- Αγγειακά σχέδια (vascular patterns). Η διαδικασία αυτή βασίζεται στο σχέδιο των φλεβών του χεριού. Αποτελεί αξιόπιστη διαδικασία διότι δεν είναι επιφανειακό χαρακτηριστικό.
- Ανάλυση γενετικού υλικού (DNA analysis). Αποτελεί μια αξιόπιστη διαδικασία αλλά παρουσιάζει ένα μειονέκτημα. Δεν μπορεί να γίνει σύγκριση του δείγματος άμεσα.
- Μέθοδος του Bertillon (Bertillonage). Είναι η παλαιότερη μέθοδος και στηρίζεται στα σωματομετρικά χαρακτηριστικά.
- Ανάλυση σωματικής οσμής (body odor analysis). Η μέθοδος αυτή βασίζεται στη χημική σύσταση του ιδρώτα, όμως βρίσκεται σε πρώιμο στάδιο.
- Αναγνώριση αυτιού(ear recognition). Αποτελεί μια από τις πιο παράξενες μεθόδους. Παρόλα αυτά αποτελεί μια από τις πιο αξιόπιστες μεθόδους και λειτουργεί παρόμοια με τα συστήματα γεωμετρίας του προσώπου και των χεριών.

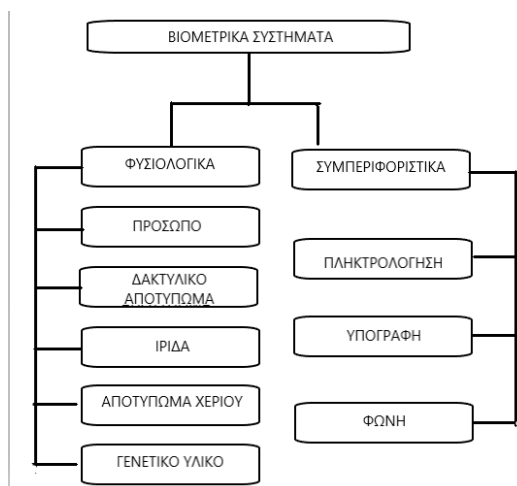


Εικόνες 2 και 3. Αναγνώρισης Ίριδας (www.frontier-security.com) και της γεωμετρίας του χεριού(www.firstsecurity.ca)

και τα δε δεύτερα είναι [1]:

- Ανάλυση βηματισμού (gait analysis). Αν και δεν αποτελεί από τις ευρέως αναπτυγμένες μεθόδους, είναι πολλά υποσχόμενη, αφού ο κάθε άνθρωπος έχει χαρακτηριστικό περπάτημα λόγω της μορφολογίας του σώματος του.
- Αναγνώριση υπογραφής (signature recognition). Σε αυτή την μέθοδο μετράται ο τρόπος , η πίεση και η ταχύτητα γραφής ενός ατόμου.

- Αναγνώριση φωνής (voice recognition), (σαν φωνή η κατάταξη της είναι στην πρώτη κατηγορία, διότι η φωνική τονικότητα είναι διαφορετική από άτομο σε άτομο. Σε αυτή την περίπτωση εστιάζουμε στον τρόπο που μιλάει το άτομο και όχι σε καθαυτή τη φωνή [2]). Σε αυτή τη μέθοδο αναγνωρίζεται η έκταση της φωνής, καθώς επίσης και η μορφή του στόματος και της ρινικής κοιλότητας.
- Ανάλυση πληκτρολόγησης (keystroke analysis). Αυτή η μέθοδος μετράει την ταχύτητα και την πίεση που ασκείται κατά την πληκτρολόγηση.



Εικόνα 4. Είδη Βιομετρικών Συστημάτων

§2. Χαρακτηριστικά Βιομετρικών Συστημάτων

Τα κύρια χαρακτηριστικά των Βιομετρικών Συστημάτων είναι αναλυτικά τα ακόλουθα [12, 15]:

2.1. Ακρίβεια

Ως ακρίβεια ορίζεται το ποσοστό αναγνώρισης ενός εξουσιοδοτημένου προσώπου από ένα μη εξουσιοδοτημένο. Η μέτρηση της ακρίβειας γίνεται με δύο μονάδες:

- α) το ποσοστό απόρριψης εξουσιοδοτημένων ατόμων και

β) το ποσοστό αποδοχής μη εξουσιοδοτημένων ατόμων.

Οι δύο αυτές μονάδες μέτρησης ρυθμίζονται ανάλογα με τις απαιτήσεις ασφαλείας. Το σημείο τομής των δυο αυτών μετρήσεων ονομάζεται Ολικό Επίπεδο Σφάλματος.

2.2. Ταχύτητα

Ως Ταχύτητα απόκρισης εννοούμε το χρονικό όριο της αναγνώρισης του ατόμου από το σύστημα.

2.3. Αξιοπιστία

Αξιοπιστία ορίζεται ως η συνεχής, ακριβής και γρήγορη λειτουργία ενός συστήματος, με τα λιγότερα έξοδα συντήρησης ή ελέγχου λειτουργίας.

2.4. Αποθήκευση Δεδομένων και Επεξεργασία

Ο χρόνος επεξεργασίας των δεδομένων ενός χρήστη επηρεάζεται από αυτά τα δυο χαρακτηριστικά. Όσο πιο χαμηλό το επίπεδο αποδοχής σφάλματος τόσο περισσότερο χρόνο έκανε για την εισαγωγή των δεδομένων και την σύγκριση με τη βάση δεδομένων. Το μέσο μέγεθος ενός αρχείου με βιομετρικά στοιχεία κυμαίνεται μεταξύ 256 και 1000 bytes.

2.5. Διαδικασία Καταχώρησης

Διαδικασία Καταχώρησης ορίζεται ως ο χρόνος που απαιτείται για την εισαγωγή των στοιχείων της ταυτότητας και του βιομετρικού χαρακτηριστικού ενός χρήστη. Στα σημερινά συστήματα δεν αποτελεί στοιχείο προς αξιολόγηση, αφού ο μέσος χρόνος καταχώρησης είναι τα δύο λεπτά.

2.6. Μοναδικότητα

Τα βιομετρικά συστήματα βασίζονται στο γεγονός ότι τα ανθρώπινα χαρακτηριστικά, είτε τα φυσικά είτε τα συμπεριφορικά, είναι μοναδικά, γεγονός που βοηθάει στην αποφυγή λαθών κατά τη διάρκεια της αναγνώρισης.

2.7. Παραποίηση Στοιχείων

Στα βιομετρικά συστήματα παίζει σημαντικό ρόλο η μη δυνατότητα εισόδου σε μη εξουσιοδοτημένο προσωπικό. Για την επίτευξη της μη εισόδου χρειάζεται μεγάλη ακρίβεια του βιομετρικού χαρακτηριστικού.

2.8. Αποδοχή του Χρήστη

Λόγω της ιδιομορφίας των δεδομένων που χρησιμοποιούνται (π.χ. δακτυλικό αποτύπωμα, ίριδα κλπ) δημιουργούνται κάποιες κοινωνικές αντιδράσεις. Η αντίδραση αυτή πηγάζει στο γεγονός της καταχώρησης ενός ατομικού του γνωρίσματος και δεδομένου ότι αυτό το χαρακτηριστικό χρησιμοποιείται, νιώθουν ότι παρακολουθούνται.

Ένας άλλος υποθετικός κίνδυνος που υπάρχει είναι με την χρήση αυτών των συστημάτων η δημιουργία κάποιας βλάβης στον οργανισμό ή η μετάδοση κάποιου νοσήματος. Κάτι τέτοιο δεν έχει όμως καταγραφεί.

§3. Πλεονεκτήματα και Μειονεκτήματα Βιομετρικών Συστημάτων

Χρησιμοποιώντας τέτοιες μεθόδους ασφαλείας, μέσω βιομετρικών συστημάτων, θα πρέπει να λάβουμε υπόψιν μας ότι διευκολύνεται η ζωή μας απαλλάσσοντάς μας από την απομνημόνευση κωδικών ή τη συνεχή σκέψη να μην ξεχάσουμε την κάρτα μας για την πρόσβαση (Εικόνα 5) [16, 17]. Μόνο με ένα σωματικό μας χαρακτηριστικό, το οποίο δεν μεταβάλλεται στο χρόνο και αποτελεί και μοναδικό στον κόσμο, έχουμε πρόσβαση στους επιτρεπόμενους χώρους. Παρόλα όμως τα θετικά υπάρχουν και αρνητικά στοιχεία όπως η απώλεια της ιδιωτικότητας. Παρακάτω θα ακολουθήσουν ενδεικτικά μειονεκτήματα και πλεονεκτήματα την βιομετρικών συστημάτων πρόσβασης [12].

3.1. Πλεονεκτήματα

- ✓ Δεν απαιτούν τη χρήση κάρτας, κωδικού πρόσβασης ή οποιαδήποτε άλλης συσκευής.
- ✓ Η αναγνώριση γίνεται με φυσικά χαρακτηριστικά και δεν απαιτείται η διαρκής ύπαρξη διαχειριστή για την ενημέρωση του συστήματος.
- ✓ Χαμηλό κόστος προμήθειας και συντήρησης.
- ✓ Χαμηλοί χρόνοι απόκρισης.
- ✓ Δεν απαιτούν διαρκή ανανέωση τα χαρακτηριστικά με την πάροδο του χρόνου.

- ✓ Σύντομη διαδικασία καταχώρησης.



Εικόνα 5. Τρόποι Εισόδου σε έναν χώρο (www.hookninja.com)

3.2. Μειονεκτήματα

- ✓ Η αντίληψη του συνόλου του κόσμου ότι η λήψη δακτυλικού αποτυπώματος συνάδει και με διάπραξη εγκληματικής ενέργειας.
- ✓ Η αντίληψη ότι η εκπεμπόμενη ακτινοβολία βλάπτει την υγεία.
- ✓ Η αντίληψη άρσης της ιδιωτικότητας

§4. Μέτρηση Απόδοσης

Δεν υπάρχει κάποιο συγκεκριμένο κριτήριο για την μέτρηση της απόδοσης, αφού για κάθε βιομετρικό χαρακτηριστικό υπάρχουν άλλα τόσα κριτήρια. Υπάρχουν κάποιοι δείκτες όπου γίνεται η μέτρηση [1, 17]:

α. Δείκτης Λανθασμένης Αποδοχής (False Acceptance Rate, FAR).

Τα αποτελέσματα εκφράζονται σε ποσοστιαία κλίμακα και δείχνουν το ποσοστό δύο διαφορετικών ατόμων να λαμβάνονται από το σύστημα ως ένα.

β. Δείκτης Λανθασμένης Απόρριψης (False Rejection Rate, FRR).

Τα αποτελέσματα εκφράζονται σε ποσοστιαία κλίμακα και δείχνουν πως δύο χαρακτηριστικά ενός ατόμου λαμβάνονται από το σύστημα ως δύο διαφορετικά άτομα.

Οι δείκτες αυτοί χρησιμοποιούνται στα συστήματα πρόσβασης έχοντας ως σκοπό την ελαχιστοποίηση της πρόσβασης στο μη αρμόδιο προσωπικό. Η σχέση αυτών των δύο δεικτών είναι αντιστρόφως ανάλογη, και αυτό φαίνεται και στο Σχήμα 1. Αυτό σημαίνει ότι

μειώνοντας τον FAR, δεν επιτρέπεται σε ένα άτομο να εισέλθει, όμως αυξάνοντας το FRR ενδέχεται ένα άτομο που του επιτρέπεται η πρόσβαση κανονικά, να χρειαστεί να γίνει λήψη αποτυπώματος παραπάνω από δυο φορές για να δημιουργηθεί το πρότυπο προς σύγκριση.

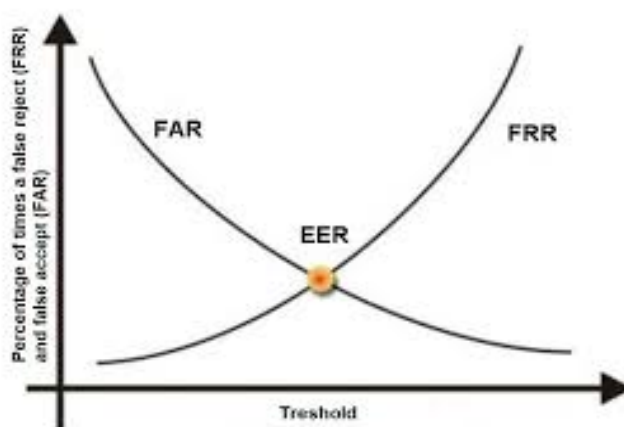
Υπάρχει και ένα ακόμη σύνολο δεικτών, το οποίο αποτελείται από τα παρακάτω:

α. Δείκτης τομής λανθασμένων εκτιμήσεων (Cross-over Error Rate, CER) ή Δείκτης ίσου σφάλματος (Equal Error Rate, EER). Τα αποτελέσματα εκφράζονται σε ποσοστιαία κλίμακα. Υπάρχει μια σύνδεση με τους προηγούμενους δύο δείκτες. Αποτελεί το σημείο τομής τους.

β. Δείκτης αποτυχίας εγγραφής (Failure to Enroll Rate, FER ή FTR). Αυτός ο δείκτης εκφράζει το ποσοστό που προσπάθησε κάποιος να εισάγει ένα πρότυπο κατά τη διαδικασία της εγγραφής. Ένας λόγος που δημιουργείται αδυναμία είναι η λήψη κακής ποιότητας προτύπου.

γ. Δείκτης αποτυχίας λήψης (Failure To Capture Rate, FTC). Μετράει την αποτυχία εντοπισμού βιομετρικού χαρακτηριστικού χωρίς να υπάρχει πρόβλημα στο εν λόγω χαρακτηριστικό.

δ. Χωρητικότητα προτύπου (template capacity). Μετράει τον μέγιστο αριθμό δεδομένων που μπορούν να εισαχθούν στο σύστημα.



Σχήμα 1. Σχεδιάγραμμα FRR, FAR και EER (www.security.stackexchange.com)

Κεφάλαιο 3

Βιομετρική Αναγνώριση και Αυθεντικοποίηση

§1. Γενικά

Ένα βιομετρικό σύστημα έχει κάποιες απαιτήσεις που θα πρέπει να ικανοποιούνται. Θα πρέπει να υπάρχουν συσκευές εισόδου και εξαγωγής χαρακτηριστικών από το αρχικό δείγμα, αποθηκευτικός χώρος με τα εξαχθέντα χαρακτηριστικά και μια διαδικασία αναγνώρισης όπου θα συγκρίνει και θα εξάγει το αποτέλεσμα.

Συνοπτικά ένα βιομετρικό σύστημα αναγνωρίζει πρότυπα που καθορίζουν το καθένα άτομο και μέσα από τη σύγκριση των δεδομένων καθορίζεται η αυθεντικότητα του. Όταν το άτομο αυτό δεν εντοπίζεται στην βάση δεδομένων απλά δεν του επιτρέπεται η πρόσβαση.

§2. Στάδια Βιομετρικής Αναγνώρισης και Αυθεντικοποίησης

Η διαδικασία της αναγνώρισης και αυθεντικοποίησης υλοποιείται σε τρία στάδια [1, 18]:

- α. Την εγγραφή
- β. Την ψηφιακή αναπαράσταση και
- γ. Την σύγκριση

2.1. Εγγραφή

Η εγγραφή είναι το βασικότερο στάδιο [19]. Σε αυτό το στάδιο αν κατά τη διάρκεια αυτής της διαδικασίας εάν δεν προσεγγιστεί ρεαλιστικά το περιβάλλον στο οποίο θα τοποθετηθεί το βιομετρικό σύστημα δεν θα είναι εφικτή και η πρόσβαση. Παραδείγματα σημαντικότητας εγγραφής είναι στις περιπτώσεις εγγραφής φωνής, όπου αλλιώς εγγράφεται η φωνή σε ένα πλήρως ήσυχο περιβάλλον και αλλιώς σε ένα περιβάλλον με θόρυβο. Αντίστοιχα και για την δική μας περίπτωση αλλιώς είναι να γίνεται η εγγραφή όταν είμαστε απόλυτα ξεκούραστοι και αλλιώς να έχει προηγηθεί ανέβασμα αριθμού σκαλιών που επηρεάζεται ο καρδιακός

παλμός και η εφίδρωση. Ακόμη θα πρέπει να συμπεριληφθεί και το γεγονός ότι με την πάροδο του χρόνου κάποια χαρακτηριστικά αλλοιώνονται επομένως η βάση δεδομένων ενδεχομένως να χρειάζεται ανά διαστήματα ενημέρωση.

2.2. Ψηφιακή Αναπαράσταση

Μετά την καταγραφή των δεδομένων, αυτά υπόκεινται σε επεξεργασία και αποθηκεύονται στη βάση δεδομένων για μελλοντική χρήση. Σκοπός αυτού του σταδίου είναι η αποθήκευση του βιομετρικού χαρακτηριστικού και όχι η διαφορετικότητα που παρουσιάζει και το διαφοροποιεί από κάποιον άλλον χρήστη. Όσον αφορά τη μνήμη του υπολογιστή και την αποθήκευση θα πρέπει να είναι σε άμεσα προσβάσιμο χώρο, για την διευκόλυνση της επεξεργασίας και της σύγκρισης.

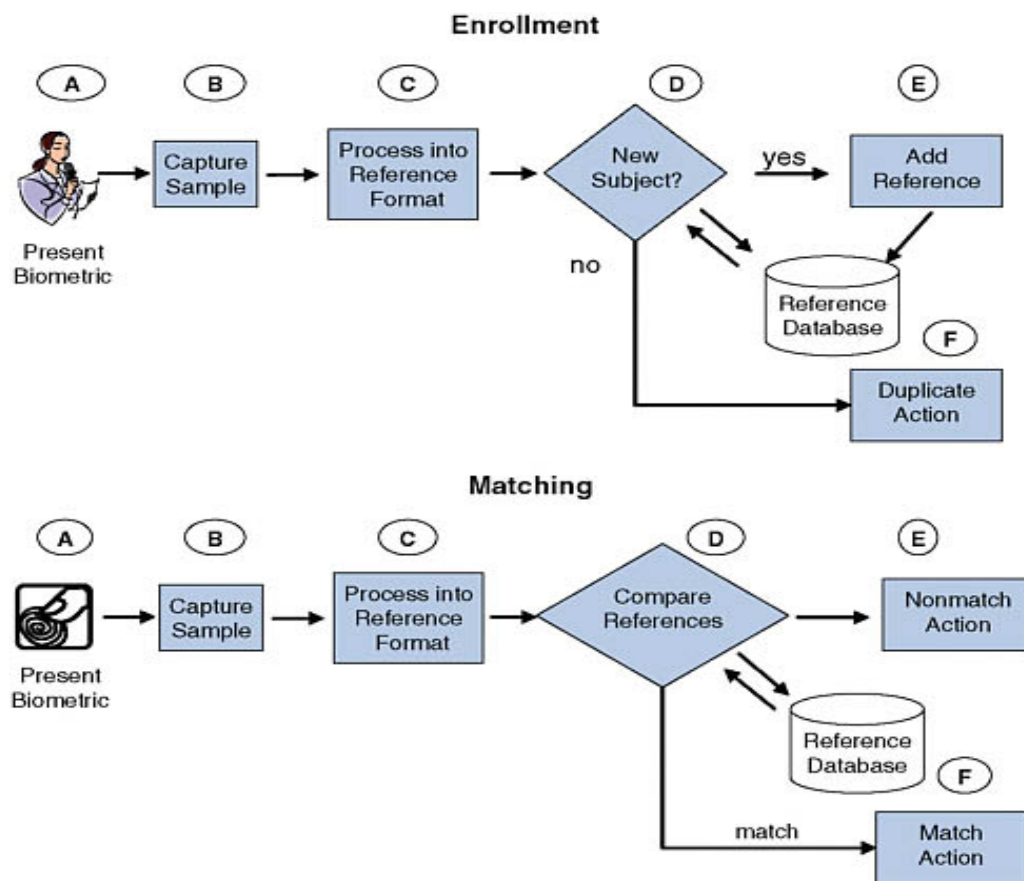
2.3. Σύγκριση

Η σύγκριση είναι το τελευταίο στάδιο της αναγνώρισης σύμφωνα με τις [4] και [19] παραπομπές. Σε αυτό το σημείο αναγνωρίζεται η δυνατότητα πρόσβασης του στο χώρο. Ως στάδιο αναγνώρισης ορίζεται εφόσον μιλάμε για σύγκριση με όλα τα αποθηκευμένα δεδομένα, και ως αυθεντικοποίησης, εφόσον μιλάμε για σύγκριση με το δείγμα που θέλουμε να ταυτιστεί.

Το απαραίτητο υλικό που χρειάζεται, για την συγκεκριμένη εργασία, είναι η ύπαρξη αισθητήρων (sensors), που θα λαμβάνει την πληροφορία από το πραγματικό σύστημα (τον άνθρωπο) και θα την μεταφέρει στο βιομετρικό. Ο ρόλος των αισθητήρων αυτών είναι να λαμβάνουν την βιομετρική πληροφορία (όπως για παράδειγμα στη δική μας περίπτωση θα υλοποιηθεί μέσω σάρωσης του δακτυλικού αποτυπώματος, την μέτρηση της θερμοκρασίας, την μέτρηση της εφίδρωσης και του καρδιακού παλμού). Στη συνέχεια αφού γίνει η συλλογή αυτών των πληροφοριών επιτελείται μια διεργασία, που ονομάζεται προ- επεξεργασία και έχει ως σκοπό την απομόνωση της βιομετρικής πληροφορίας ή τη μείωση του θορύβου.

Το επόμενο βήμα, που είναι και το πιο καθοριστικό, είναι η εξαγωγή των χαρακτηριστικών. Το σημαντικότερο στη διαδικασία αυτή είναι ότι θα πρέπει να εξαχθούν με τον καταλληλότερο τρόπο για να υπάρχει ο διαχωρισμός από κάποιο άλλο άτομο. Με την εξαγωγή έχουμε τη δημιουργία προτύπου (template), το οποίο περιλαμβάνει κωδικοποιημένα όλα τα χαρακτηριστικά που προέκυψαν από το προηγούμενο στάδιο. Στην ουσία το πρότυπο είναι αυτό που συγκρίνεται για να προκύψει ταυτοποίηση.

Επομένως, το πρότυπο μετά την εγγραφή, όπου δημιουργείται, χρησιμοποιείται κάθε φορά όπου υπάρχει κάποια σύγκριση. Για να είναι πιο γρήγορη η σάρωση της βάσης δεδομένων, υπάρχει η ανάγκη το αποθηκεύσιμο μέγεθος να είναι όσο μικρότερο γίνεται.



Εικόνα 6. Διαδικασίες Εγγραφής και Σύγκρισης (www.nap.edu)

Συνοψίζοντας, για την διαδικασία της ταυτοποίησης είναι απαραίτητο να γίνει εγγραφή του ατόμου και να δημιουργηθεί ένα πρότυπο που να αντιστοιχεί σε αυτό το άτομο. Κατά την διαδικασία της ταυτοποίησης δημιουργείται ένα νέο πρότυπο που συγκρίνεται με τα ήδη υπάρχοντα στην βάση δεδομένων. Αυτή η διαδικασία ορίζεται και ως διαδικασία αναγνώρισης. Ενώ στη διαδικασία επαλήθευσης γίνεται σύγκριση του προτύπου που δημιουργήθηκε με ένα συγκεκριμένο πρότυπο, το οποίο έχει καταχωρηθεί για το συγκεκριμένο άτομο. Η ανωτέρω διαφοροποίηση φαίνεται διαγραμματικά στην Εικόνα 6.

2.3.1 Πρότυπο

Τα πρότυπα χωρίζονται σε δύο κατηγορίες. Τα πρότυπα εγγραφής και τα πρότυπα εξακρίβωσης. Τα πρότυπα εγγραφής δημιουργούνται κατά την αρχική αλληλεπίδραση του ατόμου με το βιομετρικό σύστημα, ενώ τα πρότυπα εξακρίβωσης δημιουργούνται κατά την διάρκεια της επαλήθευσης της ταυτότητας του ατόμου. Γενικά έχουν αναπτυχθεί πολλοί αλγόριθμοι και τεχνικές για τα παραπάνω, αλλά η αναγνώριση προτύπου αποτελεί μία από τις πιο κλασσικές.

ΚΕΦΑΛΑΙΟ 4

§1. Περί ARDUINO

Το Arduino (Εικόνα 7) είναι μια απλή μητρική πλακέτα ανοιχτού κώδικα, έχοντας ενσωματωμένο έναν μικρο-ελεγκτή και άλλα εξαρτήματα, όπως εισόδους και εξόδους. Όλες οι πλακέτες περιλαμβάνουν έναν γραμμικό ρυθμιστή τάσης 5V και ένα κρυσταλλικό ταλαντωτή 16MHz. Ο τρόπος φόρτωσης του απαιτούμενου κώδικα γίνεται μέσω USB από τον Η/Υ. Ελεύθερο λειτουργικό μπορεί να μεταφορτωθεί από την διεύθυνση <http://www.arduino.cc/en/Main/Software> και να προσαρμοστεί με βάση τον τύπο ARDUINO που χρησιμοποιούμε καθώς και τα περιφερειακά στοιχεία με τα οποία έχουμε συνδέσει την πλακέτα.



Εικόνα 7. Πλακέτα ARDUINO UNO

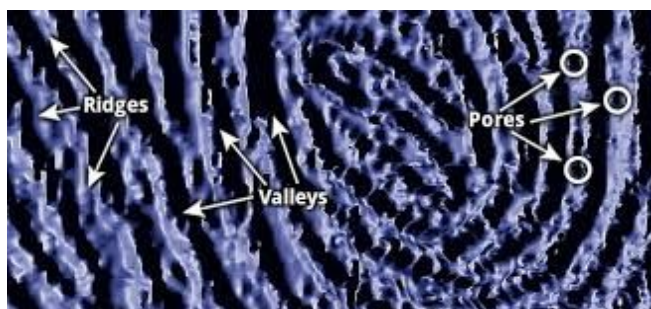
§2. Χρησιμοποιούμενοι Αισθητήρες

2.1. Fingerprint (Δακτυλικό Αποτύπωμα)

2.1.1. Γενικά

Τα δακτυλικά αποτυπώματα χαρακτηρίζονται για την μοναδικότητά τους [27], καθώς για κάθε άτομο διαφέρουν ως προς την θέση, το σχήμα και το μέγεθος [4, 14]. Τα βασικά χαρακτηριστικά των δακτυλικών αποτυπωμάτων είναι οι παρυφές (ridges) και οι κοιλάδες (valleys) [15], όπως φαίνεται στη Εικόνα 8. Σε μια απεικόνιση οι παρυφές είναι οι μαύρες

γραμμές και οι κοιλάδες οι λευκές. Οι παρυφές έχουν πάχος συνήθως 100- 300 μ m και οι κοιλάδες 200 μ m [7].



Εικόνα 8. Παρυφών και Κοιλάδων (www.ubergizmo.com)

Οι παρυφές και οι κοιλάδες είναι παράλληλες μεταξύ τους και δημιουργούν σχήματα αλλάζοντας διεύθυνση. Οι περιοχές που οι παρυφές και οι κοιλάδες σχηματίζουν ιδιαίτερα σχήματα ονομάζονται ιδιαίτερες (singular regions). Οι ιδιαίτερες περιοχές χωρίζονται σε:

α. Σημεία delta (delta points): Είναι τα σημεία που διασταυρώνονται οι παρυφές με τις κοιλάδες με τρεις διαφορετικές κατευθύνσεις με γωνία 120 μοιρών.

β. Σημεία πυρήνα (core points): Ο χαρακτηρισμός τους προκύπτει ανάλογα με την καμπυλότητα των παρυφών- κοιλάδων και διακρίνονται σε αριστερό βρόχο (left loop), δεξιό βρόχο (right loop), δακτύλιο (whorl), τόξο (arch) και τεντωμένο τόξο (tented arch).



Εικόνα 9. Αισθητήρας Fingerprint

2.1.2. Τρόπος Λειτουργίας

Ο αισθητήρας που χρησιμοποιήθηκε είναι οπτικής αναγνώρισης, όπως της Εικόνας 9, και αποτελεί το πιο διαδεδομένο είδος αισθητήρα [21]. Ο τρόπος λειτουργίας του είναι στην ουσία όπως ενός σαρωτή [29]. Τοποθετούμε το δάκτυλο μας στην γυάλινη επιφάνεια, με το που φωτιστεί το δακτυλικό αποτύπωμα λαμβάνεται η εικόνα.

Για την καταχώρηση δακτυλικών αποτυπωμάτων, χρησιμοποιήσαμε το “SFGDemo software”, το οποίο μπορεί κάποιος να το μεταφορτώσει δωρεάν από το διαδίκτυο. Ο τρόπος λειτουργίας του είναι ως εξής:

Συνδέουμε το arduino με τον αισθητήρα στο υπολογιστή. Αφού βεβαιωθούμε ότι ρευματοδοτείται, του μεταφορτώνουμε έναν “μηδενικό” κώδικα, προκειμένου να είναι δυνατή η απευθείας επικοινωνία του αισθητήρα με τον υπολογιστή, χρησιμοποιώντας την πλακέτα απλώς ως δίαυλο επικοινωνίας. Έπειτα εισερχόμαστε στο software μας και επιλέγουμε το Open Device. Αναδύεται ένα παράθυρο όπου ζητάει να διαλέξουμε τη θύρα επικοινωνίας (COM PORT). Στη συνέχεια επιλέγουμε το κουμπί Enroll για την καταγραφή του δακτυλικού αποτυπώματος με την εμφάνιση του αντίστοιχου μηνύματος από το λογισμικό, το οποίο μας δίνει σαφείς οδηγίες. Ταυτόχρονα αναδύεται ένα παράθυρο που μας ζητάει να εισάγουμε τον αριθμό καταχώρησης. Στην αριστερή πλευρά εμφανίζεται κατ’ επιλογήν η προεπισκόπηση του δακτυλικού αποτυπώματος. Τέλος το λογισμικό μας ζητάει να υλοποιήσουμε άλλη μια φορά την διαδικασία για να επιβεβαιωθεί η εγκυρότητα της ληφθείσας εικόνας. Θεωρείται αυτονόητο ότι χρησιμοποιούμε αυστηρά το ίδιο δάκτυλο. Με την ολοκλήρωση της διαδικασίας μας εμφανίζεται το μήνυμα “Success to enroll”.

2.2. Temperature Sensor (Αισθητήρας Θερμοκρασίας)

2.2.1. Γενικά

Η μέτρηση της θερμοκρασίας δεν αποτελεί σημερινή ανακάλυψη. Έχει περάσει από διάφορα στάδια, όπως τη δημιουργία θερμομέτρων είτε με υδράργυρο είτε ηλεκτρονικά πια προκειμένου να γνωρίζουμε αν στην ουσία είμαστε καλά στη υγεία μας. Ο λόγος επιλογής αυτού του αισθητήρα, καθώς και το σημείο τοποθέτησης του στο project είναι κομβικής σημασίας. Μέσα από τα αποτελέσματα που θα μας δοθούν θα διαπιστωθεί αν το δάκτυλο που εισέρχεται στο Fingerprint παρουσιάζει την κατάλληλη θερμοκρασία [20], αποκλείοντας έτσι την πιθανότητα εισόδου μη εξουσιοδοτημένου προσωπικού, με χρήση ακρωτηριασμένου άκρου.

2.2.2. Τρόπος Λειτουργίας

Ο αισθητήρας θερμοκρασίας δέρματος λειτουργεί σαν μια υπέρυθρη κάμερα. Μια θερμοπύλη (thermopile capture) καταγράφει την υπέρυθρη ενέργεια και τη μετατρέπει σε ψηφιακό σήμα που αντιπροσωπεύει τη θερμοκρασία. Η τοποθέτησή του γίνεται συνήθως σε πολύ μικρή απόσταση ή σε άμεση επαφή με το δέρμα.

Αξίζει να τονίσουμε ότι το επίπεδο της δερματικής θερμοκρασίας δεν είναι σε όλο το σώμα μας το ίδιο, αλλά εξαρτάται από το σημείο που παίρνουμε την μέτρηση [Ramanathan 1964; Venable et al. 2013] [30].

2.3. Galvanic Skin Response (Γαλβανική Απόκριση Δέρματος)

2.3.1. Γενικά

Ο αισθητήρας ηλεκτρο- δερματικής απόκρισης Galvanic Skin Response (GSR) (Εικόνα 10) στην ουσία μετρά την μεταβολή της ψυχολογικής κατάστασης του ατόμου [26]. Συγκεκριμένα μετρά τις ηλεκτρικές ιδιότητες του δέρματος. Ένα δέρμα ξηρό έχει μεγαλύτερη αντίσταση από ένα ιδρωμένο. Η μεταβολή αυτή οφείλεται στην αντίδραση των ιδρωτοποιών αδένων κατά την μεταβολή της κατάστασης. Η διακύμανση της αντοχής του δέρματος κυμαίνεται από 5kΩ έως 25kΩ [25, 28]. Ένα πείραμα που θα μπορούσε να μας δείξει αυτή την αλλαγή στην απόκριση του δέρματος είναι είτε από την απόλυτη ηρεμία να σκεφτόμαστε αρνητικές ή θετικές καταστάσεις είτε να παρατηρούμε εικόνες που προκαλούν αρνητικά – θετικά συναισθήματα. Επίσης η διατροφή μπορεί να επηρεάσει τη μέτρηση αυτής της παραμέτρου.



Εικόνα 10. Galvanic Skin Response

2.3.2 Τρόπος λειτουργίας

Το Galvanic Skin Response (GSR) αντιλαμβάνεται την ηλεκτρική συμπεριφορά (αγωγιμότητα) του δέρματος σύμφωνα με τον Nourbakhshetal (2012) [30]. Την μέτρηση της ηλεκτρο-δερματικής απόκρισης μπορούμε να την μετρήσουμε σε οποιοδήποτε σημείο του σώματος, αρκεί οι αισθητήρες GSR να βρίσκονται σε επαφή με το δέρμα. Ο αισθητήρας GSR αποτελείται από δύο ηλεκτρόδια, τα οποία τοποθετούνται σε κοντινή απόσταση (περίπου μια ίντσα). Από το ένα ηλεκτρόδιο του αισθητήρα αποστέλλεται μια μικρής έντασης ποσότητα ηλεκτρικού ρεύματος και μετράται η ένταση του ρεύματος που λαμβάνεται από το άλλο ηλεκτρόδιο. Η αγωγιμότητα μεταβάλλεται ανάλογα με την ποσότητα της υγρασίας. Το θετικό ως προς την εφίδρωση είναι ότι το άτομο, αυτόν το μηχανισμό του σώματος, δεν μπορεί κατά κανόνα να τον ελέγξει. Τέλος σύμφωνα με τον Kurniawan(2013) η απόκριση του σώματος σε ερεθίσματα άγχους, πόνου και σωματικής δραστηριότητας διαφέρει από άτομο σε άτομο.

2.4. Heartbeat Pulse Sensor (Αισθητήρας Καρδιακού Παλμού)

2.4.1. Γενικά

Ο καρδιακός παλμός αποτελεί ένα χειροπιαστό μέσο επιβεβαίωσης της ζωτικότητας [24]. Λόγω της διαφορετικότητας των οργανισμών παρατηρείται μια διαφοροποίηση ως προς τον καρδιακό παλμό. Ένας αθλητής έχει πιο χαμηλό καρδιακό παλμό από έναν όχι και τόσο σωματικά δραστήριο, όπως και ένα μωρό έχει υψηλότερο καρδιακό παλμό από ένα πιο μεγάλο παιδί [22]. Ο καρδιακός παλμός όμως επηρεάζεται και από άλλους παράγοντες όπως από τη σωματική άσκηση (ανέβασμα σκάλας) ή και από άγχος. Σκοπός μας είναι να θέσουμε ρεαλιστικά όρια στους μετρηθέντες παλμούς από τον κώδικα μας προκειμένου να επιτραπεί η πρόσβαση.



Εικόνα 11. Αισθητήρας Heartbeat Pulse Sensor

2.4.2. Τρόπος Λειτουργίας

Σύμφωνα με την παραπομπή [23] στο επάνω μέρος του αισθητήρα, όπως φαίνεται και στην Εικόνα 11, όπου τοποθετείται το δάκτυλο, υπάρχει μια στρογγυλή οπή με μια λυχνία LED. Η λυχνία αυτή φωτίζει το άκρο του δακτύλου και ένας ανιχνευτής φωτός Light Detector (LDR) από την άλλη μεριά μετράει την ένταση του φωτός που λαμβάνεται [20]. Κάθε φορά που τα αιμοσφαίρια είναι αυξημένα απορροφούν περισσότερο φως, με αποτέλεσμα τη μείωση της έντασης του φωτός που λαμβάνεται από τον LDR. Έτσι η τιμή της αντίστασης αυξάνεται και η μεταβολή αυτή μετατρέπεται σε μεταβολή τάσης [22].

§3. Συνδεσμολογία

Λόγω του εκπαιδευτικού σκοπού της εργασίας, το σύνολο της κατασκευής έχει τοποθετηθεί σε ένα πλαστικό κουτί προκειμένου να είναι εύκολο ως προς τη μεταφορά, τη χρήση, την πρόσβαση στο εσωτερικό του, αλλά και να προστατεύονται οι αισθητήρες και οι μικροεπεξεργαστές. Παρακάτω περιγράφεται ο τρόπος λειτουργίας, ενώ τα διαγράμματα της συνδεσμολογίας καθώς και οι χρησιμοποιηθέντες κώδικες βρίσκονται στα Παραρτήματα Δ' και Ε' της διατριβής.

Το σύστημα τροφοδοτείται με ρεύμα από τον Η/Υ μέσω ενός καλωδίου USB, το οποίο καταλήγει σε έναν κόμβο (hub) με τέσσερις θύρες, εκ των οποίων αξιοποιούνται οι τρεις. Η μία συνδέεται με ένα τροφοδοτικό πολλαπλών εξόδων 3.3 και 5Volt λόγω του ότι οι πλακέτες δεν έχουν υποδομή τροφοδότησης πολλών περιφερειακών ταυτόχρονα. Οι άλλες δύο θύρες συνδέονται με αντίστοιχα ARDUINO προκειμένου να τροφοδοτηθούν και να είναι δυνατή η εξωτερική σύνδεση τους με Η/Υ. Με την εκκίνηση του συστήματος, ενεργοποιούνται οι αισθητήρες των καρδιακών παλμών, της εφίδρωσης και της θερμοκρασίας. Αν οι ληφθείσες μετρήσεις είναι εντός των τεθέντων ορίων, τότε ενεργοποιείται ο ηλεκτρονόμος και τροφοδοτείται ο αισθητήρας του δακτυλικού αποτυπώματος. Εφόσον ο χρήστης είναι καταχωρημένος τότε αναγράφεται στην οθόνη το μήνυμα “Please enter room”. Σε αντίθετη περίπτωση δεν του βγάζει καμία ένδειξη.

Τα ανωτέρω αναφέρονται στην περίπτωση που ήδη είναι εγγραμμένα τα εξουσιοδοτημένα άτομα. Η καταχώρηση νέων μελών απαιτεί μια διαφοροποίηση του κυκλώματος, διότι η αποθήκευση των δακτυλικών αποτυπωμάτων γίνεται απευθείας στον αισθητήρα. Ο αισθητήρας έχει τη δυνατότητα αποθήκευσης 162 αποτυπωμάτων. Για την υλοποίηση της εγγραφής απαιτείται η μετακίνηση δύο εξωτερικών διακοπών προς τα κάτω (βρίσκονται

εξωτερικά και επάνω από το καλώδιο της τροφοδοσίας) προκειμένου να τροφοδοτείται μόνιμα ο αισθητήρας δακτυλικού αποτυπώματος με ρεύμα και να μην αναμένει την ενεργοποίηση του ρελέ, ενώ με τον δεύτερο διακόπτη, αλλάζει η συνδεσμολογία ανταλλαγής δεδομένων μεταξύ ARDUINO και Η/Υ από “λειτουργία ελέγχου πρόσβασης” σε “λειτουργία καταχώρησης αποτυπωμάτων”. Η εν λόγω διάταξη επιλέχθηκε προκειμένου να απαιτείται η παρέμβαση με χρήση Η/Υ για να καταχωρηθούν νέα αποτυπώματα κάτι που (ενώ θα μπορούσε να υπάρχει η δυνατότητα) δεν επιτρέπεται να γίνει αυτόνομα από την κονσόλα. Κατά την εκκίνηση του συστήματος θα πρέπει να γίνεται χρήση του διακόπτη που τροφοδοτεί μόνιμα τον αισθητήρα αποτυπώματος, προκειμένου η σε αυτόν συνδεδεμένη πλακέτα να τον εντοπίσει άπαξ και εν συνεχεία να μεταπέσει στη “λειτουργία ελέγχου πρόσβασης”.

ΚΕΦΑΛΑΙΟ 5

Προοπτικές για το μέλλον

§1. Μελλοντική Εξέλιξη της Εργασίας

Κατά τη διάρκεια υλοποίησης της εργασίας παρουσιάστηκαν κάποια προβλήματα, τα οποία είχαν ως αποτέλεσμα, την απόκλιση από τον αρχικό σχεδιασμό του συστήματος. Ενώ ο καθένας αισθητήρας μόνος του λειτουργούσε σωστά, αν ήταν συνδεδεμένος κατά μόνος σε μια πλακέτα Arduino, η προσπάθεια διασύνδεσης και των τεσσάρων ταυτόχρονα σε μια, απέβη άκαρπη. Επομένως μετά από διερεύνηση [31, 32] επιλέχθηκε η δυνατότητα να λειτουργούν ταυτόχρονα τρεις αισθητήρες συνδεδεμένοι σε μια πλατφόρμα και στη συνέχεια να ενεργοποιείται μέσω ηλεκτρονόμου, ο αισθητήρας του δακτυλικού αποτυπώματος, ο οποίος είναι συνδεδεμένος στη δεύτερη πλατφόρμα. Με την διαφοροποίηση αυτή, λόγω χρήσης δύο Arduino, αντί ενός που ήταν η αρχική σκέψη, δημιουργήθηκε η δυνατότητα να προσαρμοστούν και άλλοι αισθητήρες, εν σειρά ή εν παραλλήλω στο ήδη υπάρχον σύστημα, με χρήση ηλεκτρονικών .

Μια ενδεχόμενη δυνατότητα είναι η προσαρμογή επιπλέον αισθητήρων δακτυλικού αποτυπώματος, έτσι ώστε να γίνει ακόμη πιο αδιάβλητο το σύστημα, αφού θα λαμβάνει δακτυλικά αποτυπώματα από όσα δάκτυλα χεριού επιθυμούμε. Ως εκ τούτου και με τη δυνατότητα να μετράται ταυτόχρονα η θερμοκρασία (στο πλαίσιο ελέγχου ζωτικότητας) σε όλα τα ελεγχόμενα δάκτυλα, τετραπλασιάζεται η ασφάλεια εισόδου σε διαβαθμισμένο χώρο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Γεροντίδης Ευγένιος (2012), Βιομετρικά Συστήματα Ασφαλείας. Τεχνικές Υλοποίησης και Εφαρμογές τους, pp.7-29, Πτυχιακή Εργασία.
- [2] Αραμπατζής Νίκος (2014),Ειδικά Θέματα Ασφαλείας Πληροφοριών- Βιομετρικά Συστήματα, pp.12-21, Πτυχιακή Εργασία.
- [3] Abhishek Nagar (2012), Biometric Template Security, pp. 1-6.
- [4] Τσέλιος Κωνσταντίνος (2008), Σχεδιασμός και ανάπτυξη συστήματος βιομετρικής αναγνώρισης βασισμένο στα δακτυλικά αποτυπώματα, pp. 1-15, Ειδική Επιστημονική Εργασία.
- [5] Αναστασία Ν. Ουζούνoglou (2011), Αυτόματη Ταυτοποίηση Βιομετρικών Χαρακτηριστικών: Εφαρμογή στα Δακτυλικά Αποτυπώματα, pp. 20- 26, Διδακτορική Διατριβή.
- [6] Ling Hong (1998), Automatic Personal Identification Using Fingerprints, pp.10, 15, 22- 47, Doctor of Philosophy.
- [7] Ψαράγκας Απόστολος (2013), Εξακρίβωση Δακτυλικών Αποτυπωμάτων Μέσω Η/Υ, pp. 14- 22, Πτυχιακή Εργασία.
- [8] Bertillonage Metrics, www.slideshare.net/migod/software-bertillonage-finding-the-provenance-of-an-entity.
- [9] J. Mauceri (1965), Feasibility Studies of Personal Identification by Signature Verification, Space and Information System Division, North American Aviation Co., Anaheim, USA.
- [10] L. Sirovich and M. Kirby (1987), Low-Dimensional Procedure for the Characterization of Human Faces, Journal of the Optical Society of America, pp. 519-524.

- [11] M. Turk and A. Pentland (1991), Eigenfaces for Recognition, Journal of Cognitive Neuroscience, vol. 3, no. 1, pp. 71-86, hard copy.
- [12] Σφυράκης Παναγιώτης (2008), Η Χρήση των Βιομετρικών Συστημάτων ως Μέσο Προστασίας των Πολιτών και των Πληροφοριών. Η Αναγκαιότητα Αποδοχής από τους Πολίτες, pp.8-12 και 22-27, Πτυχιακή Εργασία.
- [13] Karthik Nandakumar (2005), Integration of Multiple Cues in Biometric Systems, pp.1-12, Master of Science.
- [14] Arun Abraham Ross (2003), Information Fusion in Fingerprint Authentication, pp. 1-13, Doctor of Philosophy.
- [15] Tiago Duarte, Joao Paulo Pimentao, Pedro Sousa, Sergio Onofre, Biometric Control Access Systems: A Review on technologies to improve their efficiency, Paper.
- [16] Αντώνογλου Ι. Δημήτριος (2012), Βιομετρική και Εφαρμογές, pp.10-15, Διπλωματική Εργασία Μεταπτυχιακού Διπλώματος Ειδίκευσης.
- [17] Bill Spence, Biometrics In Physical Access Control Issues, Status and Trends, Recognition Systems, Inc.
- [18] Πάντος Λαέρτης, Μελέτη, Σχεδίαση και Ανάπτυξη Εφαρμογής Λογισμικού για τον Έλεγχο της Εισόδου σε Προστατευόμενο Χώρο με τη Βοήθεια του Προσώπου και του Δακτυλικού Αποτυπώματος, pp.9-11 και 33-37, Πτυχιακή Εργασία.
- [19] Omar Abdulwahabe Mohamad, Rasha Talal Hameed and Nicolae Țăpuș (2014), Access Control Using Biometrics Features with Arduino Galileo, Research Paper, www.ijarcsse.com.
- [20] Martin Drahanský (2011), Advanced Biometric Technologies, pp.180-194, Brno University of Technology, Faculty of Information Technology, Czech Republic.
- [21] Emanuela Marasco and Arun Ross (2014), A Survey on Anti-Spoofing Schemes for Fingerprint Recognition Systems, ACM Computing Surveys, Vol.47, No.2, Article A.

- [22] Mohammad Wajih Alam, Tanin Sultana and Mohammad Sami Alam(2016), A Heartbeat and Temperature Measuring System for Remote Health Monitoring using Wireless Body Area Network, Article in International Journal of Bio- Technology.
- [23] Pulse Sensor Getting Started Guide, www.media.digikey.com/pdf/Data%20Sheets/Pulse%20PDFs/PulseSensorAmpedGettingStartedGuide.pdf.
- [24] Bandana Mallick and Ajit Kumar Patro (2016), Heart Rate Monitoring System Using Finger Tip Through Arduino and Processing Software, International Journal of Science, Engineering and Technology Research, Vol.5 .
- [25] Jan Peuscher (2012), Galvanic Skin Response (GSR), TMSi.
- [27] Mouad. M. H. Ali and A. T. Gaikwad (2016), Multimodal Biometrics Enhancement Recognition System based on Fusion of Fingerprint and Palm Print: A Review, Vol.16, Global Journals Inc.
- [29] Lady Ada (2016), Adafruit Optical Fingerprint Sensor, Guide, www.learn.adafruit.com/adafruit-optical-fingerprint-sensor
- [30] Jorge Blasco, Thomas M. Chena, Juan Taplador and Pedro Peris-Lopez (2016), Survey of Wearable Biometric Recognition Systems, Article in ACM Computing Surveys.
- [26] María Viqueira Villarejo, Begoña García Zapirain and Amaia Méndez Zorrilla (2012), A Stress Sensor Based on Galvanic Skin Response (GSR) Controlled by ZigBee, Article, www.mdpi.com/journal/sensors.
- [28] P. A. Vijaya and G. Shivakumar (2013), Galvanic Skin Response: A Physiological Sensor System for Affective Computing, International Journal of Machine and Computing, Vol.3, No.1, Paper.
- Ιστότοποι
- [31] Ιστοσελίδα <https://www.arduino.cc/>
- [32] Ιστοσελίδα <https://www.instructables.com/>

ΠΑΡΑΡΤΗΜΑΤΑ

ΠΑΡΑΡΤΗΜΑ Α΄

[31, 32]

“Μηδενικός” Κώδικας Καταχώρησης Δακτυλικών Αποτυπωμάτων

```
//GREEN PIN->D1 WHITE PIN->D0  
//RED PIN->5V BLACK PIN->GND  
//ΜΕΤΑ ΤΗ ΜΕΤΑΦΟΡΤΩΣΗ ΤΟΥ ΚΩΔΙΚΑ ΩΣ ΚΑΤΩΘΙ, ΤΡΕΧΟΥΜΕ ΤΟ SFGDemo  
//OPEN DEVICE (ΕΠΙΛΕΓΟΥΜΕ ΤΗ ΘΥΡΑ COM ΠΟΥ ΕΧΟΥΜΕ ΣΥΝΔΕΣΕΙ ΤΟ ARDUINO-  
//ΠΡΟΣΟΧΗ ΝΑ ΕΧΟΥΜΕ ΑΠΕΝΕΡΓΟΟΠΗΣΕΙ ΤΟ ARDUINO ΙΔΕ ΓΙΑ ΝΑ ΜΗΝ ΦΑΙΝΕΤΑΙ Η  
//ΘΥΡΑ ΑΠΑΣΧΟΛΗΜΕΝΗ).ΑΝ ΟΛΑ ΕΙΝΑΙ ΟΚ ΘΑ ΔΟΥΜΕ ΤΗΝ ΕΝΔΕΙΞΗ "Open Device Success!"  
//ΣΤΟ ΠΕΔΙΟ ENROLL ΕΠΙΛΕΓΟΥΜΕ ΤΟ PREVIEW ΚΑΙ ΠΑΤΑΜΕ ENROLL ΑΚΟΛΟΥΘΩΝΤΑΣ ΤΙΣ ΟΔΗΓΙΕΣ.  
//Η ΕΠΙΛΟΓΗ Con Enroll ΜΑΣ ΕΠΙΤΡΕΠΕΙ ΝΑ ΚΑΤΑΧΩΡΟΥΜΕ ΣΥΝΕΧΟΜΕΝΑ (CONtinuous) ΑΠΟΤΥΠΩΜΑΤΑ.  
//Ο ΣΕΝΣΟΡΑΣ ΔΥΝΑΤΑΙ ΝΑ ΑΠΟΘΗΚΕΥΣΕΙ ΜΕΧΡΙ 162 ΑΠΟΤΥΠΩΜΑΤΑ.  
void setup() {}  
void loop() {}
```

ΠΑΡΑΡΤΗΜΑ Β'

[31,32]

Κώδικας Ταυτοποίησης Δακτυλικού Αποτυπώματος και Τοπικής Οθόνης Πληροφοριών

```
//ΣΥΝΔΕΣΜΟΛΟΓΙΑ
//ΑΙΣΘΗΤΗΡΑΣ ΔΑΚΤΥΛΙΚΟΥ ΑΠΟΤΥΠΩΜΑΤΟΣ
//ΠΡΑΣΙΝΟ PIN->D2 (ΕΙΣΟΔΟΣ ΑΠΟ ΣΕΝΣΟΡΑ) ΛΕΥΚΟ PIN->D3 (ΕΞΟΔΟΣ ΠΡΟΣ ΣΕΝΣΟΡΑ)
//VCC->5V GND->GND
//ΟΘΟΝΗ LCD I2C
//SDA->A4 SCL->A5 VCC->5V GND->GND
////////////////////////////////////
//ΑΠΑΙΤΟΥΜΕΝΕΣ ΒΙΒΛΙΟΘΗΚΕΣ
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <LCD.h>
#include <LiquidCrystal_I2C.h>
////////////////////////////////////
int getFingerprintIDez();

SoftwareSerial mySerial(2, 3);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
////////////////////////////////////
LiquidCrystal_I2C lcd(0x3F, 2, 1, 0, 4, 5, 6, 7, 3, POSITIVE);
// Addr, En, Rw, Rs, d4, d5, d6, d7, backlightpin, polarity
//ΠΡΙΝ ΤΗΝ ΣΥΝΔΕΣΗ ΤΗΣ ΟΘΟΝΗΣ ΑΠΑΙΤΕΙΤΑΙ Η ΕΥΡΕΣΗ ΤΗΣ ΔΙΕΥΘΥΝΣΕΩΣ ΤΗΣ(ΕΔΩ 0x3F)ΜΕΣΩ ΣΧΕΤΙΚΟΥ
ΚΩΔΙΚΑ
////////////////////////////////////
void setup()
{
  lcd.begin(20, 4);
  lcd.backlight();
  lcd.clear();
  lcd.setCursor(6, 0);
  lcd.print("BIOMETRIC");
  lcd.setCursor(4, 1);
```

```

lcd.print("ACCESS SYSTEM");
lcd.setCursor(9, 2);
lcd.print("BY");
lcd.setCursor(0, 3);
lcd.print("ALEXΟΡΟΥΛΟΥ ΕΥΑΓΕΛΙΑ");
delay(5000);
lcd.clear();
lcd.print("Checking fingerprint");
delay(1000);
while (!Serial);
Serial.begin(9600);
Serial.println("CHECKING CONNECTIVITY WITH SENSOR");
finger.begin(57600); // ΡΥΘΜΟΣ ΑΝΤΑΛΛΑΓΗΣ ΔΕΔΟΜΕΝΩΝ ΜΕ ΑΙΣΘΗΤΗΡΑ ΔΑΚΤΥΛΙΚΟΥ
ΑΠΟΤΥΠΩΜΑΤΟΣ
if (finger.verifyPassword())
{
  Serial.println("FINGERPRINT SENSOR DETECTED !!!");
} else
{
  Serial.println("FINGERPRINT SENSOR NOT DETECTED !!!");
  while (1);
}
Serial.println("WAITING FOR ENROLLED FINGERPRINT...");
}
////////////////////////////////////
void loop()
{
  getFingerprintIDez();
  delay(50);
}
////////////////////////////////////
// ΕΠΙΣΤΡΕΦΕΙ -1 ΕΑΝ Η ΤΑΥΤΟΠΟΙΗΣΗ ΑΠΟΤΥΧΕΙ, ΕΙΔΑΛΛΩΣ ΕΠΙΣΤΡΕΦΕΙ
//ΤΗΝ ΤΑΥΤΟΤΗΤΑ ΤΟΥ ΧΡΗΣΤΗ --> ID #
int getFingerprintIDez()
{
  uint8_t p = finger.getImage();
  if (p != FINGERPRINT_OK) return -1;

  p = finger.image2Tz();

```

```
if (p != FINGERPRINT_OK) return -1;

p = finger.fingerFastSearch();
if (p != FINGERPRINT_OK) return -1;

// found a match!
Serial.print("FOUND USER No "); Serial.print(finger.fingerID);
Serial.print(" WITH CREDIBILITY OF "); Serial.println(finger.confidence);
Serial.print(" PLEASE ENTER ROOM ");
lcd.clear();
lcd.print("Please Enter Room");
delay(2000);
lcd.clear();
return finger.fingerID;
}
```

ΠΑΡΑΡΤΗΜΑ Γ'

[31, 32]

Κώδικας των Αισθητήρων Galvanic Skin Response, Heartbeat Pulse και Temperature

```
//ΣΥΝΔΕΣΜΟΛΟΓΙΑ
//ΑΙΣΘΗΤΗΡΑΣ IR TEMP
//PINS SDA->A4 SCL->A5 VCC->5V GND->GND
//GALVANIC SKIN RESPONSE
//GND->GND VCC->5V SIG->A2 LED->D13
//ΑΙΣΘΗΤΗΡΑΣ ΠΑΛΜΩΝ
//PINS GND->GND VCC->5V SIG->A0
////////////////////////////////////
// Volatile Variables, used in the interrupt service routine!
volatile int BPM;           // int that holds raw Analog in 0. updated every 2mS
volatile int Signal;        // holds the incoming raw data
volatile int IBI = 600;     // int that holds the time interval between beats! Must be seeded!
volatile boolean Pulse = false; // "True" when User's live heartbeat is detected. "False" when not a "live
                             // beat".
volatile boolean QS = false; // becomes true when Arduino finds a beat.

// Regards Serial OutPut -- Set This Up to your needs
static boolean serialVisual = true; // Set to 'false' by Default. Re-set to 'true' to see Arduino Serial Monitor
ASCII Visual Pulse

volatile int rate[10];      // array to hold last ten IBI values
volatile unsigned long sampleCounter = 0; // used to determine pulse timing
volatile unsigned long lastBeatTime = 0;  // used to find IBI
volatile int P = 512;       // used to find peak in pulse wave, seeded
volatile int T = 512;       // used to find trough in pulse wave, seeded
volatile int thresh = 525;  // used to find instant moment of heart beat, seeded
volatile int amp = 100;     // used to hold amplitude of pulse waveform, seeded
volatile boolean firstBeat = true; // used to seed rate array so we startup with reasonable BPM
volatile boolean secondBeat = false; // used to seed rate array so we startup with reasonable BPM
```



```
////////////////////////////////////

//ΑΠΑΙΤΟΥΜΕΝΕΣ ΒΙΒΛΙΟΘΗΚΕΣ
#include <Wire.h>
#include <Adafruit_MLX90614.h>
////////////////////////////////////
const int GSR = A2;
int threshold = 0;
int sensorValue;
int pulsePin = 0; // ΜΩΒ ΚΑΛΩΔΙΟ ΑΙΣΘΗΤΗΡΑ ΠΑΛΜΩΝ->Α0
int ledPin = 8; // ΚΑΘΟΡΙΣΜΟΣ PIN ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΗΛΕΚΤΡΟΝΟΜΟΥ

Adafruit_MLX90614 mlx = Adafruit_MLX90614();
////////////////////////////////////
void setup() {
  setup1();
  setup2();
  setup3();
  setup4();
}
void setup1()
{
  Serial.begin(9600);
  pinMode(ledPin, OUTPUT);
}
void setup2() {
  mlx.begin();
}
void setup3()
{
  interruptSetup(); // sets up to read Pulse Sensor signal every 2mS
}
void setup4()
{
  long sum = 0;
  for (int i = 0; i < 500; i++)
  {
    sensorValue = analogRead(GSR);
    sum += sensorValue;
  }
}
```

```
    delay(5);
  }
  threshold = sum / 500;
  Serial.print("threshold =");
  Serial.println(threshold);
}
////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////////
void loop() {
  delay(5000);
  //AFORA PULSE
  serialOutput();
  if (QS == true) // A Heartbeat Was Found
  {
    // BPM and IBI have been Determined
    // Quantified Self "QS" true when arduino finds a heartbeat
    serialOutputWhenBeatHappens(); // A Beat Happened, Output that to serial.
    QS = false; // reset the Quantified Self flag for next time
  }
  //AFORA IRTEMP
  Serial.print("FINGER TEMPERATURE = ");
  Serial.print(mlx.readObjectTempC());
  Serial.println("*C");
  //AFORA GSR
  int temp;
  sensorValue = analogRead(GSR);
  Serial.print("sensorValue=");
  Serial.println(sensorValue);
  temp = threshold - sensorValue;
  if (abs(temp) > 60)
  {
    sensorValue = analogRead(GSR);
    temp = threshold - sensorValue;
    if (abs(temp) > 60) //default 60
    {
      Serial.println("Emotion Changes Detected!");
    }
  }
  Serial.println(" ");
  delay(1000);
}
```

```
if (QS == true //ΑΝ ΕΝΤΟΠΙΣΤΟΥΝ ΠΑΛΜΟΙ
and BPM<120 //ΚΑΙ ΑΝ ΟΙ ΠΑΛΜΟΙ ΕΙΝΑΙ ΚΑΤΩ ΑΠΟ 120
and BPM>60 //ΚΑΙ ΑΝ ΟΙ ΠΑΛΜΟΙ ΕΙΝΑΙ >60
and mlx.readObjectTempC() > 28 //ΚΑΙ ΑΝ Η ΘΕΡΜΟΚΡΑΣΙΑ ΤΟΥ ΔΕΙΚΤΗ ΕΙΝΑΙ >28
and mlx.readObjectTempC() < 37 //ΚΑΙ ΑΝ Η ΘΕΡΜΟΚΡΑΣΙΑ ΤΟΥ ΔΕΙΚΤΗ ΕΙΝΑΙ <37
and (abs(temp) < 65)) //ΚΑΙ ΕΑΝ ΔΕΝ ΕΝΤΟΠΙΣΤΕΙ ΣΥΝΑΙΣΘΗΜΑΤΙΚΗ ΜΕΤΑΒΟΛΗ
digitalWrite(ledPin, HIGH); //ΔΩΣΕ ΤΑΣΗ ΣΤΟ PIN 8
else digitalWrite(ledPin, LOW); //ΑΛΛΙΩΣ ΜΗΝ ΔΩΣΕΙΣ ΤΑΣΗ ΣΤΟ PIN 8
}
////////////////////////////////////
void interruptSetup()
{
    // Initializes Timer2 to throw an interrupt every 2mS.
    TCCR2A = 0x02; // DISABLE PWM ON DIGITAL PINS 3 AND 11, AND GO INTO CTC MODE
    TCCR2B = 0x06; // DON'T FORCE COMPARE, 256 PRESCALER
    OCR2A = 0x7C; // SET THE TOP OF THE COUNT TO 124 FOR 500Hz SAMPLE RATE
    TIMSK2 = 0x02; // ENABLE INTERRUPT ON MATCH BETWEEN TIMER2 AND OCR2A
    sei(); // MAKE SURE GLOBAL INTERRUPTS ARE ENABLED
}
////////////////////////////////////
void serialOutput()
{ // Decide How To Output Serial.
    if (serialVisual == true)
    {
        arduinoSerialMonitorVisual('-', Signal); // goes to function that makes Serial Monitor Visualizer
    }
    else
    {
        sendDataToSerial('S', Signal); // goes to sendDataToSerial function
    }
}
////////////////////////////////////
void serialOutputWhenBeatHappens()
{
    if (serialVisual == true) // Code to Make the Serial Monitor Visualizer Work
    {
        Serial.print("*** Heart-Beat Detected *** ");
        Serial.print("BPM: ");
    }
}
```

```

    Serial.println(BPM);
}
else
{
    sendDataToSerial('B', BPM); // send heart rate with a 'B' prefix
    sendDataToSerial('Q', IBI); // send time between beats with a 'Q' prefix
}
}
////////////////////////////////////
void arduinoSerialMonitorVisual(char symbol, int data )
{
    const int sensorMin = 0;    // sensor minimum, discovered through experiment
    const int sensorMax = 1024; // sensor maximum, discovered through experiment
    int sensorReading = data; // map the sensor range to a range of 12 options:
    int range = map(sensorReading, sensorMin, sensorMax, 0, 11);
    // do something different depending on the
    // range value:
    switch (range);

}
////////////////////////////////////
void sendDataToSerial(char symbol, int data )
{
    Serial.print(symbol);
    Serial.println(data);
}
////////////////////////////////////
ISR(TIMER2_COMPA_vect) //triggered when Timer2 counts to 124
{
    cli();                // disable interrupts while we do this
    Signal = analogRead(pulsePin);    // read the Pulse Sensor
    sampleCounter += 2;        // keep track of the time in mS with this variable
    int N = sampleCounter - lastBeatTime;    // monitor the time since the last beat to avoid noise
    // find the peak and trough of the pulse wave
    if (Signal < thresh && N > (IBI / 5) * 3) // avoid dichrotic noise by waiting 3/5 of last IBI
    {
        if (Signal < T) // T is the trough
        {
            T = Signal; // keep track of lowest point in pulse wave
        }
    }
}

```

```
}  
}  
  
if (Signal > thresh && Signal > P)  
{ // thresh condition helps avoid noise  
  P = Signal;           // P is the peak  
}                       // keep track of highest point in pulse wave  
  
// NOW IT'S TIME TO LOOK FOR THE HEART BEAT  
// signal surges up in value every time there is a pulse  
if (N > 250)  
{ // avoid high frequency noise  
  if ( (Signal > thresh) && (Pulse == false) && (N > (IBI / 5) * 3) )  
  {  
    Pulse = true;           // set the Pulse flag when we think there is a pulse  
    IBI = sampleCounter - lastBeatTime; // measure time between beats in mS  
    lastBeatTime = sampleCounter;      // keep track of time for next pulse  
  
    if (secondBeat)  
    { // if this is the second beat, if secondBeat == TRUE  
      secondBeat = false;           // clear secondBeat flag  
      for (int i = 0; i <= 9; i++) // seed the running total to get a realistic BPM at startup  
      {  
        rate[i] = IBI;  
      }  
    }  
  }  
  
  if (firstBeat) // if it's the first time we found a beat, if firstBeat == TRUE  
  {  
    firstBeat = false;           // clear firstBeat flag  
    secondBeat = true;           // set the second beat flag  
    sei();                       // enable interrupts again  
    return;                     // IBI value is unreliable so discard it  
  }  
  
  // keep a running total of the last 10 IBI values  
  word runningTotal = 0;        // clear the runningTotal variable  
  
  for (int i = 0; i <= 8; i++)  
  { // shift data in the rate array
```

```

    rate[i] = rate[i + 1];          // and drop the oldest IBI value
    runningTotal += rate[i];        // add up the 9 oldest IBI values
}
rate[9] = IBI;                    // add the latest IBI to the rate array
runningTotal += rate[9];           // add the latest IBI to runningTotal
runningTotal /= 10;               // average the last 10 IBI values
BPM = 60000 / runningTotal;        // how many beats can fit into a minute? that's BPM!
QS = true;                        // set Quantified Self flag
// QS FLAG IS NOT CLEARED INSIDE THIS ISR
}
}

if (Signal < thresh && Pulse == true)
{ // when the values are going down, the beat is over
    Pulse = false;                 // reset the Pulse flag so we can do it again
    amp = P - T;                   // get amplitude of the pulse wave
    thresh = amp / 2 + T;          // set thresh at 50% of the amplitude
    P = thresh;                   // reset these for next time
    T = thresh;
}

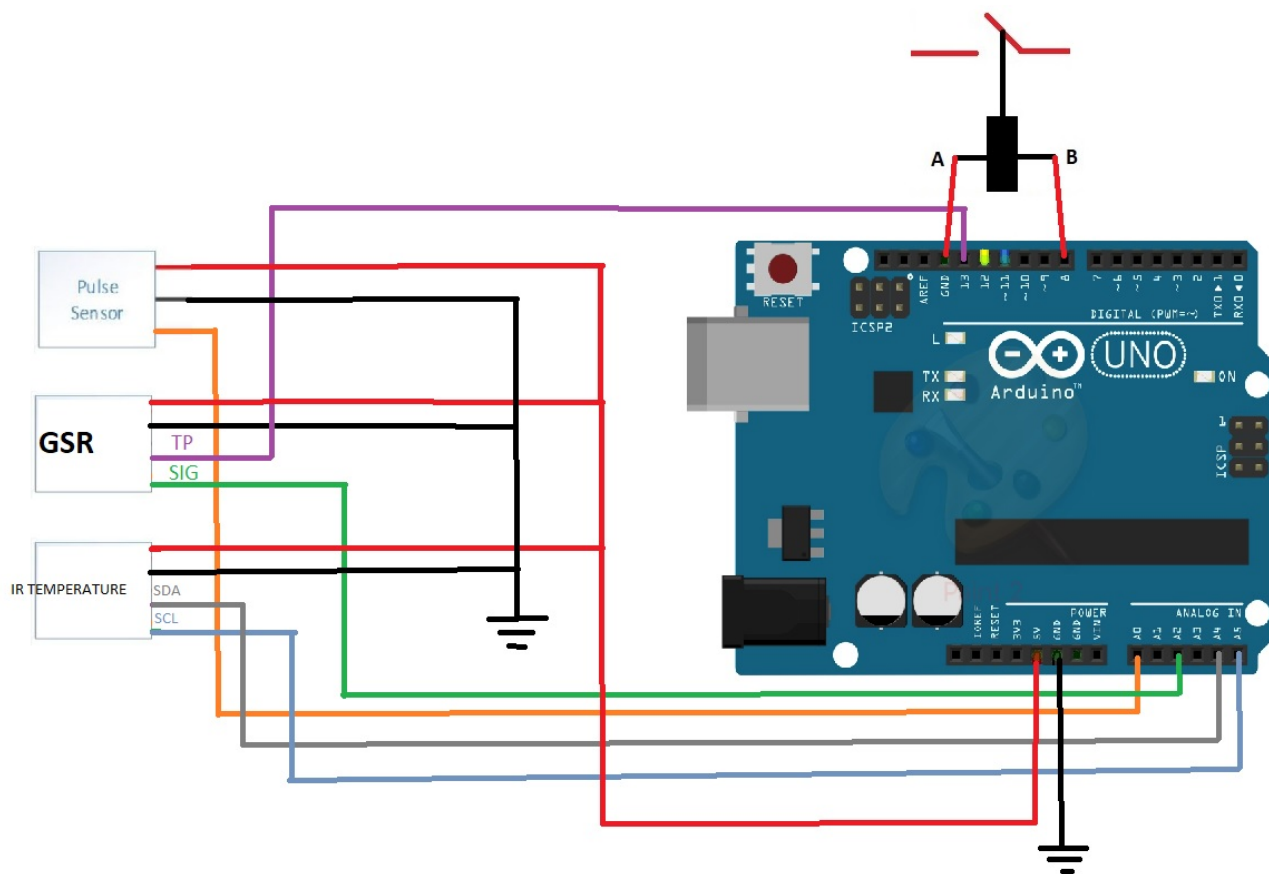
if (N > 2500)
{ // if 2.5 seconds go by without a beat
    thresh = 512;                  // set thresh default
    P = 512;                      // set P default
    T = 512;                      // set T default
    lastBeatTime = sampleCounter;  // bring the lastBeatTime up to date
    firstBeat = true;              // set these to avoid noise
    secondBeat = false;            // when we get the heartbeat back
}

sei();                            // enable interrupts when youre done!
} // end isr

```

ΠΑΡΑΡΤΗΜΑ Δ'

Σκαρίφημα συνδεσμολογίας Αισθητήρων Galvanic Skin Response, Heartbeat Pulse και IR Temperature sensor.



ΠΑΡΑΡΤΗΜΑ Ε΄

Σκιαρίφημα συνδεσμολογίας αισθητήρα Fingerprint και τοπικής οθόνης πληροφοριών.

