ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

Σχεδίαση και Ανάπτυξη Συστήματος Αυτοματοποιημένου Ελέγχου Πρόσβασης σε Χώρους με Διακρίβωση Ταυτοπροσωπίας

Φοιτήτρια: Μαρία - Σταματίνα Τσαβάλου
ΑΜ: 50106715

Επιβλέπων:

Διονύσης Κανδρής
Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, Ιούνιος 2022

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

Design and Development of an Automated Access Control System with Identity Verification

Student: Maria - Stamatina Tsavalou
Registration Number: 50106715

Supervisor

Dionisis Kandris
Professor

ATHENS-EGALEO, June 2022

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Διονύσης Κανδρής, Καθηγητής	Γρηγόρης Κουλούρας, Αναπληρωτής Καθηγητής	Ηλίας Ζώης, Επίκουρος Καθηγητής
Dionisis Kandris Digitally signed by Dionisis Kandris Date: 2022.07.16 18:32:21 +03'00' (Υπογραφή)	 Digitally signed by Grigorios Koulouras DN: c=GR, l=Athens, o=University of West Attica, ou=Class A - Private Key created and stored in hardware CSP, sn=Koulouras, givenName=Grigorios, serialNumber=6090016933, cn=Grigorios Koulouras, email=gregkoul@uniwa.gr Date: 2022.07.16 18:42:56 +03'00' (Υπογραφή)	Ilias Zois Digitally signed by Ilias Zois Date: 2022.07.16 10:52:34 +03'00' (Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη **Μαρία - Σταματίνα Τσαβάλου** του **Λεωνίδα**, με αριθμό μητρώου **50106715** φοιτήτρια του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.»

Η Δηλούσα

Μαρία - Σταματίνα Τσαβάλου

Περίληψη

Τα συστήματα βιομετρικού ελέγχου πρόσβασης χρησιμοποιούνται όλο και περισσότερο από ένα ευρύ φάσμα μεγάλων και μικρών οργανισμών. Βασικοί λόγοι για την ανάπτυξη αυτή είναι η παροχή μιας βελτιωμένης ασφάλειας αλλά και άνεσης για τους χρήστες. Επιλέγοντας ένα τέτοιο σύστημα που να εξακριβώνει την ταυτοπροσωπία τους μέσω σάρωσης του δακτυλικού τους αποτυπώματος, διευκολύνεται σε μεγάλο βαθμό η καθημερινότητά τους, καθώς δεν χρειάζεται να έχουν στην κατοχή τους αντικείμενα όπως, κλειδιά, κάρτες αναγνώρισης ή να θυμούνται κάποιον κωδικό PIN, για να εισέλθουν στους χώρους.

Οι σαρωτές δακτυλικών αποτυπωμάτων συλλέγουν μια εικόνα από τις παρυφές και τις κοιλάδες που εντοπίζονται στα δάκτυλα του κάθε ανθρώπου. Η εικόνα αυτή μετατρέπεται σε ένα πρότυπο χαρακτηριστικών και αποθηκεύεται στη βάση δεδομένων του συστήματος, ώστε έπειτα να χρησιμοποιηθεί για να γίνει η σύγκριση με το δάκτυλο που ο χρήστης τοποθετεί πάνω στον σαρωτή.

Η παρούσα διπλωματική εργασία εστιάζει στη διαδικασία της ανάπτυξης ενός τέτοιου συστήματος, το οποίο παρέχει πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες. Αφού γίνει έλεγχος από μια μονάδα σάρωσης και το δακτυλικό αποτύπωμα του χρήστη ταυτιστεί με κάποιο στη βάση δεδομένων, τότε η κλειδαριά που είναι τοποθετημένη στον χώρο ανοίγει και επιτρέπει την πρόσβαση. Ωστόσο, υπάρχουν μεγάλες πιθανότητες, άτομα χωρίς εξουσιοδότηση να προσπαθήσουν να παραβιάσουν τον χώρο. Για τον λόγο αυτό, το σύστημα έπειτα από τρεις εσφαλμένες προσπάθειες εισόδου, κλειδώνει τελείως, και επικοινωνεί ασύρματα με μια εφαρμογή που είναι εγκατεστημένη στο κινητό τηλέφωνο του διαχειριστή. Ο διαχειριστής τότε ενημερώνεται για την κατάσταση του συστήματος και είναι σε θέση να το επαναφέρει στην αρχική του κατάσταση, δηλαδή να το θέσει ξανά σε λειτουργία.

Λέξεις – κλειδιά: Δακτυλικό αποτύπωμα, βιομετρικό σύστημα, εξουσιοδοτημένος χρήστης, διαχειριστής, σάρωση, κλειδαριά, ασύρματη σύνδεση.

Abstract

Biometric access control systems are increasingly used by a wide range of organizations, large and small. The main reasons for this development are to provide an improved security, but also comfort for the users. Choosing such a system that verifies their identity by scanning their fingerprint, greatly facilitates their daily life, as they do not need to have items such as keys, ID cards or to remember a PIN code to enter on the premises.

Fingerprint scanners collect an image of the ridges and the valleys found on every human finger. This image is converted to a feature template and stored in the system database so that it can then be used to compare with the user's finger on the scanner.

This diploma thesis presents the procedures associated with the development of such a system, which provides access only to authorized users. The user's fingerprint is scanned by a scanner unit and then as soon as it is matched to any of the ones existing in the database, the system allows access to the space by opening the lock located in the corresponding entrance. However, there is a high probability that unauthorized persons will attempt to breach the facility. For this reason, the system, after three incorrect login attempts, locks in completely, and communicates wirelessly with an application that is installed on the administrator's mobile phone. The administrator is then informed about the status of the system and is able to restore it to its original state, i.e. to restart it.

Keywords: Fingerprint, biometric system, authorized user, administrator, scanning, lock, wireless connection.

Περιεχόμενα

Κατάλογος Εικόνων

Αλφαβητικό Ευρετήριο

A/D: Analog to Digital

AFIS: Automated Fingerprint Identification System

A-KAZE: Accelerated KAZE

AREF: Analog Reference

ATMEL: Advanced Technology for Memory and Logic

AVR RISC: Alf and Vegard's RISC

CCD: Charge-Coupled Device

CMOS: Complementary Metal-Oxide Semiconductor

DC: Direct Current

DSP: Digital Signal Processing

EEPROM: Electrically Erasable Programmable Read Only Memory

EER: Equal Error Rate

FAR: False Acceptance Rate

FRR: False Rejection Rate

FVC: Fingerprint Verification Competition

HOG: Histograms of Oriented Gradients

ID: Identity

IDE: Integrated Development Environment

IoT: Internet of Things

I2C: Inter-Integrated Circuit

LBP: Local Binary Patterns

LCD: Liquid-Crystal Display

LED: Light-Emitting Diode

PIN: Personal Identification Number

PWM: Pulse-Width Modulation

RISC: Reduced Instruction Set Computer

RFID: Radio Frequency Identification

RSA: Rivest Shamir Adleman

RX: Receiving

SIFT: Scale-Invariant Feature Transform

SMD: Surface Mount Device

SRAM: Static Random Access Memory

TX: Transmitting

UART: Universal Asynchronous Receiver Transmitter

USB: Universal Serial Bus

Wi-Fi: Wireless Fidelity

2D: Two Dimensional

3D: Three Dimensional

ΕΙΣΑΓΩΓΗ

Η ανάπτυξη ενός ασφαλούς συστήματος ελέγχου πρόσβασης σε χώρους και εγκαταστάσεις που απαιτούν υψηλή ασφάλεια, αποτελεί καθοριστικό ρόλο στην καθημερινότητα των ανθρώπων. Λόγω της ραγδαίας αύξησης των ηλεκτρονικών εγκλημάτων και της παραβίασης της ιδιωτικής ζωής, τόσο σε ψηφιακό όσο και σε φυσικό επίπεδο, τα συστήματα αυτά παρέχουν πρόσβαση μόνο σε χρήστες οι οποίοι είναι εξουσιοδοτημένοι. Αυτό έχει ως αποτέλεσμα, πολλά βιομετρικά συστήματα ελέγχου ταυτότητας να έχουν αναπτυχθεί εδώ και πολύ καιρό με κύριο σκοπό να παρέχουν περισσότερη αξιοπιστία. Τέτοια μοντέλα έχουν καταφέρει και έχουν ξεπεράσει άλλες παραδοσιακές μεθόδους ασφαλείας, όπως είναι οι κωδικοί πρόσβασης και οι αριθμοί PIN.

Αντικείμενο της διπλωματικής εργασίας

Η συγκεκριμένη διπλωματική εργασία έχει ως κύριο θέμα την υλοποίηση ενός βιομετρικού συστήματος για να ελέγχεται η πρόσβαση σε διάφορους χώρους. Στη σημερινή εποχή, τα βιομετρικά χαρακτηριστικά των ανθρώπων απασχολούν πολύ τις νέες τεχνολογίες και εντάσσονται σε ολοένα και περισσότερες ηλεκτρονικές συσκευές. Τα βιομετρικά συστήματα, και συγκεκριμένα αυτά που κάνουν χρήση των δακτυλικών αποτυπωμάτων, βασίζονται στο γεγονός ότι κάθε άτομο είναι διαφορετικό όσον αφορά τη φυσιολογία του. Το δακτυλικό αποτύπωμα αποτελεί μόνιμο και ξεχωριστό χαρακτηριστικό για κάθε άνθρωπο, καθώς σχηματίζεται πριν ακόμα από την γέννησή του. Για τον λόγο αυτό, η διακρίβωση της ταυτοπροσωπίας των ανθρώπων στο υλοποιημένο σύστημα της εργασίας αυτής, γίνεται μέσω αναγνώρισης των δακτυλικών τους αποτυπωμάτων.

Σκοπός και στόχοι

Στόχος της διπλωματικής αυτής εργασίας είναι να αναπτυχθεί ένα αξιόπιστο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων με σκοπό να παρέχει πρόσβαση σε έναν χώρο. Για να είναι όμως το σύστημα αρκετά αξιόπιστο, απαραίτητη προϋπόθεση είναι να υπάρχει πλήρης έλεγχος για πιθανές παραβιάσεις από μη εξουσιοδοτημένους χρήστες. Συνεπώς, ένας ακόμη σημαντικός στόχος είναι η παροχή ασφάλειας στους ελεγχόμενους χώρους, όπου θα τοποθετηθεί το σύστημα αυτό, και ο αποκλεισμός όλων των ανθρώπων που θα προσπαθούν να το εξαπατήσουν.

Μεθοδολογία

Στο πρώτο στάδιο για την ανάπτυξη του συστήματος ασφαλείας, υλοποιήθηκε το πρακτικό κομμάτι, δηλαδή η κατασκευή του κυκλώματος. Αναπτύσσοντας τον σχετικό κώδικα λειτουργίας, ο οποίος ανέβηκε στην πλακέτα του Arduino, επιτεύχθηκε το άνοιγμα της κλειδαριάς στους εξουσιοδοτημένους χρήστες και η εμπλοκή του συστήματος έπειτα από εσφαλμένες προσπάθειες εισόδου. Εν συνεχεία, στο δεύτερο στάδιο, προστέθηκε η τεχνολογία Bluetooth και αναπτύχθηκε κώδικας για την υλοποίηση της Android εφαρμογής. Μέσω της εφαρμογής αυτής επιτεύχθηκε η επικοινωνία μεταξύ του κινητού τηλεφώνου και της κατασκευής, με σκοπό την αλληλεπίδρασή τους για ανάγνωση - εμφάνιση μηνυμάτων και επαναφορά του συστήματος έπειτα από πιθανές εμπλοκές.

Καινοτομία

Καθώς η τεχνολογία των smart home συνεχίζει να αναπτύσσεται τόσο σε επίπεδο επαγγελματικό, όσο και σε οικιακό, θεωρείται πλέον κρίσιμη η ένταξη βιομετρικών συστημάτων για να ελέγχουν την πρόσβαση σε τέτοιου είδους χώρους. Η συγκεκριμένη διπλωματική εργασία αξιοποιεί την τεχνολογία αυτή και επιτρέπει την πρόσβαση χάρη στα δακτυλικά αποτυπώματα των χρηστών.

Δομή

Η παρούσα διπλωματική εργασία οργανώνεται σε 3 κύρια κεφάλαια. Αρχικά, στις πρώτες ενότητες του 1^{ου} κεφαλαίου γίνεται ανάλυση στα χαρακτηριστικά των δακτυλικών αποτυπωμάτων και στην διαδικασία με την οποία αυτά αναγνωρίζονται, εξάγονται και ταυτοποιούνται σε ένα βιομετρικό σύστημα ελέγχου. Στις επόμενες ενότητες αναλύονται οι διάφορες συσκευές μέσω των οποίων γίνεται η διαδικασία αυτή και οι συνθήκες που την επηρεάζουν. Στη συνέχεια, στις αρχικές ενότητες του 2^{ου} κεφαλαίου εξηγούνται τα οφέλη από την ανάπτυξη βιομετρικών συστημάτων και αναλύονται όλα τα εξαρτήματα που χρησιμοποιήθηκαν για την εργασία. Έπειτα, παρατίθενται η συνδεσμολογία του συστήματος και η ανάπτυξη των κωδίκων για την υλοποίησή του. Τέλος, στο 3^{ο} κεφάλαιο προτείνονται μελλοντικές αλλαγές και που θα βελτιώσουν την λειτουργία του βιομετρικού αυτού συστήματος.

ΚΕΦΑΛΑΙΟ 1ο: Το Δακτυλικό Αποτύπωμα ως Βιομετρικό Χαρακτηριστικό Αναγνώρισης

1.1 Εισαγωγή

Σκοπός του 1ου κεφαλαίου είναι η εισαγωγή του αναγνώστη στις διαδικασίες αναγνώρισης ανθρώπων μέσω της χρήσης βιομετρικών χαρακτηριστικών και ειδικότερα των δακτυλικών αποτυπωμάτων τους. Ειδικότερα, ανάλυση των ιδιαίτερων χαρακτηριστικών τα οποία συνθέτουν ένα δακτυλικό αποτύπωμα και το καθιστούν μοναδικό από άνθρωπο σε άνθρωπο. Η εξαγωγή και η αντιστοίχισή τους σε ένα βιομετρικό σύστημα αναγνώρισης αποτελούν δύο πολύ σημαντικές διαδικασίες, οι οποίες καθορίζουν την μετέπειτα ταυτοποίησή τους στο σύστημα αυτό και αναλύονται παρακάτω. Ακόμη, θα γίνει αναφορά στις συσκευές με τις οποίες γίνεται εξαγωγή των βιομετρικών αυτών χαρακτηριστικών, καθώς και στις συνθήκες που μπορεί να επηρεάσουν την διαδικασία αυτή.

1.2 Αναγνώριση μέσω Βιομετρικών Χαρακτηριστικών

Η αναγνώριση ανθρώπων βάσει των βιομετρικών τους χαρακτηριστικών είναι ένα αναδυόμενο φαινόμενο στη σημερινή κοινωνία. Τα τελευταία χρόνια έχει τραβήξει όλο και περισσότερο το ενδιαφέρον εξαιτίας της ανάγκης για ασφάλεια σε ένα μεγάλο εύρος εφαρμογών, όπως είναι η αντικατάσταση του προσωπικού αριθμού αναγνώρισης (PIN) σε τράπεζες και επιχειρήσεις λιανικής πώλησης, ασφάλεια συναλλαγών μεταξύ δικτυακών υπολογιστών, υψηλής ασφαλείας ασύρματη πρόσβαση και άδεια εισόδου σε ειδικούς χώρους (Jain, Bolle & Pankanti, 1999). Βιομετρικά στοιχεία χρησιμοποιούνται σε καθημερινή βάση στα κινητά τηλέφωνα και σε άλλες συσκευές με σκοπό την ταυτοποίηση του χρήστη ώστε να έχει πρόσβαση στην προσωπική του συσκευή.

Τα παραδοσιακά συστήματα εξακρίβωσης της ταυτότητας ενός ανθρώπου βασίζονται στη γνώση (μυστικός κωδικός) ή στα αποκτήματα (ID κάρτα). Παρόλα αυτά οι κωδικοί μπορούν εύκολα να ξεχαστούν ή να ακουστούν από τρίτους και οι κάρτες μπορεί να χαθούν ή να κλαπούν, δίνοντας έτσι σε διάφορους επιτήδειους την πιθανότητα να περάσουν από ένα τεστ ταυτοποίησης. Η χρήση χαρακτηριστικών που είναι άμεσα συνδεδεμένα με το ανθρώπινο σώμα, μειώνει σημαντικά τις πιθανότητες απάτης. Επιπρόσθετα, η βιομετρία είναι ικανή για να διευκολύνει τον χρήστη σε πολλές περιπτώσεις, καθώς αντικαθιστά τις κάρτες, τους κωδικούς, τα κλειδιά κ.ά..

Πολλά από τα βιομετρικά χαρακτηριστικά που ξεχωρίζουν είναι: το δακτυλικό αποτύπωμα, η ίριδα, το πρόσωπο, η φωνή, η γεωμετρία του χεριού, ο αμφιβληστροειδής χιτώνας, ο γραφικός χαρακτήρας, το βάδισμα κ.ά. (Riaz & Khan, 2017). Για διάφορους λόγους, το δακτυλικό αποτύπωμα θεωρείται ως ένα από τα πιο πρακτικά χαρακτηριστικά. Τα δακτυλικά αποτυπώματα θεωρούνται πιο εύκολα προσιτά, ο χρήστης καταβάλει ελάχιστο κόπο προκειμένου να αναγνωριστεί από το σύστημα και δεν απαιτούνται πολλές πληροφορίες πέρα από τις απολύτως αναγκαίες για την διαδικασία της αναγνώρισης. Ένας ακόμη λόγος που τα καθιστούν πιο δημοφιλή είναι το χαμηλό κόστος αγοράς των αισθητήρων αναγνώρισης. Έξυπνες κάρτες με ενσωματωμένους αισθητήρες δακτυλικών αποτυπωμάτων είναι ήδη διαθέσιμες στην αγορά και οι αισθητήρες αυτοί μπορούν εύκολα να ενσωματωθούν σε ένα ασύρματο υλικό.

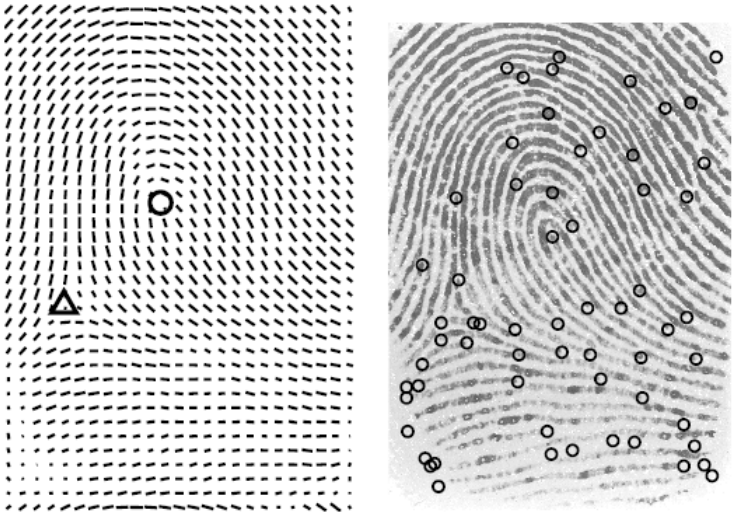
Ο πρώτος Διαγωνισμός Επαλήθευσης Δακτυλικών Αποτυπωμάτων που διεξήχθη το 2000 (Fingerprint Verification Competition) έδειξε ότι πολλοί παράγοντες μπορούν να μειώσουν την απόδοση μιας ταυτοποίησης (Maio, Maltoni, Cappelli, Wayman & Jain, 2002). Ο θόρυβος που απεικονίζεται στην εικόνα του αποτυπώματος, η ελαστική παραμόρφωση του δέρματος την στιγμή που ακουμπάει κάποιος τον αισθητήρα και οι μεγάλες βάσεις δεδομένων αποτελούν παράγοντες που καθιστούν δύσκολη την επίτευξη υψηλής απόδοσης των αλγορίθμων αναγνώρισης δακτυλικών αποτυπωμάτων. Έπειτα από πολλές προσπάθειες ερευνητών, όμως, τις τελευταίες δεκαετίες, έχει επιτευχθεί αξιοσημείωτη ακρίβεια στην αντιστοίχιση των δακτυλικών αποτυπωμάτων. Για παράδειγμα, υπάρχει μια διαδικτυακή πλατφόρμα αξιολόγησης που ονομάζεται FVC-onGoing (Maio, Maltoni, Cappelli, Franco, Ferrara & Turroni, 2013), όπου οι ερευνητές μπορούν να ανεβάσουν τους αλγορίθμους αναγνώρισης και να τους συγκρίνουν με άλλους και να ελέγξουν την απόδοση και την ακρίβεια της αντιστοίχισης.

1.3 Χαρακτηριστικά Δακτυλικών Αποτυπωμάτων

Το δακτυλικό αποτύπωμα είναι ένα μοτίβο από καμπύλες γραμμές, οι οποίες ονομάζονται παρυφές και αποτελούν το υψηλότερο διακριτό σημείο στο δέρμα. Τα σημεία που βρίσκονται ανάμεσά τους ονομάζονται κοιλάδες. Στις περισσότερες εικόνες με δακτυλικά αποτυπώματα, οι παρυφές διακρίνονται με σκούρο χρώμα (συνήθως μαύρο) και οι κοιλάδες με ανοιχτόχρωμη απόχρωση (συνήθως λευκές). Τα χαρακτηριστικά των δακτυλικών αποτυπωμάτων (Hong, Wan & Jain, 1998) που χρησιμοποιούνται συνήθως είναι τα εξής:

- Μοναδικά σημεία (Singular points): Αντιπροσωπεύουν τις ασυνέχειες στο πεδίο προσανατολισμού. Υπάρχουν δύο τύποι μοναδικών σημείων. Ο πυρήνας είναι το ανώτερο μέρος της πιο εσωτερικής καμπυλωτής παρυφής και το σημείο δέλτα, όπου συναντώνται τρεις

ροές παρυφών. Χρησιμοποιούνται για την καταχώριση και την ταξινόμηση των δακτυλικών αποτυπωμάτων. Στην Εικόνα 1.1 με «Ο» απεικονίζεται ο πυρήνας και με «Δ» απεικονίζεται το δέλτα.

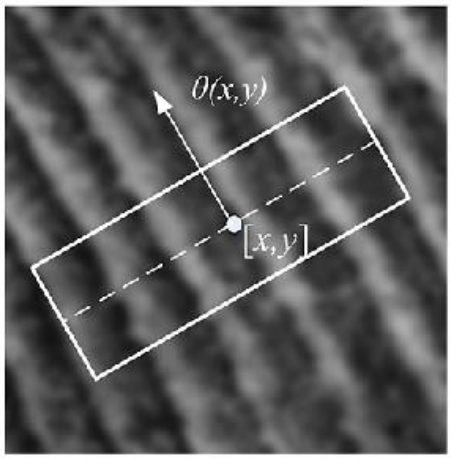


Εικόνα 1.1: Μοναδικά σημεία σε ένα δακτυλικό αποτύπωμα

- Πεδίο προσανατολισμού παρυφών (Ridge Orientation Field): Αντιπροσωπεύει την τοπική κατεύθυνση της δομής παρυφών και κοιλάδων. Χρησιμοποιείται συνήθως για ταξινόμηση, βελτίωση εικόνας και φιλτράρισμα των χαρακτηριστικών στοιχείων των μικρολεπτομερειών.

Εικόνα 1.2: Χάρτης προσανατολισμού παρυφών

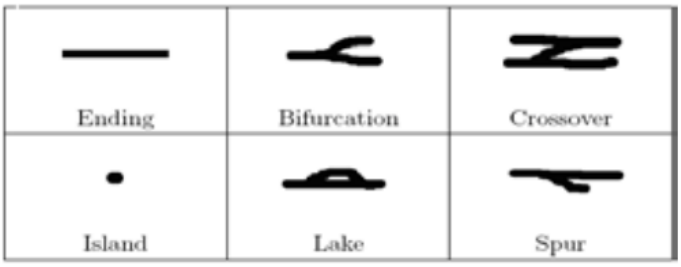
- Χάρτης συχνότητας παρυφών (Ridge Frequency): Υποδεικνύει τον αριθμό των παρυφών σε μια μονάδα μήκους μιας εικόνας. Είναι η τοπική συχνότητα των παρυφών που σχηματίζουν συλλογικά την εικόνα του δακτυλικού αποτυπώματος. Η εκτίμηση της συχνότητας των παρυφών είναι βασική προϋπόθεση για τη βελτίωση της απόδοσης των εικόνων που λαμβάνονται στο σύστημα.



Εικόνα 1.3: Χάρτης συχνότητας παρυφών

- Μικρολεπτομέρειες (Minutiae): Πρόκειται για τις μικρές λεπτομέρειες που εντοπίζονται στις δομές των παρυφών και των κοιλάδων. Αυτά τα μικροσκοπικά στοιχεία χρησιμοποιούνται για τον προσδιορισμό της μοναδικότητας μιας εικόνας δακτυλικού αποτυπώματος. Ο Francis Galton ήταν ο πρώτος άνθρωπος που παρατήρησε τις δομές και τη μονιμότητα των μικροσκοπικών αυτών στοιχείων, τα οποία δεν αλλοιώνονται με το πέρας των χρόνων, οπότε ονομάζονται και «λεπτομέρειες Galton» (Henry, 1900). Χρησιμοποιούνται από ιατροδικαστές για να ταιριάξουν δύο δακτυλικά αποτυπώματα. Υπάρχουν περίπου 150 διαφορετικοί τύποι, οι οποίοι κατηγοριοποιούνται με βάση τη διαμόρφωσή τους. Μεταξύ αυτών, η λήξη παρυφής (ridge ending) και η διακλάδωση παρυφής (bifurcation) χρησιμοποιούνται σε συστήματα αυτόματης αναγνώρισης δακτυλικών αποτυπωμάτων, καθώς όλοι οι άλλοι τύποι μπορούν να θεωρηθούν ως συνδυασμοί «απολήξεων» και «διακλαδώσεων». Παρακάτω φαίνονται μερικοί από τους τύπους αυτούς.

Εικόνα 1.4: Τύποι μικρολεπτομερειών



Εικόνα 1.5: Συνηθέστεροι τύποι μικρολεπτομερειών

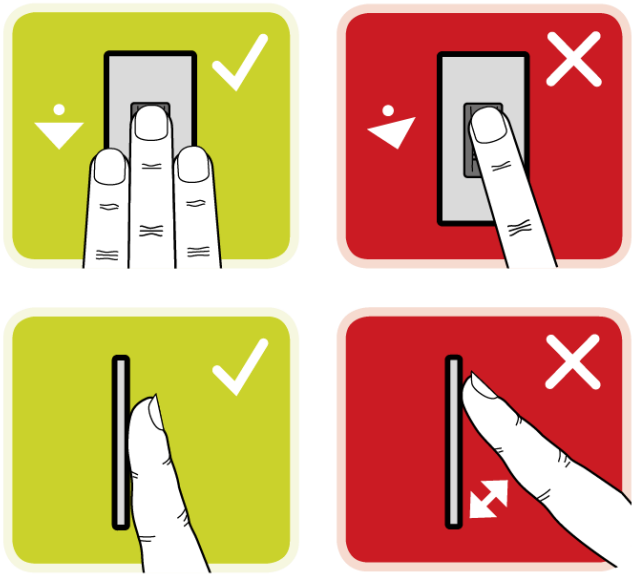
Στα περισσότερα συστήματα αναγνώρισης δακτυλικών αποτυπωμάτων, το πεδίο προσανατολισμού χρησιμοποιείται για τη βελτίωση του δακτυλικού αποτυπώματος και, μαζί με τα μοναδικά σημεία, για ταξινόμηση, ενώ οι μικρολεπτομέρειες χρησιμοποιούνται για την αντιστοίχιση.

1.4 Εξαγωγή Χαρακτηριστικών και Αντιστοίχιση

Η αυτόματη αναγνώριση δακτυλικών αποτυπωμάτων είναι ένα πολύ σημαντικό ερευνητικό θέμα τις τελευταίες δύο δεκαετίες. Καθώς πολλά υλικά hardware γίνονται όλο και πιο εύκολα διαθέσιμα στην αγορά, ο αριθμός των ιδρυμάτων και των εταιρειών που χρησιμοποιούν τεχνικές αναγνώρισης αυξάνεται σταθερά με τα χρόνια, μαζί με τον αριθμό των ατόμων που πρόκειται να αναγνωριστούν (Jain & Feng, 2010). Τα δακτυλικά αποτυπώματα παρουσιάζουν διάφορα χαρακτηριστικά που τα καθιστούν εξαιρετικά βιομετρικά χαρακτηριστικά για σκοπούς αναγνώρισης, όπως η μοναδικότητα, το μέγεθος και η ιδιαιτερότητά τους. Παρά τα πολλά χαρακτηριστικά που μπορούν να προκύψουν, οι μικρολεπτομέρειες

είναι οι πιο ευρέως χρησιμοποιούμενες. Οι αλγόριθμοι, συνήθως, βασίζουν τους υπολογισμούς τους σε ένα σύνολο τοπικών δομών που εξάγονται από τις μικρολεπτομέρειες των δακτυλικών αποτυπωμάτων.

Σε ένα σύστημα ελέγχου πρόσβασης κρίνονται απαραίτητες κάποιες αρχικές διαδικασίες, όπως η συλλογή δεδομένων, η εγγραφή και η αντιστοίχιση. Κατά την διαδικασία της ***συλλογής – λήψης του δακτυλικού αποτυπώματος***, γίνεται σάρωση της εικόνας από την άκρη του δακτύλου, εξάγεται το μοτίβο των παρυφών και των κοιλάδων και ελέγχεται αν ταιριάζει με το μοτίβο μιας από τις ήδη σαρωμένες εικόνες (Dorai, Ratha & Bolle, 2004). Από την διαδικασία αυτή μπορεί να παραχθεί είτε καλή είτε κακή ποιότητα αυτών ανάλογα με τη συσκευή λήψης ή τον σαρωτή που χρησιμοποιείται και την κατάσταση στην οποία βρίσκεται το δέρμα του ατόμου εκείνη τη χρονική στιγμή (π.χ. ξηρό, υγρό, καθαρό, βρώμικο, τραυματισμένο κ.ά.). Πολλοί ερευνητές θεωρούν ότι πολλά από τα προβλήματα που εντοπίζονται στην ποιότητα της εικόνας προκύπτουν από συσκευές με σαρωτή χαμηλής ποιότητας. Κάθε αισθητήρας είναι διαφορετικός και κατά συνέπεια λαμβάνει και διαφορετική ποιότητα εικόνας. Για πρακτικούς λόγους, προτείνεται η χρήση σαρωτών υψηλής ποιότητας και απαιτείται σωστή χρήση του δακτύλου κατά τη σάρωση (Zhang, Shan, Fang & Shao, 2019). Εάν χρησιμοποιηθεί αισθητήρας υψηλής ποιότητας και τα άκρα είναι καθαρά και σωστά τοποθετημένα, θα μπορούν να ληφθούν καλής ποιότητας εικόνες των δακτυλικών αποτυπωμάτων.



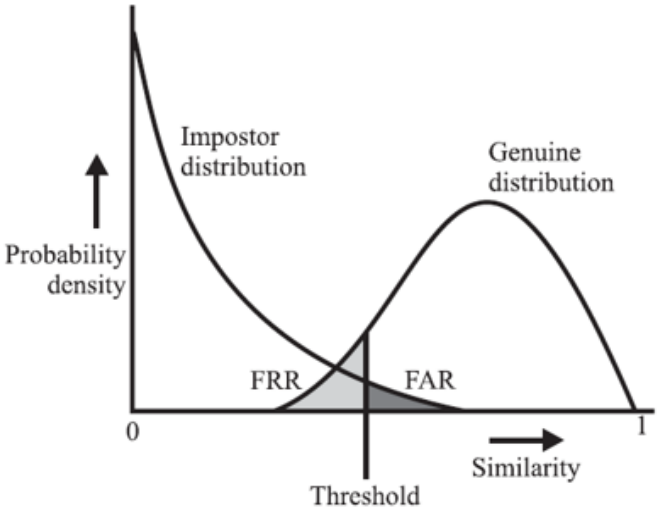
Εικόνα 1.6: Σωστή και λανθασμένη τοποθέτηση δακτύλου στον σαρωτή

Κατά την ***εγγραφή των δακτυλικών αποτυπωμάτων*** σε ένα σύστημα χρειάζεται να ακολουθηθούν κάποια σημαντικά βήματα, όπως είναι η συλλογή τους από μια συσκευή, η λήψη μιας βελτιωμένης

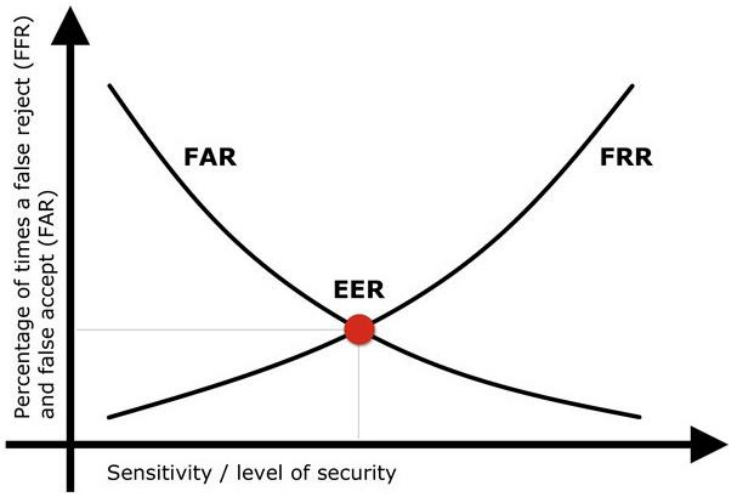
εικόνας, η ανάλυση των μοναδικών χαρακτηριστικών τους και η αποθήκευση αυτών στη βάση δεδομένων (Kindt, 2013). Η διαδικασία αυτή αποτελεί, στις περισσότερες περιπτώσεις, το πρώτο βήμα σε μια βιομετρική σύγκριση και είναι πολύ σημαντική για την αποθήκευση του αποτελέσματος αυτού σε ψηφιακό πρότυπο. Οι χρήστες, επομένως, θα πρέπει να καταχωρούν στο σύστημα τα βιομετρικά τους χαρακτηριστικά μέσω βιομετρικών συσκευών (προ-επεξεργασία και εξαγωγή χαρακτηριστικών) και να αποθηκεύσουν το βιομετρικό τους πρότυπο στη βάση δεδομένων.

Στα συστήματα ελέγχου πρόσβασης η ***αντιστοίχιση*** είναι ένα πολύ σημαντικό βήμα. Πρόκειται για την σύγκριση ενός συγκεκριμένου δακτυλικού αποτυπώματος με ένα άλλο. Το αποτέλεσμα αυτής της σύγκρισης θα δηλώνει είτε ότι «ταιριάζουν» είτε ότι «δεν ταιριάζουν». Πολλοί παράγοντες οι οποίοι επηρεάζουν την αντιστοίχιση είναι ο θόρυβος στην εικόνα, οι αλλαγές στη φυσιολογία του χρήστη (όπως κάποια γρατζουνιά ή κόψιμο), οι εξωτερικές συνθήκες (όπως θερμοκρασία ή υγρασία) αλλά και ο τρόπος που ο χρήστης θα τοποθετήσει το δάκτυλο του στον αισθητήρα. Επομένως, το αποτέλεσμα της σύγκρισης αυτής είναι ένας αριθμός που δείχνει σε τι ποσοστό είναι όμοια δύο δακτυλικά αποτυπώματα, συγκρίνοντας την είσοδο και το ήδη υπάρχον πρότυπο. Όσο μεγαλύτερο είναι αυτό το ποσοστό, τόσο πιο σίγουρο είναι το σύστημα ότι οι δύο βιομετρικές μετρήσεις προέρχονται από το ίδιο άτομο. Οι αποφάσεις ορίζονται στο σύστημα από ένα όριο (threshold). Δύο δακτυλικά αποτυπώματα θεωρούνται ίδια αν η ομοιότητά τους υπερβεί ή είναι ίση με αυτό το όριο, ενώ θεωρούνται αταίριαστα (προέρχονται από διαφορετικό δάκτυλο) αν η ομοιότητα τους είναι κάτω από το όριο (Wayman, 1999).

Η κατανομή που προκύπτει από δείγματα ίδιων ατόμων ονομάζεται αληθής κατανομή (genuine distribution), ενώ από διαφορετικά άτομα ονομάζεται ψευδής κατανομή (impostor distribution). Σε γενικές γραμμές, οι κατανομές των τιμών ομοιότητας των επαληθευμένων προσπαθειών (αντιστοίχιση δακτυλικών αποτυπωμάτων) και των λανθασμένων (μη αντιστοίχιση δακτυλικών αποτυπωμάτων) δεν μπορούν να διαχωριστούν πλήρως με ένα όριο. Συνεπώς, οι κατανομές επικαλύπτονται σε κάποιο βαθμό, προκαλώντας λάθη στην αντιστοίχιση. Αυτό απεικονίζεται στην Εικόνα 1.7.



Εικόνα 1.7: Ταιριαστές και μη-ταιριαστές κατανομές



Εικόνα 1.8: Γράφημα συσχέτισης των ποσοστών

Η απόδοση της αντιστοίχισης στα συστήματα επαλήθευσης δακτυλικών αποτυπωμάτων διακρίνεται από δύο σφάλματα μετρήσεων. Το ***Ποσοστό Ψευδούς Αποδοχής*** *(FAR)* δηλώνει την πιθανότητα ένα σύστημα να βγάλει «ταιριαστά» αποτυπώματα από διαφορετικά δάκτυλα, όπως φαίνεται στην σκούρα γκρι περιοχή του γραφήματος στην Εικόνα 1.7. Το ***Ποσοστό Ψευδούς Απόρριψης*** *(FRR)* δηλώνει την πιθανότητα ένα σύστημα να βγάλει «μη ταιριαστά» αποτυπώματα από το ίδιο δάκτυλο, όπως φαίνεται στην ανοιχτή γκρι περιοχή του ίδιου γραφήματος. Το σημείο στο οποίο τέμνονται οι δύο καμπύλες

ονομάζεται ***Ποσοστό Ίσου Σφάλματος*** *(EER)* και πρόκειται για το σημείο στο οποίο το FAR και το FRR είναι ίσα.

Ιδανικά, ο δείκτης EER θα πρέπει να είναι μηδέν, που σημαίνει ότι τα FAR και FRR είναι επίσης ίσα με μηδέν. Στην πράξη, αυτό δεν είναι εφικτό. Αν μειωθεί το FAR όσο το δυνατόν πιο χαμηλά, τότε το FRR είναι πιθανό να αυξηθεί απότομα, πράγμα το οποίο σημαίνει ότι όσο πιο ασφαλής είναι ο έλεγχος πρόσβασης, τόσο λιγότερο βολικό θα είναι για τους χρήστες, καθώς θα τους απορρίπτει το σύστημα πιο εύκολα. Το ίδιο ισχύει και στην αντίθετη περίπτωση. Συνεπώς, είτε το σύστημα θα είναι πιο ασφαλές αλλά λιγότερο φιλικό προς τον χρήστη, είτε θα είναι λιγότερο ασφαλές, αλλά πιο φιλικό προς τον χρήστη.

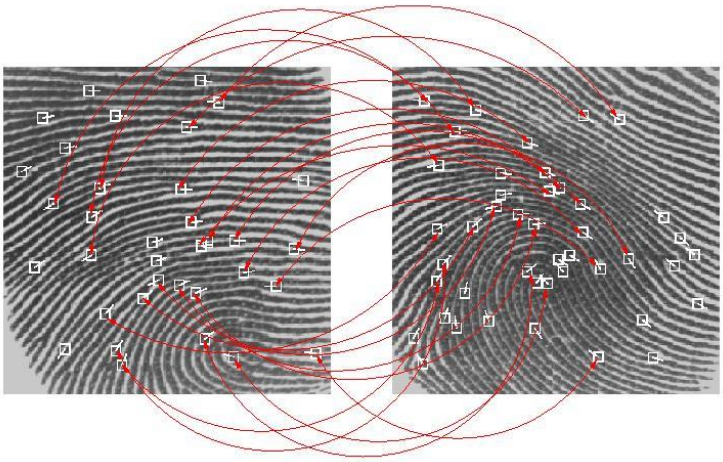
Η αντιστοίχιση των δακτυλικών αποτυπωμάτων μεταξύ τους, συνήθως, εκτελείται αξιοποιώντας μόνο τις μικρολεπτομέρειες των άκρων ή τις διακλαδώσεις που εντοπίζονται στα δάκτυλα (Maltoni, Maio, Jain & Prabhakar, 2009). Στα Συστήματα Αυτόματης Αναγνώρισης Δακτυλικών Αποτυπωμάτων (AFIS), η επιτυχής ταύτιση δύο δακτυλικών αποτυπωμάτων γίνεται όταν παρατηρούνται περισσότερα από 12 ταιριαστά ζεύγη μικρολεπτομερειών. Ωστόσο, σε εικόνες που λαμβάνονται από μικρούς αισθητήρες δακτυλικών αποτυπωμάτων, παρατηρείται ότι περιέχουν πολύ λιγότερο από τον απαιτούμενο αριθμό μικρολεπτομερειών που θα επέτρεπαν την ακριβέστερη αντιστοίχιση. Ορισμένα εμπορικά συστήματα ζητούν από τον χρήστη να καταχωρήσει διάφορα τμήματα του δακτυλικού του αποτυπώματος, με σκοπό να ξεπεραστεί αυτή η ανεπάρκεια των μικρολεπτομερειών (Mathur, Vjav, Shah, Das & Malla, 2016).

Η χρήση επιπρόσθετων χαρακτηριστικών, πέρα από τις μικρολεπτομέρειες, μπορεί να βελτιώσει την ακρίβεια της αντιστοίχισης μεταξύ δακτυλικών αποτυπωμάτων. Για το λόγο αυτό έχουν προταθεί διάφορες μέθοδοι αντιστοίχισης που δεν χρησιμοποιούν τις μικρολεπτομέρειες. Αυτές οι μέθοδοι μπορούν να κατηγοριοποιηθούν σε τέσσερις ομάδες: αντιστοίχιση βάσει εικόνας, αντιστοίχιση βάσει χαρακτηριστικών των παρυφών, αντιστοίχιση βάσει σημείων χαρακτηριστικών και αντιστοίχιση βάσει χαρακτηριστικών επιπέδου 3. Η αντιστοίχιση που βασίζεται ***στην εικόνα*** αξιολογεί τον βαθμό της ομοιότητας μεταξύ δύο εικόνων δακτυλικών αποτυπωμάτων. Η πιο συνηθισμένη μέθοδος υπολογισμού της συσχέτισης μεταξύ δύο εικόνων γίνεται χρησιμοποιώντας πληροφορίες σε κλίμακα του γκρι (Hatano, Adachi, Shigematsu, Morimura, Onishi, Okazaki & Kyuragi, 2002). Αν και αυτή η προσέγγιση συγκρίνει άμεσα τα μοτίβα των παρυφών δύο δακτυλικών αποτυπωμάτων, είναι ευάλωτη στο σφάλμα ευθυγράμμισης που προκαλείται από τη μη γραμμική παραμόρφωση. Άλλες μέθοδοι που βασίζονται σε εικόνα χρησιμοποιούν διακριτικά χαρακτηριστικά υφής όπως η απόκριση Gabor, τοπικά δυαδικά μοτίβα

(LBP) και ιστόγραμμα προσανατολισμένων κλίσεων (HoG) (Benhammadi, Amirouche, Hentous, Beghdad & Aissani, 2007). Ωστόσο, εξακολουθούν να είναι ευαίσθητες στη διακύμανση της εικόνας που προκαλείται από αιτίες όπως ο θόρυβος, η κατάσταση του δέρματος ή η μη γραμμική παραμόρφωση.

Εικόνα 1.9: Εγγραφή ενός δακτυλικού αποτυπώματος

Οι αντιστοιχίσεις που βασίζονται ***στα χαρακτηριστικά των παρυφών*** χρησιμοποιούν πληροφορίες από τα μοτίβα των παρυφών. Συγκεκριμένα, αξιοποιώντας τον προσανατολισμό και την συχνότητά τους βελτιώνουν την απόδοση της αντιστοίχισης, καθώς είναι ανθεκτικά στις μη γραμμικές παραμορφώσεις και κατά συνέπεια ενισχύουν την ατομικότητα ενός δακτυλικού αποτυπώματος. Για να το πετύχουν αυτό, οι παρυφές αντιπροσωπεύονται εξ ολοκλήρου από μια λίστα σημείων δειγματοληψίας που εξάγονται κατά μήκος των αραιωμένων παρυφών. Σε μια τέτοια διαδικασία αντιστοίχισης, η άμεση σύγκριση παρυφών πραγματοποιείται από αυτά τα σημεία δειγματοληψίας. Ωστόσο, απαιτείται υψηλός ρυθμός δειγματοληψίας για να επιτευχθεί υψηλή απόδοση, η οποία αυξάνει την υπολογιστική πολυπλοκότητα της διαδικασίας. Ωστόσο, η εξαγωγή των χαρακτηριστικών των παρυφών είναι ασταθής εξαιτίας του σφάλματος εξαγωγής μικρολεπτομερειών (Fang, Srihari, Srinivasan & Phatak, 2007). Ελάχιστες μόνο παρυφές που σχετίζονται με μικρολεπτομέρειες έχουν την δυνατότητα να ενσωματώνονται στην αντιστοίχιση.



Εικόνα 1.10: Σημεία δειγματοληψίας προς αντιστοίχιση

Ακόμη, αρκετές έρευνες πρότειναν αντιστοίχιση με βάση ***χαρακτηριστικά σημεία – κλειδιά***, όπως το SIFT και το A-KAZE (Yamazaki, Li, Isshiki & Kunieda, 2015). Επικύρωσαν ότι οι δυνατότητες των σημείων αυτών μπορούν να παρέχουν διακριτικές πληροφορίες για αντιστοίχιση των δακτυλικών αποτυπωμάτων, χρησιμοποιώντας χαρακτηριστικά της υφής των παρυφών. Αυτές οι μέθοδοι, ωστόσο, είναι σχετικά ευαίσθητες στις μεγάλες διακυμάνσεις της υφής του δέρματος που προκαλούνται από θόρυβο ή την κατάσταση στην οποία βρίσκεται το δέρμα.

Τέλος, οι αντιστοιχίσεις που βασίζονται σε ***χαρακτηριστικά επιπέδου 3*** επικύρωσαν τη χρησιμότητα χαρακτηριστικών, όπως οι πόροι, οι αρχικές παρυφές, οι κουκκίδες και τα περιγράμματα παρυφής στην αντιστοίχιση δακτυλικών αποτυπωμάτων. Πρότειναν σχέδια που ενσωματώνουν και τις μικρολεπτομέρειες των παρυφών, εκτός από τις συμβατικές μικρολεπτομέρειες, και πέτυχαν έτσι βελτιωμένη απόδοση. Παρόλα αυτά, η χρήση των χαρακτηριστικών επιπέδου 3 εξετάστηκε μόνο σε εικόνες δακτυλικών αποτυπωμάτων υψηλής ανάλυσης 1000 dpi και άνω, ενώ οι περισσότερες από τις συμβατικές εικόνες δακτυλικών αποτυπωμάτων είχαν ανάλυση 500 dpi (Ashbaugh, 1999).

1.5 Επαλήθευση, Ταυτοποίηση και Ταξινόμηση

Διάφορα προβλήματα που προκύπτουν στην αναγνώριση των δακτυλικών αποτυπωμάτων, μαζί με τους σχετικούς αλγορίθμους και τα συστήματά τους, είναι η επαλήθευση, η ταυτοποίηση και η ταξινόμηση. Ο όρος *αναγνώριση* χρησιμοποιείται ως γενική έννοια και περιλαμβάνει και τα τρία αυτά είδη εργασιών.

Τα ***Συστήματα Επαλήθευσης*** *(Verification Systems)* χρησιμοποιούν την τεχνολογία των δακτυλικών αποτυπωμάτων για να επαληθεύσουν την απαιτούμενη ταυτότητα ενός ανθρώπου. Τέτοια συστήματα δέχονται σαν εισόδους δύο γνωρίσματα: την ταυτότητα του χρήστη για τον οποίο απαιτείται πιστοποίηση (συνήθως ένα όνομα ή μια έξυπνη κάρτα) και το σαρωμένο δακτυλικό του αποτύπωμα, το οποίο σαρώνεται εκείνη τη στιγμή. Η ταυτότητα του χρήστη χρησιμοποιείται για να ανακτήσει μια αναφορά του δακτυλικού αποτυπώματος που είναι ήδη αποθηκευμένο στη βάση δεδομένων και ταιριάζει με αυτό που δόθηκε στον σαρωτή για έλεγχο. Αυτό έχει ως αποτέλεσμα να ελέγχεται αν υπάρχει ομοιότητα, πάνω στην οποία βασίζεται και η απόφαση για την επαλήθευση του συγκεκριμένου χρήστη.

Τα ***Συστήματα Ταυτοποίησης*** *(Identification Systems)* επιτυγχάνουν την ταυτοποίηση ενός ανθρώπου με βάση το δακτυλικό του αποτύπωμα. Τέτοια συστήματα δέχονται μόνο μια είσοδο, η οποία είναι απλά το σαρωμένο δακτυλικό αποτύπωμα. Μέσα στη βάση δεδομένων του συστήματος γίνεται αναζήτηση ενός ταιριαστού δακτυλικού αποτυπώματος, η οποία διαδικασία αναφέρεται και ως αναζήτηση ενός προς πολλά (1:N). Ο χρήστης ταυτοποιείται εφόσον βρεθεί στη βάση δεδομένων ένα δακτυλικό αποτύπωμα που να ταιριάζει με το δικό του. Το σύστημα τότε παραθέτει την ταυτότητα που αντιστοιχεί στο δακτυλικό αποτύπωμα του ατόμου αυτού. Από την άλλη, αν δεν βρεθεί στη βάση δεδομένων ταιριαστό δακτυλικό αποτύπωμα, το άτομο αυτό απορρίπτεται. Τόσο για τα συστήματα επαλήθευσης όσο και για τα συστήματα ταυτοποίησης, η ***εγγραφή*** είναι ένα πολύ σημαντικό βήμα. Πρόκειται για τη διαδικασία που λαμβάνει τις αναφορές δακτυλικών αποτυπωμάτων από όλους τους χρήστες και τις αποθηκεύει στη βάση δεδομένων ώστε να μπορούν να γίνονται οι απαραίτητες συγκρίσεις.

Ο ρόλος ενός ***Συστήματος Ταξινόμησης*** *(Classification System)* είναι να καθορίζει σε ποια κλάση (ομάδα) ανήκει το εκάστοτε δακτυλικό αποτύπωμα. Τα συστήματα αυτά δέχονται επίσης σαν είσοδο μόνο το δακτυλικό αποτύπωμα. Ένα πολύ παλιό και γνωστό τέτοιο σύστημα είναι το σύστημα ταξινόμησης Henry, με βάση το οποίο τα δακτυλικά αποτυπώματα ταξινομούνται σύμφωνα με την φυσιολογία τους και γίνεται αναζήτηση ενός προς πολλούς (1:N). Υλοποιήθηκε από τους Hem Chandra Bose, Qazi Azizul Haque και Sir Edward Henry στα τέλη του 19ου αιώνα για ποινικούς σκοπούς και αποτέλεσε τη βάση για τα νέα συστήματα ταξινόμησης AFIS (Automated Fingerprint Identification Systems) μέχρι τη δεκαετία του ‘90. Η ταξινόμηση μπορεί να αποτελέσει ένα αρχικό βήμα για το στάδιο της ταυτοποίησης, καθώς μειώνει τον αριθμό των καταχωρήσεων προς αναζήτηση σε μια βάση δεδομένων.

1.6 Εφαρμογές Αναγνώρισης Δακτυλικών Αποτυπωμάτων

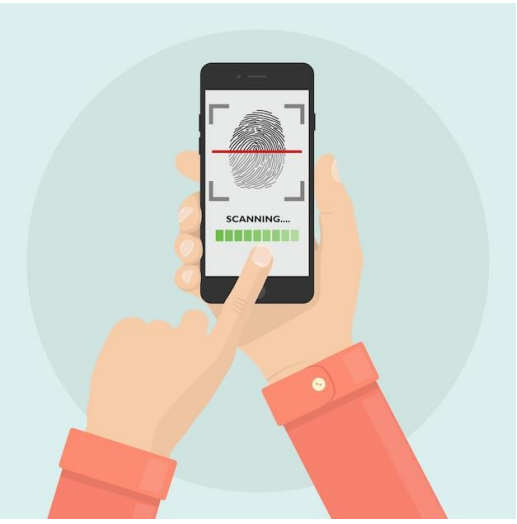
Μια σειρά από εφαρμογές όπως είναι τα βιομετρικά συστήματα ελέγχου πρόσβασης, η ταυτοποίηση στο διαδίκτυο, οι ψηφιακές υπογραφές και οι βιομετρικές θυρίδες χωρίς κλειδιά έχουν ήδη αναπτυχθεί, ενώ τα τελευταία χρόνια πραγματοποιούνται και ταυτοποιήσεις μέσω έξυπνων βιομετρικών καρτών και ευέλικτων αισθητήρων δακτυλικών αποτυπωμάτων.

Ο *βιομετρικός έλεγχος πρόσβασης* αποτελεί μια από τις πρώτες εφαρμογές βιομετρικών τεχνικών. Ο στόχος αυτής της παραδοσιακής εφαρμογής είναι να παρέχει έλεγχο πρόσβασης υψηλής ασφαλείας σε διάφορους τομείς, όπως είναι οι επιχειρήσεις, η υγειονομική περίθαλψη και οι κρατικές εγκαταστάσεις. Παρέχοντας, επομένως, σημαντικά υψηλή ασφάλεια και ευκολία, οι βιομετρικές τεχνολογίες κάνουν μεγάλη διαφορά σε αυτόν τον τομέα. Ένας μεγάλος αριθμός οργανισμών έχει αντικαταστήσει τα πιο παραδοσιακά συστήματα ασφαλείας τους, όπως οι συσκευές ανάγνωσης καρτών/κλειδιών, με συστήματα που επιτρέπουν την πρόσβαση μέσω σάρωσης δακτυλικών αποτυπωμάτων. Όπως είναι λογικό οι κάρτες εισόδου ενδέχεται να πέσουν σε λάθος χέρια, ωστόσο τα βιομετρικά στοιχεία είναι αυτά που παρέχουν βελτιωμένη ασφάλεια διασφαλίζοντας ότι το άτομο που επιθυμεί πρόσβαση σε έναν χώρο είναι και εξουσιοδοτημένο. Τα βιομετρικά συστήματα ελέγχου πρόσβασης είναι επίσης πιο βολικά, καθώς τα εξουσιοδοτημένα άτομα μπορούν εύκολα να αποκτήσουν πρόσβαση χωρίς να χρειάζεται να ανησυχούν μήπως ξεχάσουν τα διαπιστευτήριά τους στο σπίτι. Μια δημοφιλής λύση ελέγχου πρόσβασης από την IDEMIA, για παράδειγμα, διευκολύνει τη γρήγορη είσοδο σε εκατοντάδες άτομα με ένα απλό κούνημα του χεριού. Επίσης, αναδεικνύονται λύσεις ελέγχου πρόσβασης για φορητές συσκευές που βασίζονται στην αναγνώριση προσώπου και επιτρέπουν στους χρήστες να επιβεβαιώνουν την ταυτότητά τους μέσω μιας φωτογραφίας selfie ή τοποθετώντας το δακτυλικό αποτύπωμα στον ειδικό αισθητήρα της συσκευής. Αυτές είναι μερικές μόνο από τις καινοτομίες που συμβάλλουν στο να γίνει ο βιομετρικός έλεγχος πρόσβασης η προτιμώμενη προσέγγιση για την ασφάλεια των χώρων και των εγκαταστάσεων.

Η συνεχής καθημερινή χρήση του Παγκόσμιου Ιστού από τους ανθρώπους δημιουργεί την ανάγκη για *ταυτοποίηση μέσω διαδικτύου*, καθώς το ηλεκτρονικό εμπόριο και, ειδικότερα, οι εφαρμογές που επιτρέπουν την απομακρυσμένη πρόσβαση σε πόρους κάθε είδους, προκαλεί ιδιαίτερο ενδιαφέρον. Ακόμα κι αν προσφέρει μεγάλες ευκαιρίες, δεν πρέπει να υποτιμηθούν οι κίνδυνοι που επιφυλάσσει. Πρόκειται για έναν τομέα όπου υπάρχει έντονη ανάγκη για ασφάλεια. Συχνά είναι απαραίτητο να επαληθευτεί η ταυτότητα ενός χρήστη στο Διαδίκτυο όταν αυτός είναι συνδεδεμένος σε έναν ιστότοπο που προσφέρει κάποιο είδος υπηρεσίας. Οι κωδικοί πρόσβασης δεν αποτελούν πάντα μια ασφαλή λύση, καθώς μπορούν να κλαπούν ή να μοιραστούν σε περισσότερους χρήστες. Τα βιομετρικά στοιχεία είναι αυτά που παρέχουν μια φυσική λύση για απομακρυσμένο έλεγχο της ταυτότητας ενός χρήστη. Όταν

ένας ιστότοπος, για παράδειγμα, απαιτεί την εισαγωγή κωδικού πρόσβασης, το σύστημα αναγνωρίζει το προφίλ του χρήστη και απαιτεί βιομετρικό έλεγχο ταυτότητας, δηλαδή μόλις επαληθευτεί η ταυτότητά του, το σύστημα παρέχει αυτόματα τον σωστό κωδικό πρόσβασης στην εφαρμογή ή τον ιστότοπο. Μεταξύ των εφαρμογών που σήμερα μπορούν να επωφεληθούν πολύ από μια τέτοια τεχνολογία είναι το e-banking, το ηλεκτρονικό εμπόριο, η πρόσβαση σε απομακρυσμένα αρχεία ή κατανεμημένες βάσεις δεδομένων, η ασφαλής λήψη/φόρτωση εγγράφων σε απομακρυσμένα αρχεία κ.ά.

Πρόσφατα, πολλές χώρες έχουν θεσπίσει νόμους που προσδίδουν νομική αξία στην *ψηφιακή υπογραφή*. Η ψηφιακή υπογραφή είναι ένας όρος που χρησιμοποιεί ένα ζεύγος κλειδιών χρήστη για την υπογραφή και την επαλήθευση ενός εγγράφου. Αποτελεί απόδειξη ότι ένα ψηφιακό μήνυμα ή έγγραφο δεν τροποποιήθηκε (σκόπιμα ή ακούσια) από τη στιγμή που υπογράφηκε. Οι χρήστες μπορούν να δημιουργήσουν την δική τους ψηφιακή υπογραφή χρησιμοποιώντας βιομετρική τεχνολογία, δηλαδή με τη χρήση δακτυλικών αποτυπωμάτων. Όταν ένας χρήστης, για παράδειγμα, στείλει ένα έγγραφο σε έναν άλλον, ο χρήστης που στέλνει το έγγραφο πρέπει να τοποθετήσει το δακτυλικό του αποτύπωμα στον αισθητήρα δακτυλικών αποτυπωμάτων της συσκευής που χρησιμοποιεί (πχ. κινητό ή laptop) και το έγγραφο αυτό θα κρυπτογραφηθεί. Μόλις ολοκληρωθεί αυτή η διαδικασία, το ψηφιακό έγγραφο υπογράφεται ψηφιακά και αποστέλλεται στον παραλήπτη. Στη συνέχεια, ο χρήστης που λαμβάνει το κρυπτογραφημένο μήνυμα θα το αποκρυπτογραφήσει χρησιμοποιώντας το δημόσιο κλειδί του αποστολέα. Εάν ταιριάζουν, το ψηφιακό έγγραφο τότε δεν έχει τροποποιηθεί και ο αποστολέας έχει επικυρωθεί. Ένας τέτοιος αλγόριθμος ζεύγους κλειδιών για αυτό το σύστημα, μπορεί να επιτευχθεί μέσα από έναν αλγόριθμο κρυπτογράφησης RSA (Rahmawati, Listyasari, Aziz, Sukaridhoto, Damastuti, Bachtiar & Sudarsono, 2017).



Εικόνα 1.11: Ψηφιακή βιομετρική υπογραφή

Οι περισσότεροι χώροι αθλήσεως, όπως γυμναστήρια ή κολυμβητήρια, διαθέτουν ντουλάπια στα οποία οι αθλητές μπορούν να αφήσουν τα πολύτιμα πράγματά τους. Τα συνηθισμένα ντουλάπια με κλειδαριά απαιτούν από τον άνθρωπο να κουβαλάει το κλειδί κατά τη διάρκεια της προπόνησης. Καθώς αυτό είναι αρκετά άβολο και επικίνδυνο να χαθεί, η χρήση δακτυλικού αποτυπώματος για την αντικατάσταση του κλειδιού είναι μια ελκυστικά εναλλακτική λύση. Τα *βιομετρικά ντουλάπια χωρίς κλειδί* έχουν δοκιμαστεί σε πολλά πιλοτικά έργα. Οι θυρίδες αυτές ελέγχονται από κοινού από έναν μικροϋπολογιστή που είναι συνδεδεμένος με έναν αισθητήρα δακτυλικών αποτυπωμάτων. Αυτή η εφαρμογή, ωστόσο, επιφέρει πολλές ειδικές προκλήσεις. Πρώτον, η αναγνώριση των βρεγμένων δακτύλων μετά από μια προπόνηση προκαλεί διάφορα προβλήματα, όπως μειωμένη ποιότητα της εικόνας των δακτυλικών αποτυπωμάτων. Αυτό το πρόβλημα διογκώνεται από το γεγονός ότι το στρώμα του λίπους στην επιφάνεια του δέρματος μειώνεται λόγω παρατεταμένης παραμονής στο ενισχυμένο με χλώριο νερό. Επίσης, το νερό κάνει το δέρμα να εφαρμόζει λιγότερο σφιχτά γύρω από το δάχτυλο, με αποτέλεσμα να προκαλούνται σημαντικά υψηλές ελαστικές παραμορφώσεις του δακτυλικού αποτυπώματος, μειώνοντας έτσι την απόδοση στο σύστημα.

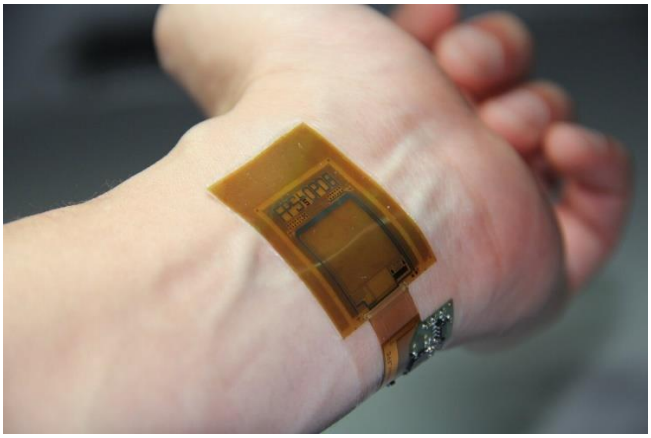
Εικόνα 1.12: Βιομετρική κλειδαριά

Οι *έξυπνες βιομετρικές κάρτες*, όπως υποδηλώνει το όνομά τους, είναι πλαστικές κάρτες με ολοκληρωμένα κυκλώματα που τους επιτρέπουν να περιέχουν σημαντικά δεδομένα. Οι πιο συνηθισμένες από αυτές είναι οι σύγχρονες πιστωτικές και χρεωστικές κάρτες, καθώς και, σε ορισμένες χώρες, οι εθνικές κάρτες ταυτότητας. Οι κάρτες αυτές περιέχουν βιομετρικά δεδομένα που χρησιμοποιούνται για σκοπούς ταυτοποίησης και επαλήθευσης ταυτότητας. Παρόλο που περιέχουν απλώς βιομετρικά δεδομένα που μπορούν να συγκριθούν με αυτά που καταγράφονται από μια ξεχωριστή

βιομετρική συσκευή ανάγνωσης με σκοπό την επαλήθευση της ταυτότητας του χρήστη, οι νέες εξελίξεις στην παραγωγή αισθητήρων δακτυλικών αποτυπωμάτων οδήγησαν στην εμφάνιση ενός νέου τύπου έξυπνης κάρτας με ενσωματωμένο βιομετρικό αισθητήρα, ικανό να εκτελεί αντιστοίχιση ένα προς ένα (1:1) στη συσκευή.

Εικόνα 1.13: Έξυπνη βιομετρική κάρτα

Πλέον οι αισθητήρες δακτυλικών αποτυπωμάτων βρίσκονται σε κάθε συσκευή κινητού τηλεφώνου σε όλο το φάσμα τιμών, και συνεπώς οι μεγάλοι κατασκευαστές αισθητήρων αναγκάζονται να επικεντρώνουν τις προσπάθειές τους για να φέρουν την τεχνολογία τους στις έξυπνες κάρτες. Η εστίαση αυτή τροφοδότησε μια καινοτομία, οδηγώντας σε εφευρέσεις όπως ο *ευέλικτος αισθητήρας δακτυλικών αποτυπωμάτων* – μια κρίσιμη εξέλιξη που βοήθησε να ανοίξει ο δρόμος για βιομετρικές κάρτες πληρωμών. Αυτό προέκυψε από την ανάγκη για εξαιρετικά λεπτούς αισθητήρες που μπορούν να εφαρμοστούν σε μη επίπεδες επιφάνειες και που μπορούν να κατασκευαστούν σε μεγάλες επιφάνειες. Έχουν την ικανότητα να κατασκευάζονται σε διάφορες μορφές επιτρέποντας την ενσωμάτωσή τους σε συσκευές με διάφορα σχέδια. Δεδομένου ότι είναι κατασκευασμένοι από πλαστικό, προσφέρουν πλεονεκτήματα κόστους για κατασκευή μεγάλων επιφανειών. Η FlexEnable ανέπτυξε τον πρώτο στον κόσμο εύκαμπτο αισθητήρα δακτυλικών αποτυπωμάτων 500 dpi σε πλαστικό. Ο οπτικός αισθητήρας πάχους 0,3 χιλιοστών επιτρέπει τη σάρωση δακτυλικών αποτυπωμάτων μικρής και μεγάλης περιοχής και μπορεί επίσης να απεικονίσει φλέβες. Η δυνατότητα λήψης τόσο των δακτυλικών αποτυπωμάτων όσο και των φλεβών καθιστά αυτή τη λύση μοναδική καθώς παρέχει δύο τρόπους ελέγχου ταυτότητας και μια λειτουργία για ανίχνευση ζωντάνιας.



Εικόνα 1.14: Εύκαμπτος βιομετρικός αισθητήρας

1.7 Συσκευές Σάρωσης Δακτυλικών Αποτυπωμάτων

Τα δακτυλικά αποτυπώματα είναι μια αξιόπιστη μέθοδος για την επαλήθευση της προσωπικής ταυτότητας κάθε ανθρώπου. Σε συνδυασμό με την αναγνώριση προσώπου (face ID) ή άλλα βιομετρικά συστήματα ταυτοποίησης, όπως η σάρωση αμφιβληστροειδούς, τα δακτυλικά αποτυπώματα προσφέρουν έναν άψογο τρόπο αναγνώρισης οποιουδήποτε ανθρώπου. Πολλές εφαρμογές του Διαδικτύου των Πραγμάτων (IoT), όπως ο έξυπνος οικιακός αυτοματισμός και οι εφαρμογές ψηφιακής ασφάλειας, χρησιμοποιούν ήδη σαρωτές δακτυλικών αποτυπωμάτων οπουδήποτε απαιτείται αναγνώριση χρήστη, έλεγχος ταυτότητας ή πιστοποίηση.

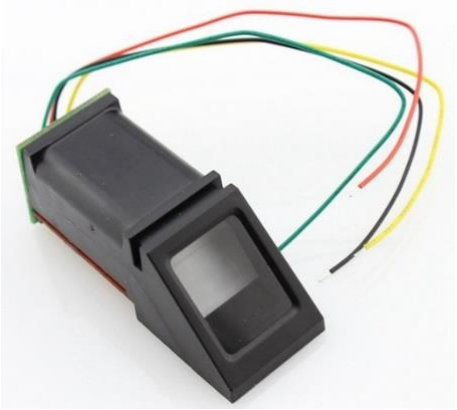
Οποιοσδήποτε σαρωτής δακτυλικών αποτυπωμάτων, ανεξάρτητα από τα ηλεκτρονικά του μέρη, σαρώνει μια ψηφιακή εικόνα του δακτυλικού αποτυπώματος. Το δείγμα της εικόνας αυτής αποθηκεύεται στη μνήμη και χρησιμοποιείται για σύγκριση με μελλοντικές σαρώσεις. Όπως το δακτυλικό αποτύπωμα, έτσι και τα σχήματα και οι διαστάσεις που προκύπτουν είναι πάντα μοναδικά. Προσδιορίζοντας έναν επαρκή αριθμό μικρολεπτομερειών, τις απόλυτες θέσεις τους στη σάρωση και το σχετικό μοτίβο, ένας σαρωτής μπορεί να αναγνωρίσει ένα συγκεκριμένο δακτυλικό αποτύπωμα μοναδικά. Όλα αυτά περιλαμβάνουν πολύπλοκους αλγόριθμους επεξεργασίας εικόνας.

Πολλοί σαρωτές δακτυλικών αποτυπωμάτων διαθέτουν επιπρόσθετους αισθητήρες, όπως αισθητήρες παλμών ή αισθητήρες θερμότητας προκειμένου να προσδιορίσουν εάν η σαρωμένη εικόνα προέρχεται από δάκτυλο ή όχι. Ορισμένες φορές είναι δυνατό τα δακτυλικά αποτυπώματα να πλαστογραφηθούν χρησιμοποιώντας εκτυπωμένη εικόνα, καλούπι από δάκτυλο ή μέσω κλωνοποίησης από υπολείμματα άλλων δακτυλικών αποτυπωμάτων. Η χρήση πρόσθετων αισθητήρων επίσης βοηθά στην ανίχνευση ατυχημάτων (π.χ. γρατζουνιών, κοψιμάτων).

Στην ηλεκτρονική υπάρχουν τρεις τύποι σαρωτών δακτυλικών αποτυπωμάτων: οπτικοί σαρωτές, χωρητικοί σαρωτές και σαρωτές υπερήχων (π.χ. σε οθόνη). Σε ενσωματωμένες εφαρμογές, οι οπτικοί και οι χωρητικοί σαρωτές είναι πιο συνηθισμένοι. Οι κινητές συσκευές και τα smartwatches έχουν ως επί το πλείστων χωρητικούς σαρωτές ή σαρωτές υπερήχων στην οθόνη.

1.7.1 Οπτικοί Σαρωτές

Οι οπτικοί σαρωτές είναι τα παλαιότερα μοντέλα σαρωτών δακτυλικών αποτυπωμάτων. Όπως υποδηλώνει το όνομά τους, αυτοί οι σαρωτές καταγράφουν την οπτική εικόνα του δακτυλικού αποτυπώματος χρησιμοποιώντας αισθητήρες εικόνας CCD ή CMOS. Είναι παρόμοιοι με τους αισθητήρες κάμερας, αν και έχουν σχεδιαστεί για λήψη εικόνων υψηλής αντίθεσης σε σχέση με μια οποιαδήποτε κανονική κάμερα. Ο εν λόγω σαρωτής αποτελείται από μια σειρά από LED και οι αισθητήρες CCD/CMOS καταγράφουν το φως στις περιοχές του δακτύλου και τα ανακλώμενα κύματα φωτός. Προκειμένου να ληφθεί μια λεπτομερή εικόνα του δακτυλικού αποτυπώματος, ο αισθητήρας είναι γεμάτος με υψηλή πυκνότητα διόδων. Η εικόνα αυτή είναι μιας 2D διάστασης του σαρωμένου δακτυλικού αποτυπώματος. Τα πιο πρόσφατα μοντέλα έχουν διαστάσεις μόλις 1 χιλιοστού και μπορούν να σαρώσουν ακόμη και βρεγμένα δάχτυλα. Καθώς το κόστος αγοράς τους μειώνεται σταδιακά, οι υβριδικοί σαρωτές οπτικής-χωρητικότητας που μπορούν να ανιχνεύουν ζωντανά δάχτυλα είναι πλέον πιο διαδεδομένοι (Fujieda, Ono & Sugama, 1995).

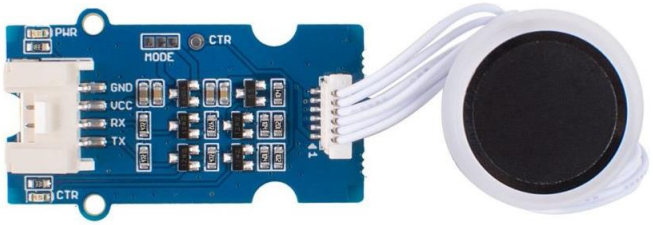


Εικόνα 1.15: Οπτικός σαρωτής

Οι οπτικοί σαρωτές, παρά τις τρέχουσες εξελίξεις, εξακολουθούν να είναι εύκολο να εξαπατηθούν. Τα δακτυλικά αποτυπώματα μπορούν να πλαστογραφηθούν αν κάποιος χρήστης χρησιμοποιήσει μια εικόνα από ένα δακτυλικό αποτύπωμα με πολύ υψηλή ανάλυση, ένα πρόσθετο ή ένα τεχνητό δάκτυλο.

1.7.2 Χωρητικοί Σαρωτές

Οι χωρητικοί σαρωτές χρησιμοποιούν εντελώς διαφορετική τεχνολογία για την ανάγνωση ενός δακτυλικού αποτυπώματος. Χρησιμοποιούν μια σειρά από εκατοντάδες μικρούς πυκνωτές για την ανίχνευση της χωρητικότητας μεταξύ της πλάκας του πυκνωτή και των παρυφών-κοιλάδων. Όπου υπάρχει μια παρυφή, η απόστασή της από την πλάκα του πυκνωτή είναι μικρή, με αποτέλεσμα η χωρητικότητα να είναι αρκετά μικρή. Όπου υπάρχει κοιλάδα, η απόστασή της με την πλάκα του πυκνωτή είναι μεγάλη δημιουργώντας ένα διάκενο αέρα ενδιάμεσα. Αυτό έχει ως αποτέλεσμα μεγαλύτερη χωρητικότητα. Η χωρητικότητα από κάθε πυκνωτή στη συστοιχία μεταβιβάζεται στον λειτουργικό ενισχυτή και καταγράφεται με τη βοήθεια μετατροπέων A/D αναλογικού σε ψηφιακό. Αυτό παράγει μια ψηφιακή σάρωση του δακτυλικού αποτυπώματος σύμφωνα με την χωρητική αίσθηση αφής (Edwards, 1984).



Εικόνα 1.16: Χωρητικός σαρωτής

Οι χωρητικοί σαρωτές, σε αντίθεση με τους οπτικούς, δεν είναι εύκολο να εξαπατηθούν, καθώς μπορούν ακόμη και να ανιχνεύσουν ένα ζωντανό δάκτυλο. Ο μόνος τρόπος για να «ξεγελάσει» κάποιος τον χωρητικό σαρωτή είναι να χακάρει το hardware ή το λογισμικό του ελεγκτή αν έχει πρόσβαση. Διαφορετικά, αυτοί οι σαρωτές δεν μπορούν να εξαπατηθούν από μια τυπωμένη εικόνα ή κάποιο πρόσθετο δάκτυλο. Μια τυπωμένη εικόνα θα έχει προφανώς και διαφορετικά χωρητικά αποτελέσματα, όπως επίσης και ένα πρόσθετο δάκτυλο δεν θα μπορέσει να μιμηθεί ακριβώς τη χωρητικότητα αφής ενός ζωντανού.

1.7.3 Σαρωτές Υπερήχων

Οι σαρωτές υπερήχων είναι οι πιο πρόσφατοι και πιο εξελιγμένοι σαρωτές δακτυλικών αποτυπωμάτων, καθώς μπορούν να παράγουν τρισδιάστατες σαρώσεις δακτυλικών αποτυπωμάτων. Σε έναν σαρωτή υπερήχων υπάρχει μια σειρά από πομπούς και δέκτες υπερήχων. Οι πομποί εκπέμπουν υπερηχητικούς παλμούς που αντανακλώνται στις κορυφογραμμές, τις κοιλάδες και τους πόρους του δακτυλικού αποτυπώματος. Μια παράταξη από δέκτες ανιχνεύει τους ανακλώμενους παλμούς. Οι δέκτες είναι στην πραγματικότητα αισθητήρες που μετρούν τη μηχανική καταπόνηση λόγω της έντασης των ανακλώμενων υπερηχητικών παλμών σε διαφορετικά σημεία. Αυτό οδηγεί στον σχεδιασμό ενός τρισδιάστατου χάρτη από σαρωμένα δακτυλικά αποτυπώματα, ο οποίος οφείλει να είναι λεπτομερής σε σύγκριση με τη δισδιάστατη σάρωση οποιουδήποτε χωρητικού σαρωτή.

Οι σαρωτές υπερήχων απαιτούν λίγο χρόνο για να αποτυπώσουν αποτελεσματικά τον τρισδιάστατο χάρτη ενός δακτυλικού αποτυπώματος και είναι εύκολο να εφαρμοστούν. Συχνά χρησιμοποιούνται για σαρωτές στην οθόνη ενός κινητού τηλεφώνου. Είναι σχεδόν αδύνατο να δημιουργηθούν σαρωτές υπερήχων όπως οι χωρητικοί σαρωτές. Η λειτουργία 3D του σαρωμένου δακτυλικού αποτυπώματος κάνει την τεχνολογία ακόμα πιο στιβαρή. Όπως ισχύει και για τους χωρητικούς αισθητήρες, οι σαρωτές υπερήχων μπορούν επίσης να πλαστογραφηθούν μόνο με παραβίαση του υλικού ή του λογισμικού. Επιπλέον, είναι εύκολοι και οικονομικά αποδοτικοί στην εφαρμογή τους για αυτό και θεωρούνται σχεδόν άψογοι.

Εικόνα 1.17: Σαρωτής υπερήχων στην οθόνη ενός smartphone

Οι σαρωτές δακτυλικών αποτυπωμάτων είναι αδιαμφισβήτητα εύχρηστες συσκευές. Σε συνδυασμό με άλλες βιομετρικές μεθόδους ή μεθόδους ελέγχου ταυτότητας, συντελούν στην υλοποίηση ενός

αλάνθαστου συστήματος αναγνώρισης ατόμου. Αυτό μπορεί να περιλαμβάνει την ενσωμάτωση άλλων συστημάτων τύπου «ποιος είσαι;» όπως σάρωση αμφιβληστροειδούς ή ίριδας, συστήματα τύπου «τι γνωρίζεις;» όπως κωδικοί PIN ή συστήματα τύπου «τι έχεις;» όπως ετικέτες RFID ή έξυπνες κάρτες. Τα συστήματα βιομετρικής αναγνώρισης συνεπώς είναι χρήσιμα και για τον σχεδιασμό εφαρμογών IoT, καταγραφής και παρακολούθησης, έξυπνων κατοικιών και εφαρμογών ασφαλείας.

1.8 Συνθήκες που Επηρεάζουν τη Σάρωση

Ένα περιστασιακό πρόβλημα στα συστήματα δακτυλικών αποτυπωμάτων είναι η λήψη εικόνας με κακή ποιότητα. Η ποιότητα των δακτυλικών αποτυπωμάτων όχι μόνο ποικίλλει ευρέως, αλλά αλλάζει και με την πάροδο του χρόνου. Οι ηλικιωμένοι ή οι εργαζόμενοι χειρωνακτικών εργασιών τείνουν να έχουν φτωχότερα δακτυλικά αποτυπώματα. Ακόμη και το ίδιο δάκτυλο μπορεί να είναι διαφορετικό λόγω της κατάστασης του δέρματος τη δεδομένη χρονική στιγμή, των καιρικών συνθηκών και των εγκοπών των δακτύλων. Δεδομένου ότι η ποιότητα και η κατάσταση των ανθρώπινων δακτυλικών αποτυπωμάτων είναι αρκετά διαφορετικές, οι συσκευές λήψης εικόνων διαδραματίζουν κρίσιμο ρόλο δίνοντας ένα σωστό αποτέλεσμα για το σύστημα ελέγχου ταυτότητας. Η ικανότητα λήψης ξηρών, υγρών ή άλλων δακτυλικών αποτυπωμάτων κακής ποιότητας γίνεται κρίσιμη στα εμπορικά συστήματα. Στην πραγματικότητα, η ποιότητα εικόνας για το δάκτυλο του ίδιου ατόμου μπορεί να διαφέρει από συσκευή σε συσκευή (Jain, Prabhakar & Ross, 1999).

(α) (β)

Εικόνα 1.18: Δακτυλικά αποτυπώματα σε διαφορετικές συνθήκες

(α) κανονικό, (β) ξηρό

(γ) (δ)

Εικόνα 1.19: Δακτυλικά αποτυπώματα σε διαφορετικές συνθήκες

(γ) υγρό, (δ) κακής ποιότητας

ΚΕΦΑΛΑΙΟ 2ο: Το Σύστημα Ελέγχου Πρόσβασης

2.1 Εισαγωγή

Στο 2ο κεφάλαιο παρουσιάζεται η ανάλυση της δομής και της λειτουργίας του συστήματος ασφαλείας μέσω βιομετρικών χαρακτηριστικών που αναπτύχθηκε στο πλαίσιο αυτής της διπλωματικής εργασίας. Τέλος, θα ακολουθήσει επεξήγηση για τα περιβάλλοντα στα οποία έγινε η υλοποίηση των προγραμμάτων σε δύο γλώσσες προγραμματισμού.

2.2 Οφέλη Ανάπτυξης ενός Βιομετρικού Συστήματος

Τα βιομετρικά συστήματα ελέγχου πρόσβασης διαμορφώνουν το μέλλον της ασφάλειας χώρων, όπως είναι οι επιχειρήσεις, σε όλο τον κόσμο. Με τις εξαιρετικές δυνατότητες συλλογής δεδομένων, αναγνώρισης και επαλήθευσης, τα βιομετρικά συστήματα ελέγχου πρόσβασης κρίνονται ως ζωτικής σημασίας για τη διαφύλαξη και την ασφάλεια πολλών βιομηχανιών και τομέων παγκοσμίως. Ένα τυπικό σύστημα βιομετρικής πρόσβασης αποτελείται από τέσσερις μονάδες, οι οποίες έχουν ως εξής:

- ***Συσκευή σάρωσης - αισθητήρας***

Μια συσκευή σάρωσης σε ένα σύστημα βιομετρικής πρόσβασης χρησιμοποιείται για τη λήψη της εισόδου (δηλαδή του δακτυλικού αποτυπώματος) που απαιτείται για την επαλήθευση του χρήστη. Η εικόνα που λαμβάνεται χρησιμοποιείται στη συνέχεια ως βάση για περαιτέρω ανάλυση.

- ***Μονάδα αξιολόγησης ποιότητας***

Μετά τη σάρωση της εικόνας ή τη συλλογή άλλης μορφής εισαγωγής, πρέπει να γίνει έλεγχος για το αν η ποιότητα είναι κατάλληλη προς σύγκριση με τα ήδη αποθηκευμένα πρότυπα. Ουσιαστικά, γίνεται χρήση ενός αλγορίθμου για την προσαρμογή της ποιότητας από τη λήψη που εισήχθη στο σύστημα, και σε περίπτωση που δεν είναι ικανοποιητική ο χρήστης αναγκάζεται να επαναλάβει την διαδικασία και να σαρώσει το δάκτυλό του από την αρχή. Στη συνέχεια, κατά την επεξεργασία, επιλέγεται ένα σύνολο ιδιαίτερων χαρακτηριστικών που χαρακτηρίζουν την ταυτότητα του χρήστη, όπως στην προκειμένη περίπτωση του δακτυλικού αποτυπώματος λαμβάνονται βιομετρικά σχέδια των παρυφών του δακτύλου. Το αρχικό δείγμα που λαμβάνεται για αξιολόγηση και εξαγωγή ορίζεται ως πρότυπο και αποθηκεύεται στη βάση δεδομένων του συστήματος.

- ***Μονάδα σύγκρισης και αντιστοίχισης χαρακτηριστικών***

Μόλις συλλεχθεί το βιομετρικό αυτό χαρακτηριστικό, συγκρίνεται με τα πρότυπα που είναι αποθηκευμένα στο σύστημα και αντιστοιχίζεται για να γίνει αναγνώριση. Ο αριθμός των χαρακτηριστικών που ταιριάζουν με το αποθηκευμένο πρότυπο καθορίζει και επιβεβαιώνει την ταυτότητα του χρήστη ή την απορρίπτει.

- ***Βάση δεδομένων***

Η βάση δεδομένων ενός βιομετρικού συστήματος ελέγχου πρόσβασης αποθηκεύει όλες τις σχετικές πληροφορίες που απαιτούνται για την επεξεργασία μιας δεδομένης εισόδου. Για τη βελτίωση του επιπέδου ασφαλείας, στο βιομετρικό πρότυπο συμπεριλαμβάνονται συγκεκριμένες πληροφορίες και βιογραφικά δεδομένα. Ο τύπος πρόσβασης που απαιτείται κάθε φορά μπορεί να είναι διαφορετικός, καθώς ο ίδιος ο χρήστης μπορεί να ορίσει το επίπεδο ασφάλειας ή σε άλλη περίπτωση για να δοθεί πρόσβαση σε έναν νέο υπάλληλο στην εταιρεία, ο διευθυντής μπορεί να ορίσει την απαιτούμενη ασφάλεια και να εισάγει τα διαπιστευτήρια του χρήστη υπό την επίβλεψή του.

Ένα βιομετρικό σύστημα προσφέρει υψηλότερο επίπεδο ασφαλείας από ένα τυπικό σύστημα ελέγχου πρόσβασης που βασίζεται στην εγγύτητα. Μερικά από τα οφέλη της χρήσης της βιομετρίας ως κύριο μέσο σε ένα σύστημα ελέγχου πρόσβασης είναι τα παρακάτω:

- ***Παρέχει υψηλή ασφάλεια***

Δεδομένου ότι τα βιομετρικά στοιχεία αξιοποιούν τη μοναδική φυσιολογία του κάθε ανθρώπου για την επαλήθευση της ταυτότητάς του, είναι εξαιρετικά δύσκολο να ληφθούν ή να χρησιμοποιηθούν από οποιονδήποτε άλλο εκτός από τον προβλεπόμενο χρήστη.

- ***Είναι δύσκολο να αντιγραφεί***

Τα παραδοσιακά συστήματα πρόσβασης μέσω κωδικών και καρτών μπορούσαν εύκολα να κλαπούν από τον χρήστη. Σε αντίθεση, τα βιομετρικά στοιχεία είναι πιο δύσκολο να πλαστογραφηθούν, διότι τα περισσότερα σύγχρονα βιομετρικά συστήματα χρησιμοποιούν «τεστ ζωντανότητας» για να εξασφαλίσουν ότι τα δεδομένα προέρχονται από πραγματικό άνθρωπο και όχι από πλαστό αντίγραφο.

- ***Ευκολία στη χρήση***

Δεν μπορεί ούτε να χαθεί ούτε να ξεχαστεί, μιας και ο χρήστης δεν χρειάζεται να έχει μαζί του τίποτε άλλο πέρα από τον εαυτό του.

- ***Ευκολία στην πρόσβαση***

Το βιομετρικό αναγνωριστικό είναι πάντα διαθέσιμο επάνω στους χρήστες, συνεπώς δεν χρειάζεται πλέον να ψάχνουν τις τσάντες τους για να βγάλουν κάρτα ή ταυτότητα.

- ***Αποδοτικότητα***

Τα περισσότερα βιομετρικά συστήματα είναι σε θέση να αναγνωρίσουν τους χρήστες σε ελάχιστα δευτερόλεπτα, εξαλείφοντας τις χρονικές καθυστερήσεις που προκαλούνται από μη αυτόματους ελέγχους ταυτότητας, κωδικούς πρόσβασης ή PIN.

- ***Εξοικονομεί χρήματα***

Στους εργασιακούς χώρους μειώνεται η ανάγκη για προσωπικό ασφαλείας στα σημεία ελέγχου πρόσβασης. Επιπλέον, στα παραδοσιακά συστήματα η έκδοση καρτών για έλεγχο ήταν αρκετά δαπανηρή, ειδικότερα στις περιπτώσεις όπου οι υπάλληλοι έχαναν την κάρτα τους και χρειάζονταν επανέκδοση.

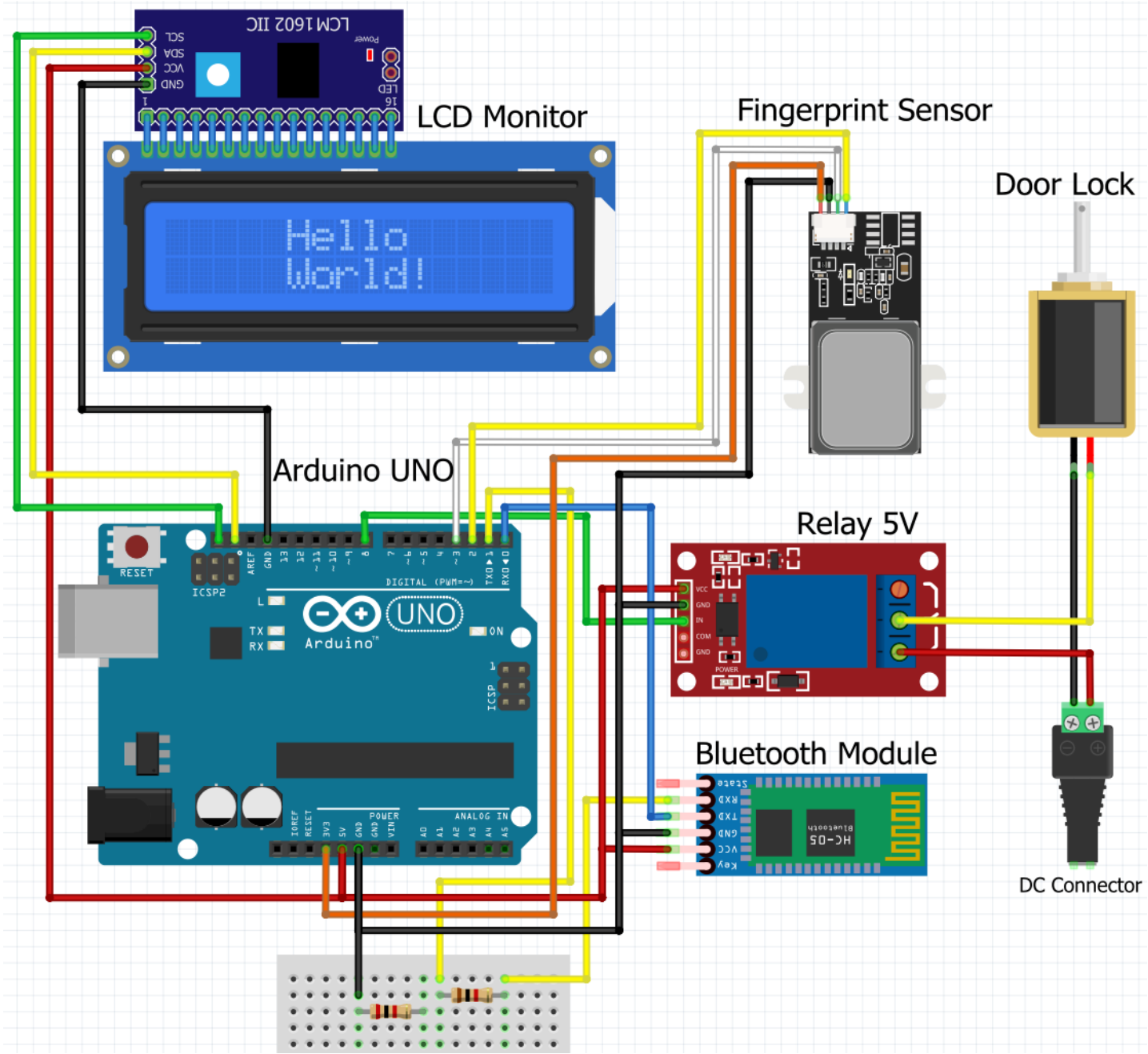
2.3 Λειτουργία και Ανάπτυξη του Συστήματος

Για την λειτουργία του συστήματος ελέγχου πρόσβασης απαιτείται πρώτα η εγγραφή των απαραίτητων δακτυλικών αποτυπωμάτων, μέσω του οπτικού αισθητήρα, και η αποθήκευσή τους στη βάση δεδομένων. Η μονάδα αναγνώρισης που χρησιμοποιείται μπορεί να αποθηκεύσει έως και 240 πρότυπα. Η διαδικασία αυτή μπορεί να εκτελεστεί μόνο από τον διαχειριστή του συστήματος και όχι από τους χρήστες που επιθυμούν την πρόσβαση στον χώρο που βρίσκεται τοποθετημένο το σύστημα. Καθώς το πρόγραμμα στο Arduino εκτελείται, γίνεται σύγκριση των ήδη αποθηκευμένων προτύπων με κάθε δάκτυλο που ακουμπάει την μονάδα σάρωσης.

Εφόσον το σύστημα αναγνωρίσει το δακτυλικό αποτύπωμα που περνάει από την σάρωση, δίνει την εντολή ώστε να ανοίξει η κλειδαριά και ο χρήστης να αποκτήσει την επιθυμητή πρόσβαση. Σε αντίθετη περίπτωση, όπου δηλαδή το σύστημα δεν μπορέσει να ταυτίσει το σαρωμένο δακτυλικό αποτύπωμα με κάποιο από αυτά της βάσης δεδομένων, τότε αυτό απαγορεύει την πρόσβαση στον συγκεκριμένο χρήστη. Η προσπάθεια αυτή μπορεί να πραγματοποιηθεί εσφαλμένα έως και 3 φορές. Έπειτα από αυτό,

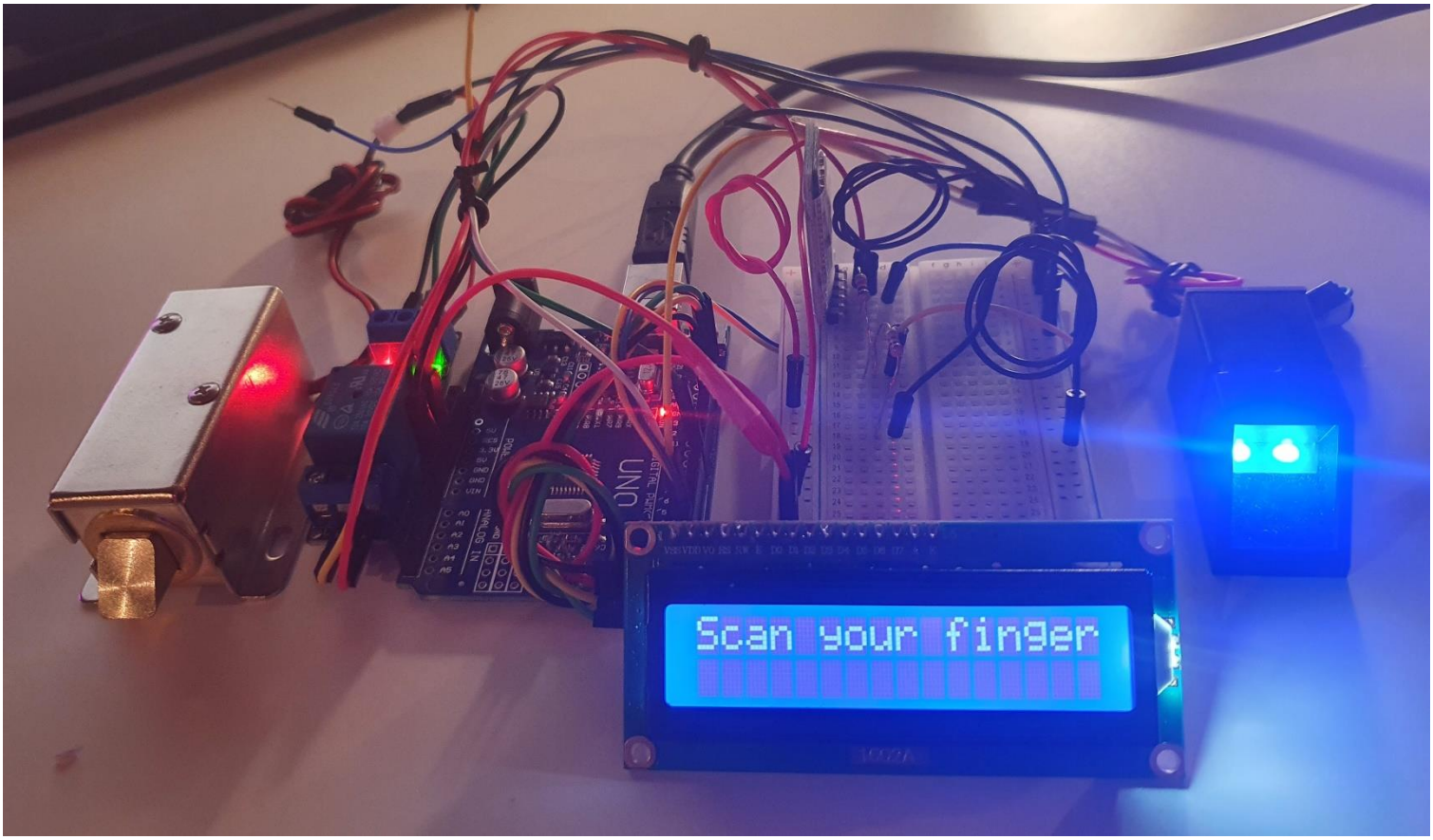
το σύστημα «μπλοκάρει» και αποτρέπει τον χρήστη από το να συνεχίσει να προσπαθεί να πετύχει είσοδο. Αυτό συμβαίνει για λόγους ασφαλείας και αποτρέπει τυχόν παραβιάσεις. Σε αυτό το σημείο, το σύστημα ειδοποιεί με μήνυμα τον διαχειριστή στην εφαρμογή που εκείνος έχει στο κινητό του και με το πάτημα ενός κουμπιού, στέλνει εντολή στο Arduino να «ξεμπλοκάρει» και να συνεχίσει η σάρωση δακτυλικών αποτυπωμάτων ξανά.

Η συνδεσμολογία του κυκλώματος σε breadboard παρουσιάζεται παρακάτω και σχεδιάστηκε στο πρόγραμμα Fritzing:



Εικόνα 2.1: Συνδεσμολογία

Η τελική υλοποίηση του κυκλώματος παρουσιάζεται στην παρακάτω φωτογραφία:



Εικόνα 2.2: Υλοποίηση του συστήματος

Οι συνδέσεις προκύπτουν ως εξής:

Arduino:

Τροφοδοσία μέσω 5V τροφοδοσίας με USB

Οθόνη LCD:

VCC → 5V Power pin στο Arduino

GND → GND στο Arduino

SDA → SDA στο Arduino

SCL → SCL στο Arduino

Οπτικός αισθητήρας:

VCC → 3.3V Power pin στο Arduino

GND → GND στο Arduino

Tx → Digital pin 2 στο Arduino

Rx → Digital pin 3 στο Arduino

Bluetooth HC-05 και αντιστάσεις:

VCC → 5V Power pin στο Arduino

GND → GND στο Arduino

Rx → 1KΩ αντίσταση

1KΩ αντίσταση → 2KΩ αντίσταση

2KΩ αντίσταση και 1KΩ αντίσταση → Tx στο Arduino

2KΩ → GND στο Arduino

Tx → Rx στο Arduino

DC ρελέ:

VCC → 5V Power pin στο Arduino

GND → GND στο Arduino

IN→ Digital pin 8 στο Arduino

NO → Θετικός πόλος (+) στον DC connector

COM → Θετικός πόλος (+) στην κλειδαριά

DC connector:

Θετικός πόλος (+) → NO του DC ρελέ

Αρνητικός πόλος (-) → Αρνητικός πόλος (-) στην κλειδαριά

Κλειδαριά:

Θετικός πόλος (+) → COM του DC ρελέ

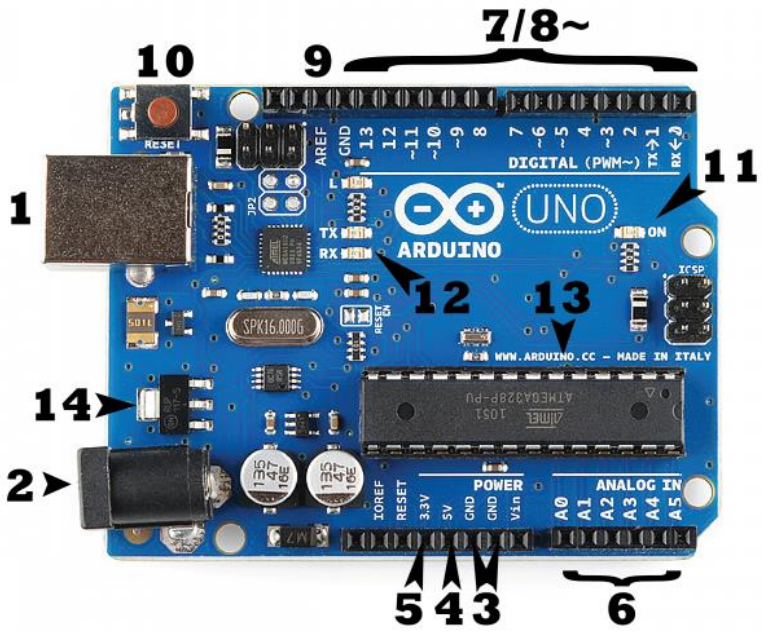
Αρνητικός πόλος (-) → Αρνητικός πόλος (-) στον DC connector

2.4 Μέρη που το Αποτελούν

2.4.1 Arduino

Το Arduino είναι μια πλατφόρμα ανοιχτού κώδικα που χρησιμοποιείται για την κατασκευή ηλεκτρονικών έργων. Το Arduino αποτελείται από μια φυσική προγραμματιζόμενη πλακέτα κυκλώματος (συχνά αναφέρεται ως μικροελεγκτής) και ένα κομμάτι λογισμικού ή IDE (Integrated Development Environment) που εκτελείται στον υπολογιστή και χρησιμοποιείται για την εγγραφή και τη μεταφόρτωση του κώδικα στην πλακέτα. Η πλατφόρμα του Arduino έχει γίνει αρκετά δημοφιλής ιδιαίτερα σε ανθρώπους που μόλις ξεκινούν με ηλεκτρονικά. Σε αντίθεση με τις περισσότερες προηγούμενες προγραμματιζόμενες πλακέτες κυκλωμάτων, το Arduino δεν χρειάζεται ξεχωριστό κομμάτι υλικού (που ονομάζεται προγραμματιστής) για να φορτώσει νέο κώδικα στην πλακέτα, καθώς συνδέεται απευθείας στον υπολογιστή μέσω καλωδίου USB. Επιπλέον, το Arduino IDE χρησιμοποιεί μια απλοποιημένη έκδοση της C++, διευκολύνοντας την εκμάθηση του προγραμματισμού.

Το υλικό και το λογισμικό Arduino σχεδιάστηκε για καλλιτέχνες, σχεδιαστές, χομπίστες, χάκερ, φοιτητές και οποιονδήποτε ενδιαφέρεται να δημιουργήσει διαδραστικά αντικείμενα ή περιβάλλοντα. Το Arduino μπορεί να αλληλεπιδράσει με κουμπιά, LED, κινητήρες, ηχεία, μονάδες GPS, κάμερες, το διαδίκτυο, ακόμη και το smartphone ή την τηλεόραση. Αυτή η ευελιξία σε συνδυασμό με το γεγονός ότι το λογισμικό του Arduino είναι δωρεάν, οι πλακέτες είναι αρκετά φθηνές και τόσο το λογισμικό όσο και το υλικό είναι εύκολο στην εκμάθηση, έχει οδηγήσει σε μια μεγάλη κοινότητα χρηστών που συνεισέφεραν κώδικα και κυκλοφόρησαν οδηγίες για μια τεράστια ποικιλία έργων αυτοματισμών και ρομποτικής που βασίζονται στο Arduino. Υπάρχουν πολλές διαφορετικές πλακέτες Arduino που μπορούν να χρησιμοποιηθούν για διαφορετικούς σκοπούς. Το Arduino UNO (R3) είναι μια από τις πιο δημοφιλείς πλακέτες στην οικογένεια του Arduino και χρησιμοποιείται για το κύκλωμα της παρούσας εργασίας.



Εικόνα 2.3: Arduino UNO (R3)

Παρόλο που ορισμένες πλακέτες είναι λίγο διαφορετικές από την παραπάνω, έχουν τα εξής κοινά στοιχεία:

- ***Τροφοδοσία (Θύρα USB – Εξωτερική τροφοδοσία)***

Κάθε πλακέτα Arduino χρειάζεται έναν τρόπο για να συνδεθεί σε μια πηγή ρεύματος. Το Arduino μπορεί να τροφοδοτηθεί από ένα καλώδιο USB το οποίο προέρχεται από τον υπολογιστή ή από ένα εξωτερικό τροφοδοτικό τοίχου (5V, 2A). Στην παραπάνω εικόνα, η σύνδεση USB συμβολίζεται με (1) και η υποδοχή για το τροφοδοτικό τοίχου (2). Η σύνδεση USB είναι επίσης ο τρόπος με τον οποίο θα φορτωθεί ο κώδικας στην πλακέτα.

- ***Ακροδέκτες (GND, 5V, 3.3V, Analog, Digital, PWM, AREF)***

Οι ακροδέκτες (pins) στο Arduino λειτουργούν ως θέσεις όπου συνδέονται τα καλώδια για να δημιουργηθεί ένα κύκλωμα (πιθανώς σε συνδυασμό με ένα breadboard). Συνήθως έχουν μαύρες πλαστικές κεφαλές που επιτρέπουν την σύνδεση ενός καλωδίου απευθείας στην πλακέτα. Το Arduino έχει πολλά διαφορετικά είδη ακροδεκτών και χρησιμοποιούνται για διαφορετικές λειτουργίες.

- **GND (3):** Υπάρχουν αρκετοί ακροδέκτες με την ένδειξη GND στο Arduino και χρησιμοποιούνται για τη γείωση του κυκλώματος.

- **5V (4) & 3.3V (5):** ο ακροδέκτης 5V τροφοδοτεί τα εξαρτήματα με τάση 5V και ο ακροδέκτης 3.3 V αντίστοιχα με τάση 3.3V.
- **Analog (6):** Η περιοχή των ακροδεκτών κάτω από την ετικέτα «Analog In» (A0 έως A5) είναι οι ακροδέκτες της αναλογικής εισόδου. Αυτοί μπορούν να διαβάσουν το σήμα από έναν αναλογικό αισθητήρα (όπως για παράδειγμα έναν αισθητήρα θερμοκρασίας) και να το μετατρέψουν σε μια ψηφιακή τιμή που να μπορεί να διαβαστεί.
- **Digital (7):** Απέναντι από τους αναλογικούς ακροδέκτες βρίσκονται οι ψηφιακοί (0 έως 13). Αυτοί μπορούν να χρησιμοποιηθούν τόσο για ψηφιακή είσοδο (όπως για παράδειγμα αν πατηθεί ένα κουμπί) όσο και για ψηφιακή έξοδο (όπως για τροφοδοσία LED).
- **PWM (8):** Οι ακροδέκτες 3, 5, 6, 9, 10 και 11 λειτουργούν ως κανονικοί ψηφιακοί ακροδέκτες, αλλά μπορούν επίσης να χρησιμοποιηθούν και για Διαμόρφωση Πλάτους Παλμού (Pulse Width Modulation). Δηλαδή, οι ακροδέκτες αυτοί μπορούν να προσομοιώσουν μια αναλογική έξοδο (όπως το ξεθώριασμα ενός LED). Ουσιαστικά, το PWM δεν αποτελεί αληθινό αναλογικό σύστημα, αλλά δίνει παλμούς που εναλλάσσονται με υψηλές συχνότητες.
- **AREF (9):** Η τάση αναφοράς μπορεί να χρησιμοποιηθεί για να δεχθεί μια εξωτερική τάση αναφοράς (μεταξύ 0-5V) ως το ανώτερο όριο για τους ακροδέκτες της αναλογικής εισόδου.

- ***Κουμπί επαναφοράς (Reset)***

Το Arduino διαθέτει κουμπί επαναφοράς (10). Πιέζοντάς το θα γίνει επανεκκίνηση οποιουδήποτε κωδικού έχει φορτωθεί στο Arduino. Αυτό είναι αρκετά χρήσιμο, ειδικότερα σε περιπτώσεις όπου ο κώδικας δεν επαναλαμβάνεται από μόνος του.

- ***Ένδειξη LED ισχύος***

Στην πλακέτα υπάρχει ένα μικρό LED δίπλα στην ένδειξη "ON" (11). Αυτή η λυχνία LED ανάβει κάθε φορά που το Arduino συνδέεται σε μια πηγή ρεύματος. Εάν η λυχνία αυτή δεν είναι αναμμένη, υπάρχει μεγάλη πιθανότητα κάτι να μην πηγαίνει καλά.

- ***TX RX LED***

Το TX (transmit) και το RX (receive) υποδεικνύουν τους ακροδέκτες που είναι υπεύθυνοι για τη σειριακή επικοινωνία, δηλαδή για μετάδοση και λήψη αντίστοιχα. Στο Arduino υπάρχουν δύο θέσεις όπου εμφανίζονται τα TX και RX και συγκεκριμένα μια φορά στους ψηφιακούς ακροδέκτες 0 και 1 και μια δεύτερη φορά δίπλα στις ενδεικτικές λυχνίες LED TX και RX (12).

Τα LED αυτά παρέχουν τις απαραίτητες ενδείξεις κάθε φορά που το Arduino λαμβάνει ή μεταδίδει δεδομένα.

- ***Μικροελεγκτής***

Ο μικροελεγκτής ή αλλιώς ολοκληρωμένο (13) διαφέρει από Arduino σε Arduino, αλλά συνήθως είναι από τη σειρά ATmega των ολοκληρωμένων της εταιρείας ATMEL. Στην παρούσα εργασία χρησιμοποιήθηκε ο μικροελεγκτής ATmega328P, ο οποίος έχει επεξεργαστή 8-bit AVR RISC με μέγιστη ταχύτητα χρονισμού στα 20MHz. Διαθέτει μνήμη Flash ISP στα 32KB, SRAM στα 2KB και EEPROM στο 1KB. Η Flash και η EEPROM έχουν την ικανότητα να αποθηκεύουν τον κώδικα που είναι ήδη περασμένος στο Arduino και έτσι σε περίπτωση που χαθεί η τροφοδοσία, δεν χάνουν τα δεδομένα τους. Ο μικροελεγκτής λειτουργεί μεταξύ 1.8 – 5.5V και εκτελεί ισχυρές εντολές σε έναν κύκλο ρολογιού, επιτυγχάνοντας έτσι απόδοση που πλησιάζει το 1 MIPS ανά MHz και εξισορροπεί την κατανάλωση ενέργειας και την ταχύτητα επεξεργασίας.

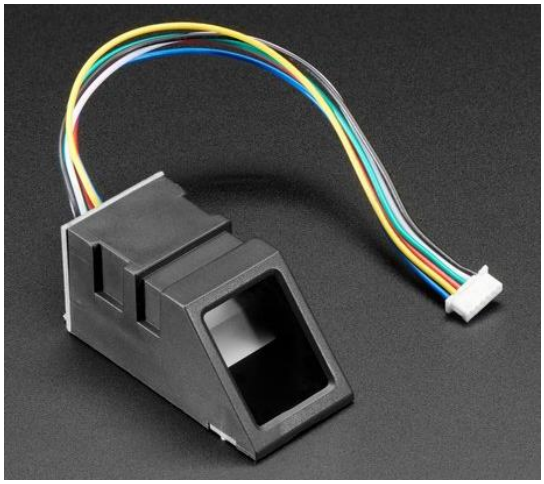
- ***Ρυθμιστής τάσης***

Ο ρυθμιστής τάσης (14) ελέγχει την ποσότητα της τάσης που περνάει στην πλακέτα. Ουσιαστικά μπορεί και απομακρύνει μια επιπλέον τάση που πιθανόν να βλάψει το κύκλωμα.

2.4.2 Μονάδα Αναγνώρισης Δακτυλικού Αποτυπώματος

Προκειμένου να επιτευχθεί σε γρήγορο χρόνο η μεταφορά της εικόνας ενός δακτυλικού αποτυπώματος στο σύστημα προς αναγνώριση και ταυτοποίηση, είναι απαραίτητο να χρησιμοποιούνται εικόνες που έχουν συμπιεστεί με τέτοιον τρόπο ώστε να παρέχουν την καλύτερη δυνατή ανάλυση από την εξαγωγή των βιομετρικών αυτών χαρακτηριστικών.

Η μονάδα που χρησιμοποιείται για την εργασία είναι ένα προϊόν της Geekcreit, το οποίο αποτελείται από έναν οπτικό αισθητήρα σάρωσης δακτυλικών αποτυπωμάτων, έναν επεξεργαστή DSP υψηλής ισχύος, έναν αλγόριθμο σύγκρισης δακτυλικών αποτυπωμάτων υψηλής απόδοσης και ένα τσιπ Flash μεγάλης χωρητικότητας. Η μονάδα αυτή έχει σταθερή απόδοση και χάρη στη βιβλιοθήκη της Adafruit που ενσωματώνει, διαθέτει πολλαπλές λειτουργίες, όπως είναι η συλλογή, η καταχώριση, η σύγκριση και η αναζήτηση δακτυλικών αποτυπωμάτων. Επίσης, ελέγχεται από τη σειριακή θύρα του υπολογιστή.



Εικόνα 2.4: Μονάδα σάρωσης δακτυλικού αποτυπώματος

Οι προδιαγραφές της μονάδας αυτής είναι οι εξής:

- Τάση τροφοδοσίας: 3.8 - 7V DC
- Ρεύμα λειτουργίας: 60 mA μέγιστο
- Ρεύμα αιχμής: 85 mA μέγιστο
- Χρόνος εξαγωγής εικόνας: <0.5 δευτερόλεπτα
- Εμβαδόν παραθύρου: 15 x 17 mm
- Μέθοδος αντιστοίχισης: μέθοδος σύγκρισης (1:1)
- Μέθοδος αναζήτησης (1:N)
- Αρχείο δυνατοτήτων: 384 bytes
- Αρχείο προτύπου: 786 bytes
- Χωρητικότητα αποθήκευσης: 240 πρότυπα
- Επίπεδο ασφαλείας 3 (1-5 χαμηλή έως υψηλή ασφάλεια)
- Ποσοστό ψευδούς αποδοχής (FAR): <0.001%
- Ποσοστό ψευδούς απόρριψης (FRR): <1%
- Χρόνος αναζήτησης: <220 ms
- Διεπαφή: UART (TTL λογικού επιπέδου)
- Ρυθμός Baud επικοινωνίας (UART): 9600, 19200, 28800, 38400, 57600 bps (προεπιλεγμένη τιμή: 57600 bps)
- Θερμοκρασία λειτουργίας: -30° C έως +70° C

- Υγρασία εργασίας: 40% - 85% RH
- Διαστάσεις (Μ x Π x Υ): 44 x 20 x 17 χιλιοστά
- Βάρος: 20 γραμμάρια

2.4.3 DC Ρελέ

Η μονάδα ελέγχου ρελέ 1 καναλιού με διέγερση 5V 10A χρησιμοποιεί οπτικό συζεύκτη SMD και διαθέτει ένα ρελέ γνήσιας ποιότητας. Οι είσοδοι της μονάδας ρελέ είναι απομονωμένες για να προστατεύουν κάθε ευαίσθητο κύκλωμα ελέγχου. Η κλειδαριά που χρησιμοποιείται στο κύκλωμα απαιτεί 12V τάση και έτσι δεν μπορεί να συνδεθεί απευθείας στο Arduino. Για τον λόγο αυτό, μεσολαβεί το ρελέ και παρέχει ασφάλεια στο Arduino.

Εικόνα 2.5: Μονάδα DC Ρελέ

Οι προδιαγραφές της μονάδας αυτής είναι οι εξής:

- Μέγιστο φορτίο: AC 250V/10A, DC 30V/10A
- Ρεύμα ενεργοποίησης: 5 mA
- Τάση λειτουργίας: 5V
- Διαστάσεις (Μ x Π x Υ): 50 x 26 x 18.5 mm

Διεπαφή μονάδας:

- DC+: θετικό τροφοδοτικό (VCC)
- DC-: αρνητικό τροφοδοτικό (GND)
- IN: μπορεί να είναι ρελέ ελέγχου υψηλής ή χαμηλής στάθμης

Έξοδοι ρελέ:

- NO: κανονικά ανοιχτή διεπαφή ρελέ
- COM: ρελέ κοινής διεπαφής
- NC: κανονικά κλειστή διεπαφή ρελέ

2.4.4 Τροφοδοσία

Η τροφοδοσία του Arduino, και κατά συνέπεια ολόκληρου του συστήματος, επιτυγχάνεται είτε μέσω υπολογιστή, συνδέοντάς το σε μια θύρα USB, είτε με εξωτερική τροφοδοσία, συνδέοντάς το σε μια υποδοχή με φις 2.1 χιλιοστών ή με μπαταρίες. Ιδανικά, η τάση της εξωτερικής τροφοδοσίας θα πρέπει να κυμαίνεται μεταξύ 7 έως 12V.

Εικόνα 2.6: USB καλώδιο τροφοδοσίας

Εικόνα 2.7: Τροφοδοσία 12V DC

2.4.5 Κλειδαριά

Οι ηλεκτρομαγνητικές κλειδαριές είναι κατασκευασμένες από ένα πηνίο και στη μέση διαθέτουν έναν οπλισμό. Ο οπλισμός αυτός είναι σε κατάσταση NO (ανοιχτός) και όταν το πηνίο ενεργοποιηθεί, τραβιέται στο κέντρο του για μικρό χρονικό διάστημα ώστε να ανοίξει η κλειδαριά. Μετά το πέρας λίγων δευτερολέπτων, ο οπλισμός επαναφέρεται στην αρχική του κατάσταση και η κλειδαριά κλείνει.

Εικόνα 2.8: Ηλεκτρομαγνητική κλειδαριά

Οι προδιαγραφές της ηλεκτρομαγνητικής κλειδαριάς που χρησιμοποιείται είναι οι εξής:

- Τάση λειτουργίας: 12V DC
- Ρεύμα λειτουργίας: 650 mA στα 12V
- Ενεργοποιημένες μορφές: διακοπτόμενες
- Μαγνητική Δύναμη: 0.3 κιλά
- Χρόνος ξεκλειδώματος: 1 δευτερόλεπτο
- Σχεδιασμένο για χρόνο ενεργοποίησης: 1-10 δευτερόλεπτα
- Ονομαστική διαδρομή: 10 χιλιοστά
- Μήκος καλωδίου: 223 χιλιοστά
- Διαστάσεις: 23.57 × 67.47 × 27.59 χιλιοστά

2.4.6 Μονάδα Bluetooth

Η μονάδα Bluetooth που χρησιμοποιείται για την κατασκευή είναι η HC-05 και είναι σχεδιασμένο για ασύρματη σειριακή επικοινωνία. Οι σειριακές μονάδες Bluetooth επιτρέπουν σε όλες τις σειριακές συσκευές να επικοινωνούν μεταξύ τους χρησιμοποιώντας τεχνολογία Bluetooth. Έχει δύο ακροδέκτες για σειριακή επικοινωνία, οι οποίοι είναι ο TXD και ο RXD. Ο TXD μπορεί να μεταδώσει σειριακά δεδομένα και ο RXD μπορεί αντίστοιχα να λάβει.

Η μονάδα αυτή διαθέτει ένα κόκκινο LED που υποδεικνύει την κατάσταση της σύνδεσης, δηλαδή αν το Bluetooth είναι συνδεδεμένο ή όχι. Πριν από τη σύνδεση, το κόκκινο αυτό LED αναβοσβήνει συνεχώς

με περιοδικό τρόπο. Όταν συνδέεται με οποιαδήποτε άλλη συσκευή Bluetooth, τότε αναβοσβήνει με πιο αργό ρυθμό.

Εικόνα 2.9: Μονάδα Bluetooth

Τα χαρακτηριστικά της HC-05 είναι τα εξής:

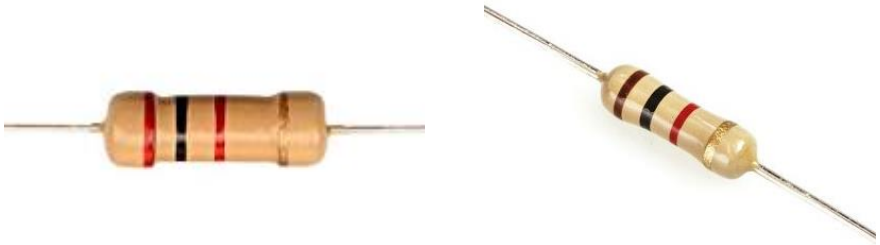
- Διαφανής μεταφορά δεδομένων TTL μεταξύ μιας κεντρικής συσκευής Bluetooth
- Προεπιλεγμένος ρυθμός Baud: 9600 bps
- Εμβέλεια έως 10 μέτρα
- Ενσωματωμένη κεραία
- Τάση λειτουργίας: 3.6 – 6V
- Διαστάσεις: 4.4 x 1.6 x 0.7 εκατοστά

2.4.7 Αντιστάσεις

Προκειμένου να συνδεθεί η μονάδα Bluetooth στην πλακέτα του Arduino, χρειάστηκε να κάνουμε χρήση διαιρέτη τάσης. Δεδομένου ότι η ελάχιστη τάση εξόδου του Arduino είναι μεγαλύτερη από την ελάχιστη τάση εισόδου της μονάδας HC-05, υπάρχει μεγάλη πιθανότητα να καταστραφεί η μονάδα αν ο ακροδέκτης TX του Arduino συνδεθεί απευθείας με τον ακροδέκτη RX της μονάδας. Για να αποφευχθεί αυτή η ζημιά, απαιτείται ένας διαιρέτης τάσης αντίστασης από τον ακροδέκτη TX του Arduino στον ακροδέκτη RX του HC-05 για να χαμηλώσει τα 5V από την ισχύ του Arduino σε μια λογική 3.3 V, έτσι ώστε τα δεδομένα να μπορούν να μεταφερθούν με ασφάλεια στη μονάδα Bluetooth.

Επομένως, για να πέσει η τάση από 5V σε 3V, με βάση τον τύπο διαίρεσης τάσης

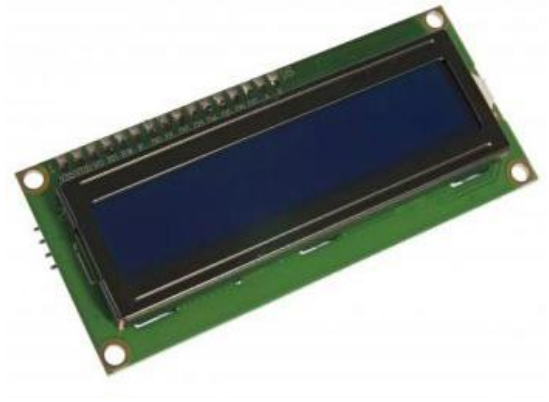
$Vout = Vin \cdot \frac{R2}{R1+R2}$ θα χρειαστούν μια αντίσταση του 1ΚΩ και μια των 2ΚΩ



Εικόνα 2.10: Αριστερά 2ΚΩ αντίσταση, δεξιά 1ΚΩ αντίσταση

2.4.8 Οθόνη LCD

Η οθόνη που χρησιμοποιείται για την εμφάνιση μηνυμάτων του συστήματος είναι μια οθόνη 16 χαρακτήρων επί 2 γραμμών με μπλε φόντο και άσπρους χαρακτήρες. Στην συγκεκριμένη είναι τοποθετημένη μια μονάδα I2C, η οποία βοηθά στη μείωση των συνδέσεων πολλών ακροδεκτών στο Arduino, καθώς απαιτεί μόνο 4 ακροδέκτες για τη σύνδεσή της.



Εικόνα 2.11: Οθόνη LCD 16x2 Χαρακτήρων

Τα χαρακτηριστικά της οθόνης είναι τα εξής:

- Τύπος: LCD χαρακτήρων
- Αριθμός χαρακτήρων: 16x2
- Χρώμα οθόνης: Μπλε
- Χρώμα φωτισμού: Λευκό

- Διεπαφή: I2C
- Τάση λειτουργίας: 5V
- Διαστάσεις: 80 x 35 x 18 χιλιοστά
- Διαστάσεις πάνελ: 71 x 25 χιλιοστά

2.5 Ανάπτυξη Κώδικα σε Περιβάλλον Arduino

Όλα τα προγράμματα που χρησιμοποιούν το Arduino είναι γραμμένα στο Ολοκληρωμένο Περιβάλλον Ανάπτυξης Arduino (IDE). Πρόκειται για ένα λογισμικό που τρέχει στον υπολογιστή και επιτρέπει να γράφουμε προγράμματα για διαφορετικές πλακέτες Arduino. Η γλώσσα προγραμματισμού που χρησιμοποιεί βασίζεται σε μια πολύ απλή hardware γλώσσα που ονομάζεται «επεξεργασία» και μοιάζει με τη γλώσσα C. Αφού ολοκληρωθεί ο κώδικας στο Arduino IDE, πρέπει να περαστεί στην πλακέτα κάνοντας upload, προκειμένου να εκτελεστεί.

Παρακάτω παρουσιάζεται ο κύριος κώδικας που αναπτύχθηκε στο περιβάλλον του Arduino, παραθέτοντας και τις απαιτούμενες επεξηγήσεις.

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>

LiquidCrystal_I2C lcd(0x27, 16, 2);
int lock = 8;
int cnt;
char c;
String data;
bool blocked = false;

SoftwareSerial mySerial(2, 3);
SoftwareSerial BTSerial(0, 1);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
```

Αρχικά, εντάσσονται οι απαραίτητες βιβλιοθήκες για τον αισθητήρα, την επικοινωνία με την πλακέτα και την οθόνη. Δηλώνονται τα εξής:

- Στον ακροδέκτη 8 της πλακέτας επιτυγχάνεται η επικοινωνία με το relay και κατά συνέπεια με την κλειδαριά ***lock***.

- Έναν μετρητή ***counter*** μέσω του οποίου κλειδώνει και ξεκλειδώνει το σύστημα έπειτα από τις τρεις εσφαλμένες προσπάθειες εισόδου.
- Έναν χαρακτήρα ***c*** ο οποίος διαβάζει τους χαρακτήρες από τη Σειριακή Οθόνη.
- Μια συμβολοσειρά ***data*** στην οποία θα αποθηκεύονται τα μηνύματα που θα διαβάζονται από τη Σειριακή Οθόνη.
- Έναν τύπο δεδομένων ***blocked*** ώστε να ελέγχεται αν είναι ή όχι κλειδωμένο το σύστημα.
- Στους ακροδέκτες 2 και 3 της πλακέτας έχει συνδεθεί ο αισθητήρας δακτυλικών αποτυπωμάτων για σειριακή επικοινωνία. Αντιστοιχούν στις θέσεις ***Rx*** και ***Tx***.
- Στους ακροδέκτες 0 και 1 της πλακέτας έχει συνδεθεί η μονάδα ***Bluetooth*** για σειριακή επικοινωνία.

```
18 void setup()
19 {
20   lcd.init();
21   lcd.backlight();
22   pinMode(lock, OUTPUT);
23   digitalWrite(lock, LOW);
24   Serial.begin(9600);
25   mySerial.begin(9600);
26   BTSerial.begin(9600);
27   while (!Serial);
28   delay(1000);
29   Serial.println("\n\nIdentification System");
30   lcd.setCursor(0,0);
31   lcd.print("Identification");
32   lcd.setCursor(0,1);
33   lcd.print("System");
```

Ο κώδικας που ακολουθεί μέσα σε αυτή την συνάρτηση θα εκτελεστεί μια μόνο φορά μόλις ξεκινήσει η εκτέλεση του συστήματος. Ενεργοποιείται αρχικά η οθόνη και ορίζεται το ρελέ για την κλειδαριά να συμπεριφέρεται ως έξοδος στο κύκλωμα. Ορίζεται επίσης η αρχική κατάσταση του ρελέ στη θέση LOW, οπότε το κύκλωμα είναι ανοιχτό και η κλειδαριά είναι ανενεργή. Εμφανίζεται στην lcd οθόνη το μήνυμα «Identification System».

```
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor");
  }
  else {
    Serial.println("Did not find fingerprint sensor");
    while (1)  {
      }
  }

  Serial.println(F("Reading sensor parameters"));
  finger.getParameters();
  Serial.print(F("Status: 0x")); Serial.println(finger.status_reg, HEX);
  Serial.print(F("Sys ID: 0x")); Serial.println(finger.system_id, HEX);
  Serial.print(F("Capacity: ")); Serial.println(finger.capacity);
  Serial.print(F("Security level: ")); Serial.println(finger.security_level);
  Serial.print(F("Device address: ")); Serial.println(finger.device_addr, HEX);
  Serial.print(F("Packet len: ")); Serial.println(finger.packet_len);
  Serial.print(F("Baud rate: ")); Serial.println(finger.baud_rate);

  finger.getTemplateCount();

  if (finger.templateCount == 0) {
    Serial.print("Sensor doesn't contain any fingerprint data. Run the 'enroll' example.");
  }
  else {
    Serial.println("Waiting for valid finger...");
      Serial.print("Sensor contains ");
      Serial.print(finger.templateCount); Serial.println(" templates");
  }
}
```

Αρχικοποιείται η σειριακή επικοινωνία του αισθητήρα και ρυθμίζεται ο ρυθμός δεδομένων για τη σειριακή θύρα στα 57600 bit/sec. Στη συνέχεια, η συνάρτηση ***finger.getParameters()*** επιστρέφει τις παραμέτρους του αισθητήρα σχετικά με την κατάστασή του, την ταυτότητα του συστήματος, την χωρητικότητα, το επίπεδο ασφαλείας, την διεύθυνση και τον ρυθμό μετάδοσης δεδομένων. Έπειτα, η συνάρτηση ***finger.getTemplateCount()*** επιστρέφει τον αριθμό από τα ήδη αποθηκευμένα πρότυπα δακτυλικών αποτυπωμάτων. Στο τέλος, το πρόγραμμα ζητάει να γίνει σάρωση του δακτύλου πάνω στον αισθητήρα αναγνώρισης.

```
67 void loop()
68 {
69   do {
70     getFingerprintID();
71     if(cnt>=3) {
72       Serial.println("Blocked;");
73       lcd.clear();
74       lcd.print("ACCESS DENIED");
75     }
76   } while(cnt>0 && cnt<3);
77 
78   while (blocked == true){
79     receive_msg();
80     if(blocked == false){
81       cnt = 0;
82       break;
83     }
84   }
85   delay(50);
86 }
```

Ο κώδικας που ακολουθεί μέσα σε αυτή την συνάρτηση θα εκτελείται ξανά και ξανά για όσο η πλακέτα είναι σε λειτουργία. Αναλυτικότερα:

- Εκτελείται ο βρόχος ***do while*** για όσο διάστημα ο μετρητής cnt έχει τιμές μικρότερες του 3.
- Καλείται η συνάρτηση ***getFingerprintID()*** στην οποία έχει αποθηκευτεί η ταυτότητα του δακτυλικού αποτυπώματος που σαρώθηκε.
- Αν ο μετρητής cnt έχει τιμές μεγαλύτερες ή ίσες του 3, δηλαδή αν ο χρήστης σαρώσει πάνω από τις 3 φορές δακτυλικό αποτύπωμα το οποίο δεν βρίσκεται αποθηκευμένο στη βάση δεδομένων, τότε εμφανίζεται στη Σειριακή Οθόνη το μήνυμα «Blocked» και στην lcd το μήνυμα «ACCESS DENIED».
- Όσο ο τύπος δεδομένων blocked είναι αληθής, δηλαδή το σύστημα είναι κλειδωμένο, καλείται η συνάρτηση ***receive_msg()***.
- Ο βρόχος τερματίζει μόλις ο τύπος δεδομένων blocked γίνει ψευδής, δηλαδή το σύστημα πλέον είναι σε λειτουργία. Επίσης ο μετρητής cnt μηδενίζεται, προκειμένου να μετρήσει ξανά από την αρχή τις εσφαλμένες προσπάθειες εισόδου του χρήστη.

```
88 uint8_t getFingerprintID() {
89
90   uint8_t p = finger.getImage();
91   switch (p) {
92     case FINGERPRINT_OK:
93       Serial.println("Image taken"); delay(3);
94       break;
95     case FINGERPRINT_NOFINGER:
96       Serial.println("No finger detected"); delay(3);
97       lcd.clear();
98       lcd.setCursor(0,0);
99       lcd.print("Scan your finger");
100      return p;
101    case FINGERPRINT_PACKETRECIEVEERR:
102      Serial.println("Communication error");
103      return p;
104    case FINGERPRINT_IMAGEFAIL:
105      Serial.println("Imaging error");
106      return p;
107    default:
108      Serial.println("Unknown error");
109      return p;
110  }
111
112  p = finger.image2Tz();
113  switch (p) {
114    case FINGERPRINT_OK:
115      Serial.println("Image converted"); delay(3);
116      break;
117    case FINGERPRINT_IMAGEMESS:
118      Serial.println("Image too messy");
119      return p;
120    case FINGERPRINT_PACKETRECIEVEERR:
121      Serial.println("Communication error");
122      return p;
123    case FINGERPRINT_FEATUREFAIL:
124      Serial.println("Could not find fingerprint features");
125      return p;
126    case FINGERPRINT_INVALIDIMAGE:
127      Serial.println("Could not find fingerprint features");
128      return p;
129    default:
130      Serial.println("Unknown error");
131      return p;
132  }
```

Καλείται η συνάρτηση ***finger.getImage()*** για να ελεγχθεί αν ο αισθητήρας έχει τραβήξει φωτογραφία του δακτυλικού αποτυπώματος κατά την σάρωση. Εξετάζονται διάφορες περιπτώσεις και εμφανίζονται στη Σειριακή Οθόνη τα αντίστοιχα μηνύματα για το αν η φωτογραφία έχει ληφθεί, αν δεν έχει σαρωθεί κάποιο δάκτυλο και αν υπάρχει κάποιο σφάλμα στην επικοινωνία ή στην εικόνα. Επίσης, καλείται η συνάρτηση ***finger.image2Tz()***για να ελεγχθεί αν ο αισθητήρας έχει μετατρέψει σωστά την φωτογραφία

της σάρωσης κατά τα πρότυπα χαρακτηριστικών και εμφανίζονται στη Σειριακή Οθόνη τα αντίστοιχα μηνύματα.

```
  p = finger.fingerSearch();
  if (p == FINGERPRINT_OK) {
    Serial.println("Found a print match!");
    blocked = false;
    cnt=0;
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
    Serial.println("Communication error");
    return p;
  } else if (p == FINGERPRINT_NOTFOUND) {
    Serial.println("Did not find a match"); delay(3);
    cnt++;
    Serial.print("Counter: "); delay(3);
    Serial.println(cnt);
    blocked = true;
    lcd.setCursor(0, 1);
    lcd.print("Attempts left: ");
    lcd.print(3-cnt);
    delay(2000);
    return p;
  } else {
    Serial.println("Unknown error");
    return p;
  }

    Serial.print("Found ID #"); Serial.print(finger.fingerID);
    // found a match!
    Serial.print(" with confidence of "); Serial.println(finger.confidence);
    lcd.clear();
    lcd.print("Door opened");
    digitalWrite(lock, HIGH); delay(3000);
    delay(1000);
    digitalWrite(lock, LOW);
    lcd.clear();
    lcd.print("Door closed");
    delay(1000);
    return finger.fingerID;
}
```

Καλείται η συνάρτηση ***finger.fingerSearch()*** για να κάνει ο αισθητήρας αναζήτηση στα τρέχοντα χαρακτηριστικά που εξήγαγε και να δει αν ταιριάζουν με αυτά των ήδη αποθηκευμένων προτύπων. Αν το σαρωμένο δακτυλικό αποτύπωμα ταυτιστεί με κάποιο πρότυπο, τότε το σύστημα θα θεωρείται κλειδωμένο (ο τύπος δεδομένων θα είναι ψευδής) και ο μετρητής cnt θα μηδενίσει. Αλλιώς αν υπάρχει κάποιο σφάλμα στην επικοινωνία, εμφανίζεται το αντίστοιχο μήνυμα. Αλλιώς αν το σαρωμένο δακτυλικό αποτύπωμα δεν ταυτίστηκε με κανένα πρότυπο, τότε ο μετρητής cnt αυξάνεται κατά 1, εμφανίζεται η τιμή του στην Σειριακή Οθόνη και τίθεται το σύστημα σε λειτουργία, ορίζοντας την τιμή του blocked ως αληθής. Αλλιώς σε κάθε άλλη περίπτωση υπάρχει σφάλμα και εμφανίζεται το κατάλληλο μήνυμα. Επιπλέον, αλλάζει την αρχική κατάσταση του ρελέ από LOW σε HIGH, δηλαδή το κύκλωμα

κλείνει, δέχοντας τάση 5V οπότε ενεργοποιείται η κλειδαριά και ξεκλειδώνει. Παραμένει ανοιχτή για 3 δευτερόλεπτα. Μετά το πέρας των 3 δευτερολέπτων, η κλειδαριά ξανακλείνει.

Στο διάστημα αυτής της διαδικασίας, εμφανίζονται στην lcd οθόνη μηνύματα με τις προσπάθειες που απομένουν στον χρήστη, όταν αυτός βάζει μη αποθηκευμένο δακτυλικό αποτύπωμα στο σύστημα («Attempts left: ») και μηνύματα για όταν η πόρτα ανοίγει και κλείνει «Door opened/closed».

```
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;

  Serial.print("Found ID #"); Serial.print(finger.fingerID);
  Serial.print(" with confidence of "); Serial.println(finger.confidence);
  return finger.fingerID;
}

void receive_msg(){
  if(Serial.available()){
    while (Serial.available()){
      delay(3);
      c = Serial.read();
      data += c;
    }

    if(data.length()>0){
      if(data == "unblock"){
        blocked = false;
      }
    }
  }
  data = "";
}
```

Η συνάρτηση ***receive_msg()*** διαβάζει τα εισερχόμενα σειριακά μηνύματα από το Bluetooth και επιστρέφει το πρώτο byte των δεδομένων αυτών. Η τιμή αυτή αποθηκεύεται στον χαρακτήρα c. Στην συμβολοσειρά data αποθηκεύονται οι χαρακτήρες c που διαβάστηκαν προηγουμένως. Αν ο αριθμός των χαρακτήρων που έχει η συμβολοσειρά data είναι μεγαλύτερος από 0 και αν επίσης αποτελείται από το μήνυμα «unblock», τότε:

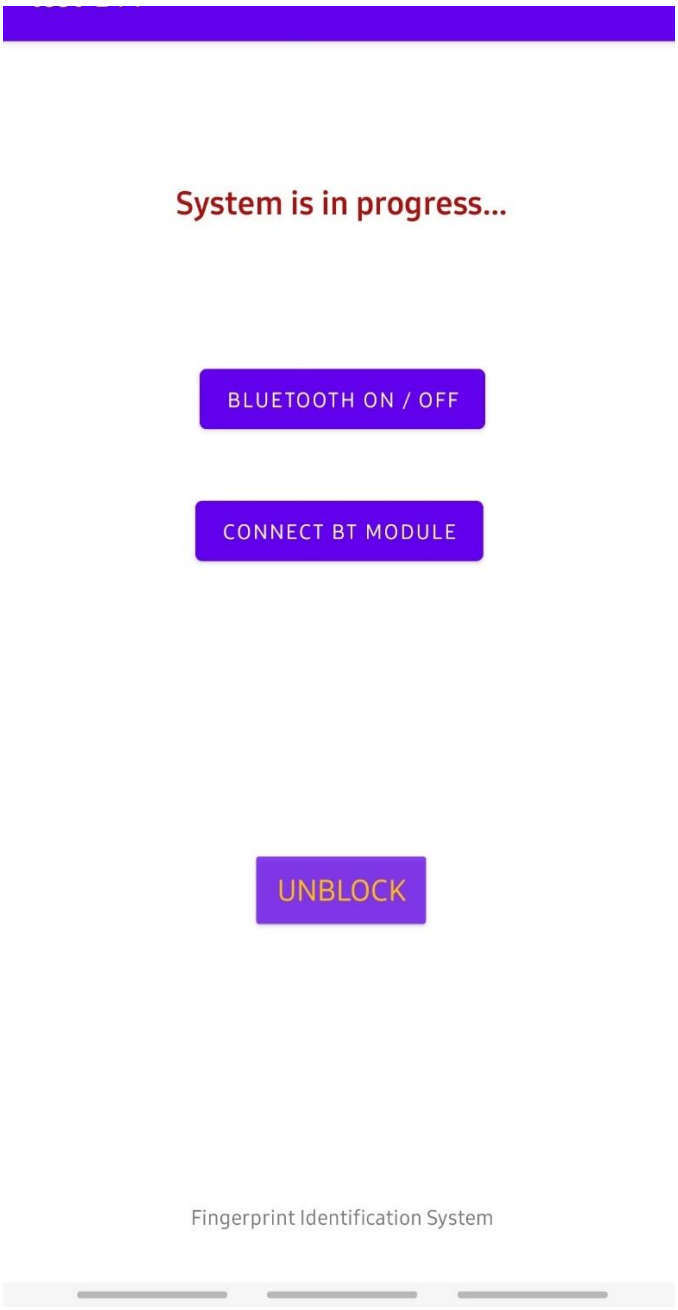
Ο τύπος δεδομένων blocked ορίζεται ως ψευδής και το σύστημα θεωρείται κλειδωμένο. Επιστρέφει την τιμή αυτή στην void loop() όπου και έγινε η κλήση της συνάρτησης αυτής και αδειάζουν οι χαρακτήρες που περιέχει η συμβολοσειρά data.

Η βιβλιοθήκη της Adafruit εμπεριέχει κώδικα για την εγγραφή των δακτυλικών αποτυπωμάτων στη βάση δεδομένων (enroll) και κώδικα για την διαγραφή τους αντίστοιχα από τη βάση δεδομένων (empty database). Οι κώδικες αυτοί δεν είναι περασμένοι στο Arduino, καθώς πρόσβαση επιτρέπεται να έχει μόνο ο διαχειριστής του συστήματος και όχι οι χρήστες που το χρησιμοποιούν για να αποκτήσουν πρόσβαση στους χώρους ασφαλείας. Για τον λόγο αυτό, αναφέρονται στο Παράρτημα της διπλωματικής.

2.6 Ανάπτυξη Εφαρμογής σε Περιβάλλον Android Studio

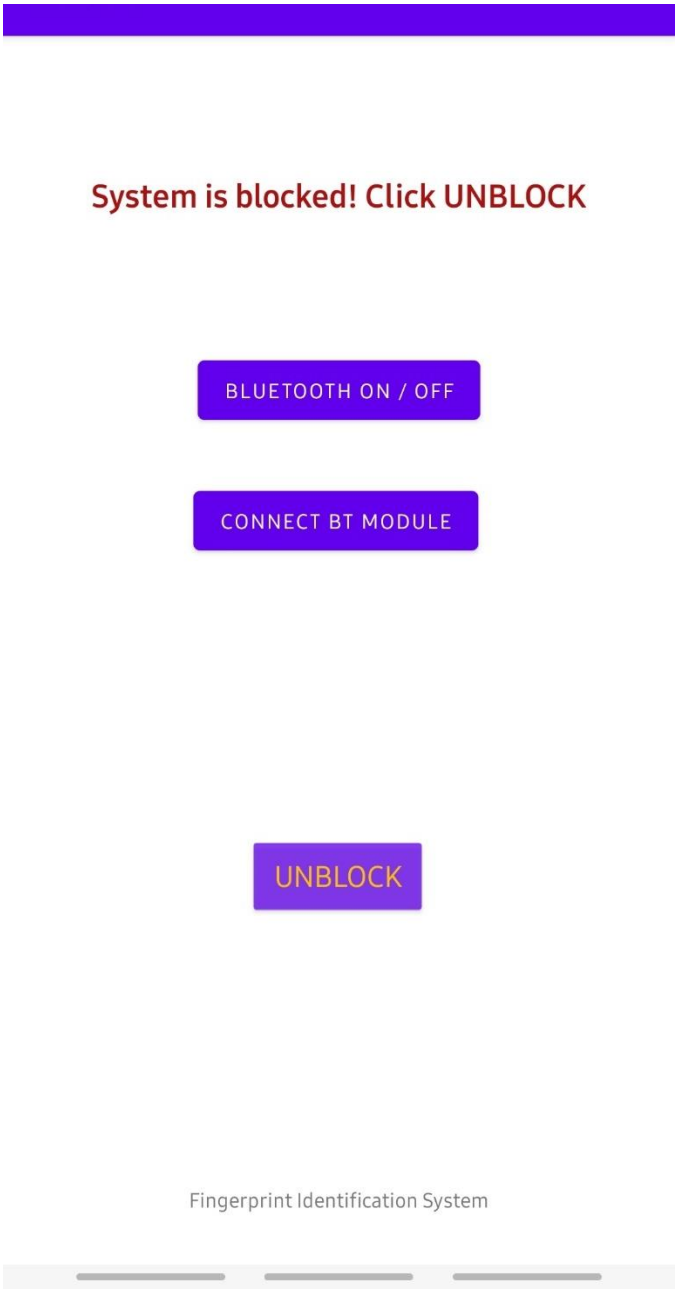
Το Android Studio είναι ένα Ολοκληρωμένο Περιβάλλον Ανάπτυξης (IDE) για το λειτουργικό σύστημα Android, στο οποίο γίνεται ανάπτυξη εφαρμογών για συμβατές συσκευές. Οι γλώσσες προγραμματισμού που χρησιμοποιεί είναι η Kotlin, η Java και η C++. Για την συγκεκριμένη εργασία, ο κώδικας γράφτηκε σε Java.

Αρχικά, για την εφαρμογή δημιουργήθηκαν 3 κουμπιά (buttons) στα οποία ο διαχειριστής του συστήματος έχει πρόσβαση. Με το πάτημα του πρώτου κουμπιού «BLUETOOTH ON/OFF», ενεργοποιείται ή απενεργοποιείται η λειτουργία Bluetooth από την συσκευή Android που χρησιμοποιεί. Στη συνέχεια, πατώντας το κουμπί «CONNECT BT MODULE», επιτυγχάνεται η σύνδεση της μονάδας HC-05 του συστήματος ώστε να επικοινωνεί με το κινητό αλλά και το Arduino. Όπως είναι γνωστό, μόλις το σύστημα δεχθεί τρεις εσφαλμένες προσπάθειες εισόδου, μπλοκάρει. Προκειμένου να μπορέσει ο διαχειριστής να το επαναφέρει σε λειτουργία, δημιουργήθηκε το κουμπί «UNBLOCK». Μόλις πατηθεί, το σύστημα είναι ξανά έτοιμο για χρήση. Επιπλέον, στο πάνω μέρος έχει δημιουργηθεί μια γραμμή κειμένου στην οποία εμφανίζονται τα απαραίτητα μηνύματα για επικοινωνία. Στο κάτω μέρος υπάρχει και μια ακόμα γραμμή κειμένου η οποία λέει μόνιμα «Fingerprint Identification System», καθώς είναι ο τίτλος της εφαρμογής.



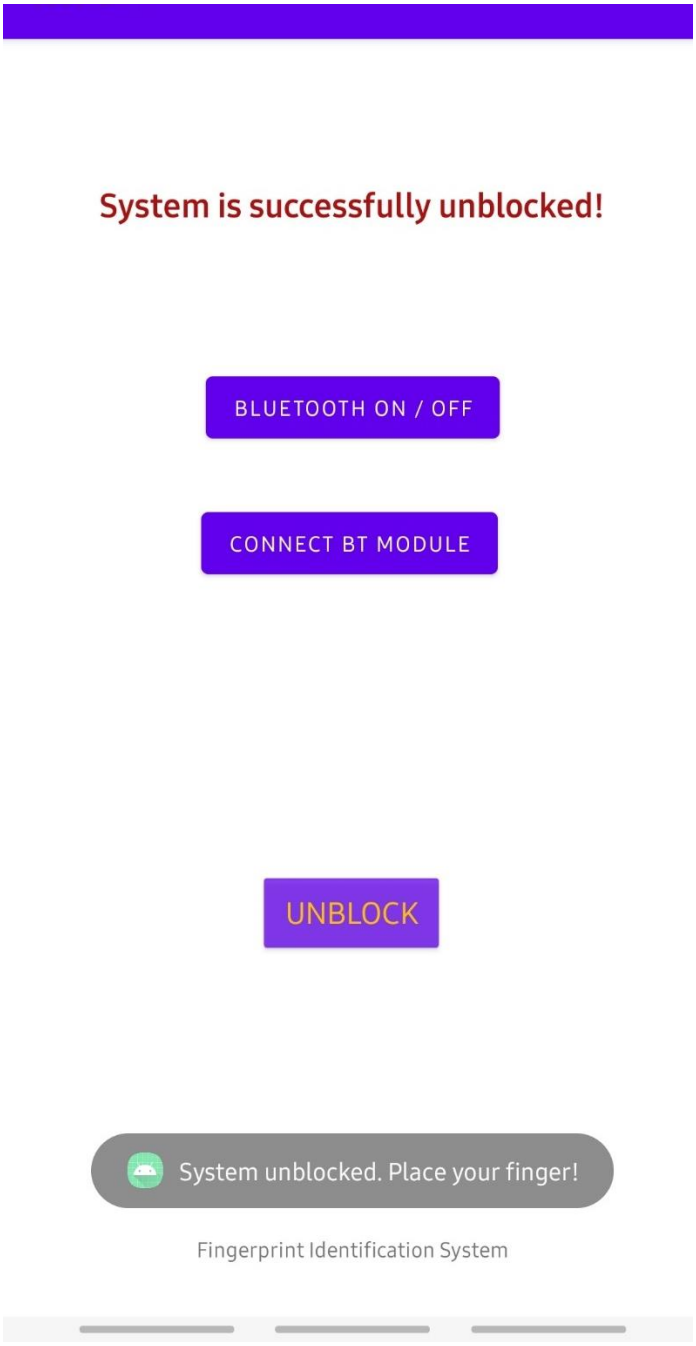
Εικόνα 2.12: Το σύστημα σε εξέλιξη

Όσο το σύστημα βρίσκεται σε εξέλιξη, δηλαδή λειτουργεί κανονικά και οι χρήστης σαρώνουν τα δακτυλικά τους αποτυπώματα, στο επάνω μέρος της οθόνης εμφανίζεται με κόκκινα γράμματα το μήνυμα «System is in progress…».



Εικόνα 2.13: Το σύστημα έχει μπλοκάρει

Μόλις το σύστημα μπλοκάρει, το μήνυμα αλλάζει σε «System is blocked. Click UNBLOCK». Έτσι ο διαχειριστής ενημερώνεται και πρέπει να πατήσει το αντίστοιχο κουμπί, ώστε να επαναφέρει το σύστημα σε λειτουργία.



Εικόνα 2.14: Το σύστημα επανέρχεται

Με το πάτημα του κουμπιού «UNBLOCK» από τον διαχειριστή, το σύστημα ξεμπλοκάρει αλλάζοντας το μήνυμα σε «System is successfully unblocked!» και στο κάτω μέρος της οθόνης εμφανίζει άλλο ένα ακόμη μήνυμα «System unblocked. Place your finger!».

Παρακάτω παρουσιάζεται ο κώδικας που αναπτύχθηκε στο περιβάλλον του Android Studio, παραθέτοντας και τις απαιτούμενες επεξηγήσεις.

```
package com.example.fingerprint_identification_system;

import androidx.appcompat.app.AppCompatActivity;
import androidx.localbroadcastmanager.content.LocalBroadcastManager;

import android.annotation.SuppressLint;
import android.bluetooth.BluetoothAdapter;
import android.bluetooth.BluetoothDevice;
import android.content.BroadcastReceiver;
import android.content.Context;
import android.content.Intent;
import android.content.IntentFilter;
import android.os.Bundle;
import android.util.Log;
import android.view.View;
import android.widget.Button;
import android.widget.TextView;
import android.widget.Toast;

import java.nio.charset.Charset;
import java.util.UUID;

public class MainActivity extends AppCompatActivity {
    private static final String TAG = "MainActivity";

    private BluetoothAdapter mBluetoothAdapter;
    private BluetoothConnectionService mBluetoothConnectionService;
    private BluetoothDevice mBTDevice;
    private String messages;
    private TextView incomingMessages;
    private TextView authormessage;
    private Button onoffBTN;
    private Button unblockBTN;
    private Button ConnectBTN;

    private static final UUID MY_UUID_INSECURE = UUID.fromString("00001101-0000-1000-8000-00805F9B34FB");
```

Αρχικά, ορίζονται οι τάξεις που θα χρειαστούν για την υλοποίηση της εφαρμογής, οι οποίες είναι:

- ***mBluetoothAdapter*** για την μονάδα HC-05.
- ***mBTDevice*** για το κινητό τηλέφωνο.
- ***BluetoothConnectionService*** για τη σύνδεση μεταξύ αυτών των δύο συσκευών.
- Συμβολοσειρά ***messages*** που λαμβάνει τα μηνύματα από το Arduino.
- Γραμμή κειμένου ***incomingMessages*** για τα εισερχόμενα μηνύματα από τη μονάδα HC-05.
- Γραμμή κειμένου ***authormessage*** για το μήνυμα στο κάτω μέρος της οθόνης.
- Κουμπί ***onoff*** για ενεργοποίηση/απενεργοποίηση του Bluetooth του κινητού.

- Κουμπί ***unblock*** για επαναφορά του συστήματος.
- Κουμπί ***Connect*** για σύνδεση του κινητού με τη μονάδα HC-05.

```
38      private final BroadcastReceiver mBroadcastReceiver1 = new BroadcastReceiver() {
39          @Override
40          public void onReceive(Context context, Intent intent) {
41              String action = intent.getAction();
42              if (action.equals(BluetoothAdapter.ACTION_STATE_CHANGED)) {
43                  final int state = intent.getIntExtra(BluetoothAdapter.EXTRA_STATE, BluetoothAdapter.ERROR);
44
45                  switch (state){
46                      case BluetoothAdapter.STATE_OFF:
47                          Log.d(TAG,  msg: "onReceive: STATE OFF");
48                          break;
49                      case BluetoothAdapter.STATE_TURNING_OFF:
50                          Log.d(TAG,  msg: "mBroadcastReceiver1: STATE TURNING OFF");
51                          break;
52                      case BluetoothAdapter.STATE_ON:
53                          Log.d(TAG,  msg: "mBroadcastReceiver1: STATE ON");
54                          break;
55                      case BluetoothAdapter.STATE_TURNING_ON:
56                          Log.d(TAG,  msg: "mBroadcastReceiver1: STATE TURNING ON");
57                          break;
58                      default:
59                          break;
60                  }
61              }
62          }
63      };
```

Στο σημείο αυτό λαμβάνονται μηνύματα για την κατάσταση στην οποία βρίσκεται το ***BluetoothAdapter***, δηλαδή αν είναι ενεργό ή όχι. Τα μηνύματα αυτά είναι εμφανή μόνο στη ροή μηνυμάτων στο πρόγραμμα και όχι στην τελική εφαρμογή.

```
65      @Override
66      protected void onDestroy() {
67          Log.d(TAG,  msg: "onDestroy: called.");
68          super.onDestroy();
69          unregisterReceiver(mBroadcastReceiver1);
70      }
71
72      @SuppressLint("SetTextI18n")
73      @Override
74      protected void onCreate(Bundle savedInstanceState) {
75          super.onCreate(savedInstanceState);
76          setContentView(R.layout.activity_main);
77
78          onoffBTN = (Button) findViewById(R.id.onoffBTN);
79          unblockBTN = (Button) findViewById(R.id.unblockBTN);
80          ConnectBTN = (Button) findViewById(R.id.connectBTN);
81          incomingMessages = (TextView) findViewById(R.id.txt);
82          authormessage = (TextView) findViewById(R.id.authorM);
83          messages = "";
84          authormessage.setText("Fingerprint Identification System");
85
86          LocalBroadcastManager.getInstance(this).registerReceiver(mReceiver, new IntentFilter( action: "incomingMessage"));
87
88          mBluetoothAdapter = BluetoothAdapter.getDefaultAdapter();
```

Μέσα στην συνάρτηση ***onCreate***, δημιουργούνται τα τρία κουμπιά της εφαρμογής, τα δύο text views μηνυμάτων, και το string με τα μηνύματα από το Arduino. Ορίζεται το ***authormessage*** σε «Fingerprint Identification System», για να εμφανίζεται μόνιμα στο κάτω μέρος της οθόνης.

```
90          onoffBTN.setOnClickListener(new View.OnClickListener() {
91              @Override
92              public void onClick(View view) {
93                  Log.d(TAG,  msg: "onClick: enabling/disabling bluetooth.");
94                  enableDisableBT();
95              }
96          });
```

Ορίζεται τι θα συμβεί μόλις πατηθεί το κουμπί ***onoff***. Πατώντας το, ενεργοποιείται ή απενεργοποιείται το Bluetooth στο κινητό μας αναλόγως με την τρέχουσα κατάσταση που έχει.

```
98          ConnectBTN.setOnClickListener(new View.OnClickListener() {
99              @Override
100             public void onClick(View view) {
101                 Log.d(TAG,  msg: "onClick: enabling/disabling.");
102                 mBluetoothAdapter.cancelDiscovery();
103                 mBTDevice = mBluetoothAdapter.getRemoteDevice( address: "98:D3:11:FC:63:F2");
104                 mBTDevice.createBond();
105                 mBluetoothConnectionService = new BluetoothConnectionService( context: MainActivity.this);
106                 startConnection();
107                 Toast.makeText(getApplicationContext(), text: "Connected to HC-05",Toast.LENGTH_SHORT).show();
108             }
109         });
```

Επιπλέον, ορίζεται τι θα συμβεί μόλις πατηθεί το κουμπί ***Connect***. Πατώντας το, δημιουργείται σύνδεση μεταξύ του Bluetooth στο κινητό με το Bluetooth της μονάδας HC-05 και αρχίζει η επικοινωνία μεταξύ τους. Μόλις συνδεθούν εμφανίζεται για μικρό χρονικό διάστημα στην οθόνη το μήνυμα «Connected to HC-05».

```
111         unblockBTN.setOnClickListener(new View.OnClickListener() {
112             @SuppressLint("SetTextI18n")
113             @Override
114             public void onClick(View view){
115                 outStream( msg: "unblock");
116                 incomingMessages.setText("System is successfully unblocked!");
117                 Toast.makeText(getApplicationContext(), text: "System unblocked. Place your finger!",Toast.LENGTH_SHORT).show();
118             }
119         });
120     }
```

Τέλος, ορίζεται τι θα συμβεί μόλις πατηθεί το κουμπί ***unblock***. Πατώντας το, στέλνεται εντολή στη μονάδα HC-05 να δώσει αντίστοιχα εντολή στο Arduino για να επανέρθει το σύστημα. Εμφανίζεται

έπειτα το μήνυμα «System is successfully unblocked!» στην οθόνη του κινητού και, για λίγο χρονικό διάστημα, το μήνυμα «System unblocked. Place your finger!».

```
122     BroadcastReceiver mReceiver = new BroadcastReceiver() {
123         @SuppressLint("SetTextI18n")
124         @Override
125         public void onReceive(Context context, Intent intent) {
126             String text = intent.getStringExtra( name: "theMessage");
127             messages += text;
128             if (messages.contains("No finger detected")){
129                 incomingMessages.setText("System is in progress...");
130                 messages = " ";
131             }
132             else if (messages.contains("Blocked;")) {
133                 incomingMessages.setText("System is blocked! Click UNBLOCK");
134                 try {
135                     Thread.sleep( millis: 500);
136                 } catch (InterruptedException ex) {
137                     Thread.currentThread().interrupt();
138                 }
139             }
140             Log.d(TAG,  msg: "messages: " + messages);
141         }
142     };
```

Με την συνάρτηση αυτή, μέσω της επικοινωνίας με τη μονάδα HC-05, διαβάζονται τα μηνύματα από την Σειριακή Οθόνη στο Arduino. Αν το μήνυμα που λαμβάνεται είναι «No finger detected», εμφανίζεται στην οθόνη του κινητού το μήνυμα «System is in progress…». Αλλιώς αν το μήνυμα που λαμβάνεται είναι «Blocked;», τότε εμφανίζεται «System is blocked! Click UNBLOCK».

```
144     public void enableDisableBT(){
145         if(mBluetoothAdapter == null){
146             Log.d(TAG,  msg: "enableDisableBT: does not have BT capabilities.");
147         }
148         if(!mBluetoothAdapter.isEnabled()){
149             Log.d(TAG,  msg: "enableDisableBT: enabling BT.");
150             Intent enableBTintent = new Intent(BluetoothAdapter.ACTION_REQUEST_ENABLE);
151             startActivity(enableBTintent);
152 
153             IntentFilter BTIntent = new IntentFilter(BluetoothAdapter.ACTION_STATE_CHANGED);
154             registerReceiver(mBroadcastReceiver1, BTIntent);
155         }
156         if(mBluetoothAdapter.isEnabled()){
157             Log.d(TAG,  msg: "enableDisableBT: disabling BT.");
158             mBluetoothAdapter.disable();
159 
160             IntentFilter BTIntent = new IntentFilter(BluetoothAdapter.ACTION_STATE_CHANGED);
161             registerReceiver(mBroadcastReceiver1, BTIntent);
162         }
163     }
```

Η συνάρτηση αυτή επιτρέπει την ενεργοποίηση ή απενεργοποίηση του Bluetooth στο κινητό.

```
165     public void startConnection(){
166         startBTConnection(mBTDevice,MY_UUID_INSECURE);
167     }
168     public void startBTConnection(BluetoothDevice device, UUID uuid){
169         Log.d(TAG,  msg: "startBTConnection: Initializing RFCOM Bluetooth Connection.");
170         mBluetoothConnectionService.startClient(device, uuid);
171     }
```

Η συνάρτηση αυτή καθορίζει την επικοινωνία και τη σύνδεση του κινητού με την μονάδα HC-05.

```
173 @       public void outStream(String msg){
174             byte[] bytes = msg.getBytes(Charset.defaultCharset());
175             mBluetoothConnectionService.write(bytes);
176         }
177     }
```

Μέσω της συνάρτησης αυτής διαβάζονται τα μηνύματα που στέλνει το Arduino.

Τέλος, μέσα στην τάξη ***BluetoothConnectionService,*** που καθορίζει την επικοινωνία και τη σύνδεση του HC-05, περιέχεται επιπλέον κώδικας που αναφέρεται στο Παράρτημα της διπλωματικής.

ΚΕΦΑΛΑΙΟ 3ο: Επίλογος

3.1 Εισαγωγή

Στο 3ο κεφάλαιο συνοψίζεται το έργο που εκπονήθηκε στο πλαίσιο αυτής της διπλωματικής εργασίας, επεξηγούνται τα προβλήματα που προέκυψαν και επεξηγήθηκε η αντιμετώπισή τους, καταγράφονται τα συμπεράσματα που προέκυψαν από αυτό και τέλος παρουσιάζονται προτάσεις για μελλοντική εξέλιξή του.

3.2 Σύνοψη

Συνοψίζοντας, η διπλωματική αυτή εργασία βασίζεται στα οφέλη και στην καινοτομία που προκύπτουν από την ένταξη της βιομετρίας σε συστήματα αυτομάτου ελέγχου. Η ανάπτυξη του συστήματος που υλοποιήθηκε, εφόσον αξιοποιηθεί σωστά μπορεί να συνεισφέρει σε μεγάλο βαθμό, παρέχοντας ασφάλεια. Το σύστημα αυτό, πέρα από επιχειρήσεις, μπορεί να ενταχθεί και σε οικιακούς χώρους για αποφυγή κλοπών. Καθώς, το κόστος υλοποίησής του δεν ξεπέρασε τα 80 ευρώ, μπορούν όλοι εύκολα να το εντάξουν στα σπίτια τους, κάνοντας ίσως και κάποιες από βελτιώσεις που προτείνονται στο τέλος του κεφαλαίου.

3.3 Προβλήματα και Αντιμετώπιση

Όσον αφορά την ανάπτυξη και την υλοποίηση του κατασκευαστικού μέρους της εργασίας, προέκυψαν μερικά προβλήματα τα οποία και αντιμετωπίστηκαν. Κατά κύριο λόγο, το δυσκολότερο σημείο ήταν η μεταφορά μηνυμάτων από την ροή της Σειριακής Οθόνης του Arduino, μέσω της μονάδας Bluetooth, και η αξιοποίησή τους στην Android εφαρμογή. Επιπλέον, με το άνοιγμα της κλειδαριάς, χανόταν η επικοινωνία στη σύνδεση του κινητού με τη μονάδα Bluetooth. Αυτό αντιμετωπίστηκε με διορθώσεις στον κώδικα και επανεγκατάσταση της εφαρμογής στο κινητό.

3.4 Συμπεράσματα

Η διπλωματική αυτή εργασία είχε ως κύριο στόχο την ανάπτυξη ενός ασφαλούς συστήματος αναγνώρισης ανθρώπων μέσω των δακτυλικών τους αποτυπωμάτων για απόκτηση πρόσβασης σε χώρους, αξιοποιώντας έτσι την χρήση της βιομετρίας. Ο στόχος αυτός επιτεύχθηκε δημιουργώντας ένα αυτοματοποιημένο σύστημα, το όποιο είναι απόλυτα ικανό να επεκταθεί και να λάβει βελτιώσεις, ώστε να ενταχθεί σε ολοένα και περισσότερους χώρους ή εγκαταστάσεις και να καλύψει τις ανάγκες

διαφορετικών χρηστών. Ο μικροελεγκτής που χρησιμοποιήθηκε διαθέτει αρκετές ακόμα ελεύθερες θέσεις για εισόδους και εξόδους, τόσο ψηφιακές όσο και αναλογικές, με αποτέλεσμα να μπορεί να αξιοποιηθεί χωρίς να χρειάζεται η αγορά πιο εξελιγμένου.

Συνεπώς, βελτιώνοντας τους κώδικες που έχουν αναπτυχθεί, αλλά και τα επίπεδα ασφαλείας, με τρόπους που αναφέρονται στην επόμενη ενότητα, επιτυγχάνεται η μελλοντική εξέλιξη του συστήματος αυτού, όσον αφορά την λειτουργικότητα και την αξιοπιστία του.

3.5 Προτάσεις Μελλοντικής Εξέλιξης

Το σύστημα που υλοποιήθηκε είναι ικανό να χρησιμοποιηθεί σε εφαρμογές όπου υπάρχει ανάγκη για ηλεκτρονική πρόσβαση σε χώρους, αξιοποιώντας τα οφέλη της βιομετρίας των δακτυλικών αποτυπωμάτων. Η μέθοδος αυτή παρέχει σε αρκετά μεγάλο βαθμό ένα ασφαλές και αξιόπιστο σύστημα, στο οποίο η πρόσβαση παρέχεται μόνο κατόπιν ελέγχου των χρηστών που είναι εξουσιοδοτημένοι. Σε συνδυασμό με τις ανάγκες κάθε ατόμων που θα χρησιμοποιήσουν το σύστημα, μπορούν να γίνουν επιπλέον βελτιώσεις αλλά και προσθήκες.

Μια μελλοντική βελτίωση στο σύστημα μπορεί να θεωρηθεί η ένταξη ενός λογισμικού στον Η/Υ που θα είναι συνδεδεμένο με το Arduino και θα μπορεί να κρατάει ιστορικό από τις κινήσεις των χρηστών που έχουν εισέλθει στον χώρο. Με αυτόν τον τρόπο, ο διαχειριστής θα έχει τη δυνατότητα να ανατρέχει στα αρχεία αυτά και να βλέπει λεπτομέρειες, όπως ημερομηνία και ώρα, για τα άτομα που πέρασαν τον έλεγχο. Ακόμη, αν τοποθετηθεί μια επιπλέον μονάδα σάρωσης δακτυλικών αποτυπωμάτων στην έξοδο του χώρου, ο διαχειριστής θα έχει πλήρη έλεγχο και για την ώρα παραμονής των ατόμων που εισήλθαν.

Μια άλλη βελτιωμένη παραλλαγή που μπορεί να ενταχθεί στο σύστημα είναι η αντικατάσταση της μονάδας Bluetooth με μια μονάδα Wi-Fi. Το Bluetooth σαν τεχνολογία έχει εμβέλεια μόλις 10 μέτρα και έτσι ο διαχειριστής είναι υποχρεωμένος να βρίσκεται πολύ κοντά στο σύστημα ελέγχου, ώστε να μπορεί να το χειρίζεται και να έχει εικόνα της σωστής λειτουργίας του. Η χρήση του Wi-Fi, λοιπόν, θα του επιτρέψει να βρίσκεται μακριά από τον χώρο αυτό, καθώς η μονάδα αυτή αποστέλλει δεδομένα μέσω του δικτύου και έτσι θα μπορεί να συνδέεται στην εφαρμογή χειρισμού απομακρυσμένα όπου κι αν βρεθεί.

Σε συνδυασμό με την παραπάνω βελτίωση με τη χρήση του Wi-Fi, ένα ακόμη επιπλέον όφελος είναι ότι ο διαχειριστής θα μπορεί να λαμβάνει ειδοποιήσεις στο κινητό του τηλέφωνο έχοντας την εφαρμογή χειρισμού κλειστή. Εφόσον είναι συνδεδεμένος σε κάποιο δίκτυο, τότε κάθε φορά που χρειάζεται, για

παράδειγμα, να δώσει εντολή για να «ξεμπλοκάρει» το σύστημα, το κινητό του θα ειδοποιείται με το αντίστοιχο μήνυμα. Αυτό δίνει την δυνατότητα στον διαχειριστή να απασχολείται και με άλλες αρμοδιότητες ταυτόχρονα, χωρίς να έχει συνεχώς ανοιχτή την εφαρμογή.

Επιπρόσθετα, μπορεί να υλοποιηθεί μια εφαρμογή, την οποία οι χρήστες θα κατεβάζουν στο κινητό τους τηλέφωνο. Εφόσον το κινητό τηλέφωνό τους διαθέτει σαρωτή δακτυλικού αποτυπώματος, θα είναι σε θέση να ανοίγουν την εφαρμογή και να σαρώνουν στην συσκευή τους το δάκτυλο. Έτσι, δεν είναι αναγκασμένοι να αγγίζουν την επιφάνεια της μονάδα σάρωσης που είναι τοποθετημένη έξω από την πόρτα, κάτι το οποίο είναι πολύ πρακτικό τη σημερινή εποχή, κυρίως, για λόγους υγιεινής.

Τέλος, επειδή η σάρωση των δακτυλικών αποτυπωμάτων μπορεί να επηρεαστεί από εξωτερικές συνθήκες, όπως υγρασία ή κάποιον τραυματισμό, και έτσι θα είναι χρήσιμο να υπάρχει μια ακόμα εναλλακτική βιομετρικού ελέγχου όπως για παράδειγμα η σάρωση της ίριδας του ματιού ή η αναγνώριση της φωνής. Αν ο χρήστης που επιθυμεί πρόσβαση είναι εξουσιοδοτημένος και το δάκτυλο του δεν αναγνωρίζεται, θα μπορεί, συνεπώς, να αποκτήσει είσοδο με άλλον τρόπο αντί να του απαγορεύεται τελείως η πρόσβαση. Εναλλακτικά, αντί της βιομετρίας, μπορεί να τοποθετηθεί και ένας πιο παραδοσιακός τρόπος εισόδου, όπως είναι οι κωδικοί PIN, όμως υπάρχει μεγάλη πιθανότητα να μειώσει την αξιοπιστία του συστήματος αυτού.

Βιβλιογραφία – Αναφορές – Διαδικτυακές Πηγές

Adafruit Optical Fingerprint Sensor. (n.d.). Retrieved May 9, 2022, from https://learn.adafruit.com/adafruit-optical-fingerprint-sensor?view=all

Ashbaugh, D. R. (1999). *Quantitative-qualitative friction ridge analysis: an introduction to basic and advanced ridgeology*. CRC press.

Atmel. (n.d.) Retrieved May 9, 2022, from https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf

Benhammadi, F., Amirouche, M. N., Hentous, H., Beghdad, K. B., & Aissani, M. (2007). Fingerprint matching from minutiae texture maps. *Pattern recognition*, *40*(1), 189-197.

Biometrics. (n.d.). Retrieved April 27, 2022, from https://www.flexenable.com/applications/biometrics/

Biometric Access Control Systems. (n.d.). Retrieved May 7, 2022, from https://www.keyo.co/biometric-news/biometric-access-control-systems-101-everything-you-should-know

Biometric security systems: a guide to devices, fingerprint scanners and facial recognition access control. (n.d.). Retrieved May 2, 2022, from https://www.ifsecglobal.com/global/biometric-security-systems-guide-devices-fingerprint-scanners-facial-recognition/

Dorai, C., Ratha, N., & Bolle, R. (2004). Dynamic behavior in fingerprint videos. In *Automatic fingerprint recognition systems* (pp. 67-86). Springer, New York, NY.

Edwards D. G. (1984). *Fingerprint sensor*. US.

Everything You Should Know About Biometric Access Control Systems. (n.d.). Retrieved May 7, 2022, from https://www.smartisystems.com/biometric-access-control-systems.php#:~:text=A%20biometric%20access%20system%20is,saved%20data%20to%20allow%20access.

Fang, G., Srihari, S. N., Srinivasan, H., & Phatak, P. (2007, April). Use of ridge points in partial fingerprint matching. In *Biometric Technology for Human Identification IV* (Vol. 6539, p. 65390D). International Society for Optics and Photonics.

FAR and FRR: security level versus user convenience. (n.d.). Retrieved April 9, 2022, from https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience

Fujieda, I., Ono, Y., & Sugama, S. (1995). *U.S. Patent No. 5,446,290*. Washington, DC: U.S. Patent and Trademark Office.

Hatano, T., Adachi, T., Shigematsu, S., Morimura, H., Onishi, S., Okazaki, Y., & Kyuragi, H. (2002, August). A fingerprint verification algorithm using the differential matching rate. In *Object recognition supported by user interaction for service robots* (Vol. 3, pp. 799-802). IEEE.

Henry, E. R. (1900). Classification and Uses of Finger Prints.[Sl]: George Routledge and Sons.

Hong, L., Wan, Y., & Jain, A. (1998). Fingerprint image enhancement: algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence*, *20*(8), 777-789.

Jain, A., Bolle, R., & Pankanti, S. (Eds.). (1999). *Biometrics: personal identification in networked society* (Vol. 479). Springer Science & Business Media.

Jain, A. K., Prabhakar, S., & Ross, A. (1999). Fingerprint matching: Data acquisition and performance evaluation. *Dept. of Computer Science, Michigan State Univ., East Lansing, Tech. Rep. MSU-CPS-99–14*.

Jain, A. K., & Feng, J. (2010). Latent fingerprint matching. *IEEE Transactions on pattern analysis and machine intelligence*, *33*(1), 88-100.

Kindt, E. J. (2013). An introduction into the use of biometric technology. In *Privacy and Data Protection Issues of Biometric Applications* (pp. 15-85). Springer, Dordrecht.

Maio, D., Maltoni, D., Cappelli, R., Franco, A., Ferrara, M., & Turroni, F. (2013). FVC-onGoing: on-line evaluation of fingerprint recognition algorithms.

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K. (2002, August). FVC2002: Second fingerprint verification competition. In *Object recognition supported by user interaction for service robots* (Vol. 3, pp. 811-814). IEEE.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition*. Springer Science & Business Media.

Mathur, S., Vjay, A., Shah, J., Das, S., & Malla, A. (2016, June). Methodology for partial fingerprint enrollment and authentication on mobile devices. In *2016 International Conference on Biometrics (ICB)* (pp. 1-8). IEEE.

Optical versus ultrasonic: The difference between in-display fingerprint scanners. (n.d.). Retrieved May 2, 2022, from https://www.androidguys.com/tips-tools/whats-difference-between-optical-ultrasonic-in-display-fingerprint-scanner/

Rahmawati, E., Listyasari, M., Aziz, A. S., Sukaridhoto, S., Damastuti, F. A., Bachtiar, M. M., & Sudarsono, A. (2017, September). Digital signature on file using biometric fingerprint with fingerprint sensor on smartphone. In *2017 International Electronics Symposium on Engineering Technology and Applications (IES-ETA)* (pp. 234-238). IEEE.

Relay Module - 1 Channel 5V Low Level Trigger (Screw Terminals). (n.d.). Retrieved May 10, 2022, from https://grobotronics.com/relay-module-1-channel-5v-high-level-trigger-screw-terminals.html

Riaz, N., Riaz, A., & Khan, S. A. (2017). Biometric template security: an overview. *Sensor Review*, *38*(1), 120-127.

Smart Cards. (n.d.). Retrieved April 19, 2022, from https://findbiometrics.com/solutions/smart-cards/

Wayman, J. L. (1999). Error rate equations for the general biometric system. *IEEE Robotics & Automation Magazine*, *6*(1), 35-48.

What is an Arduino? (n.d.). Retrieved May 8, 2022, from https://learn.sparkfun.com/tutorials/what-is-an-arduino/all

Yamazaki, M., Li, D., Isshiki, T., & Kunieda, H. (2015, March). SIFT-based algorithm for fingerprint authentication on smartphone. In *2015 6th International Conference of Information and Communication Technology for Embedded Systems (IC-ICTES)* (pp. 1-5). IEEE.

Zhang, Z., Shan, S., Fang, Y., & Shao, L. (2019). Deep learning for pattern recognition. *Pattern Recognition Letters*, *119*, 1-2.

Παράρτημα

Αρχικά παρατίθεται ο κώδικας ***enroll*** που περιέχει η βιβλιοθήκη της Adafruit για την εγγραφή των δακτυλικών αποτυπωμάτων στη βάση δεδομένων.

```
#include <Adafruit_Fingerprint.h>
#if (defined(__AVR__) || defined(ESP8266)) && !defined(__AVR_ATmega2560__)
SoftwareSerial mySerial(2, 3);
#else
#define mySerial Serial1
#endif

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

uint8_t id;

void setup()
{
  Serial.begin(9600);
  while (!Serial);
  delay(100);
  Serial.println("\n\nAdafruit Fingerprint sensor enrollment");
  finger.begin(57600);

  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1) { delay(1); }
  }

  Serial.println(F("Reading sensor parameters"));
  finger.getParameters();
  Serial.print(F("Status: 0x")); Serial.println(finger.status_reg, HEX);
  Serial.print(F("Sys ID: 0x")); Serial.println(finger.system_id, HEX);
  Serial.print(F("Capacity: ")); Serial.println(finger.capacity);
  Serial.print(F("Security level: ")); Serial.println(finger.security_level);
  Serial.print(F("Device address: ")); Serial.println(finger.device_addr, HEX);
  Serial.print(F("Packet len: ")); Serial.println(finger.packet_len);
  Serial.print(F("Baud rate: ")); Serial.println(finger.baud_rate);
}

uint8_t readnumber(void) {
  uint8_t num = 0;

  while (num == 0) {
    while (! Serial.available());
    num = Serial.parseInt();
  }
  return num;
}
```

```
47
48 void loop()
49 {
50   Serial.println("Ready to enroll a fingerprint!");
51   Serial.println("Please type in the ID # (from 1 to 127) you want to save this finger as...");
52   id = readnumber();
53   if (id == 0) {
54      return;
55   }
56   Serial.print("Enrolling ID #");
57   Serial.println(id);
58   while (!  getFingerprintEnroll() );
59 }
60
61 uint8_t getFingerprintEnroll() {
62
63   int p = -1;
64   Serial.print("Waiting for valid finger to enroll as #"); Serial.println(id);
65   while (p != FINGERPRINT_OK) {
66     p = finger.getImage();
67     switch (p) {
68     case FINGERPRINT_OK:
69       Serial.println("Image taken");
70       break;
71     case FINGERPRINT_NOFINGER:
72       Serial.println(".");
73       break;
74     case FINGERPRINT_PACKETRECIEVEERR:
75       Serial.println("Communication error");
76       break;
77     case FINGERPRINT_IMAGEFAIL:
78       Serial.println("Imaging error");
79       break;
80     default:
81       Serial.println("Unknown error");
82       break;
83     }
84   }
85
```

```
  p = finger.image2Tz(1);
  switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image converted");
      break;
    case FINGERPRINT_IMAGEMESS:
      Serial.println("Image too messy");
      return p;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      return p;
    case FINGERPRINT_FEATUREFAIL:
      Serial.println("Could not find fingerprint features");
      return p;
    case FINGERPRINT_INVALIDIMAGE:
      Serial.println("Could not find fingerprint features");
      return p;
    default:
      Serial.println("Unknown error");
      return p;
  }

  Serial.println("Remove finger");
  delay(2000);
  p = 0;
  while (p != FINGERPRINT_NOFINGER) {
    p = finger.getImage();
  }
  Serial.print("ID "); Serial.println(id);
  p = -1;
  Serial.println("Place same finger again");
  while (p != FINGERPRINT_OK) {
    p = finger.getImage();
    switch (p) {
    case FINGERPRINT_OK:
      Serial.println("Image taken");
      break;
    case FINGERPRINT_NOFINGER:
      Serial.print(".");
      break;
    case FINGERPRINT_PACKETRECIEVEERR:
      Serial.println("Communication error");
      break;
    case FINGERPRINT_IMAGEFAIL:
      Serial.println("Imaging error");
      break;
    default:
      Serial.println("Unknown error");
      break;
    }
  }
```

```
137
138   p = finger.image2Tz(2);
139   switch (p) {
140     case FINGERPRINT_OK:
141       Serial.println("Image converted");
142       break;
143     case FINGERPRINT_IMAGEMESS:
144       Serial.println("Image too messy");
145       return p;
146     case FINGERPRINT_PACKETRECIEVEERR:
147       Serial.println("Communication error");
148       return p;
149     case FINGERPRINT_FEATUREFAIL:
150       Serial.println("Could not find fingerprint features");
151       return p;
152     case FINGERPRINT_INVALIDIMAGE:
153       Serial.println("Could not find fingerprint features");
154       return p;
155     default:
156       Serial.println("Unknown error");
157       return p;
158   }
159
160   Serial.print("Creating model for #");  Serial.println(id);
161
162   p = finger.createModel();
163   if (p == FINGERPRINT_OK) {
164     Serial.println("Prints matched!");
165   } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
166     Serial.println("Communication error");
167     return p;
168   } else if (p == FINGERPRINT_ENROLLMISMATCH) {
169     Serial.println("Fingerprints did not match");
170     return p;
171   } else {
172     Serial.println("Unknown error");
173     return p;
174   }
175
176   Serial.print("ID "); Serial.println(id);

177   p = finger.storeModel(id);
178   if (p == FINGERPRINT_OK) {
179     Serial.println("Stored!");
180   } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
181     Serial.println("Communication error");
182     return p;
183   } else if (p == FINGERPRINT_BADLOCATION) {
184     Serial.println("Could not store in that location");
185     return p;
186   } else if (p == FINGERPRINT_FLASHERR) {
187     Serial.println("Error writing to flash");
188     return p;
189   } else {
190     Serial.println("Unknown error");
191     return p;
192   }
193
194   return true;
195 }
```

Επιπλέον, ο κώδικας ***emptyDatabase*** για την διαγραφή δακτυλικών αποτυπωμάτων από την βάση δεδομένων είναι ο εξής:

```
#include <Adafruit_Fingerprint.h>
#if (defined(__AVR__) || defined(ESP8266)) && !defined(__AVR_ATmega2560__)
SoftwareSerial mySerial(2, 3);
#else
#define mySerial Serial1
#endif

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

void setup()
{
  Serial.begin(9600);
  while (!Serial);
  delay(100);
  Serial.println("\n\nDeleting all fingerprint templates!");
  Serial.println("Press 'Y' key to continue");
  while (1) {
    if (Serial.available() && (Serial.read() == 'Y')) {
      break;
    }
  }
  finger.begin(57600);
  if (finger.verifyPassword()) {
    Serial.println("Found fingerprint sensor!");
  } else {
    Serial.println("Did not find fingerprint sensor :(");
    while (1);
  }
  finger.emptyDatabase();
  Serial.println("Now database is empty :)");
}

void loop() {

}
```

Τέλος, παρακάτω παρατίθεται ο κώδικας που εμπεριέχει η Java τάξη ***BluetoothConnectionService*** για την επικοινωνία της μονάδας Bluetooth HC-05.

```
package com.example.fingerprint_identification_system;

import ...

public class BluetoothConnectionService {
    private static final String TAG = "BluetoothConnectionServ";
    private static final String appName = "MYAPP";
    private static final UUID MY_UUID_INSECURE = UUID.fromString("a4dbf17f-7dd7-4f71-9684-d2a59b88624c");
    private final BluetoothAdapter mBluetoothAdapter;
    Context mContext;
    private AcceptThread mInsecureAcceptThread;
    private ConnectThread mConnectThread;
    private BluetoothDevice mmDevice;
    private UUID deviceUUID;
    ProgressDialog mProgressDialog;
    private ConnectedThread mConnectedThread;

    public BluetoothConnectionService(Context context) {
        mContext = context;
        mBluetoothAdapter = BluetoothAdapter.getDefaultAdapter();
        start();
    }

    private class AcceptThread extends Thread {
        private final BluetoothServerSocket mmServerSocket;
        public AcceptThread(){
            BluetoothServerSocket tmp = null;
            try{
                tmp = mBluetoothAdapter.listenUsingInsecureRfcommWithServiceRecord(appName, MY_UUID_INSECURE);
                Log.d(TAG, msg: "AcceptThread: Setting up Server using: " + MY_UUID_INSECURE);
            }catch (IOException e){
                Log.e(TAG, msg: "AcceptThread: IOException: " + e.getMessage() );
            }
            mmServerSocket = tmp;
        }

        public void run(){
            Log.d(TAG, msg: "run: AcceptThread Running.");
            BluetoothSocket socket = null;
            try{
                Log.d(TAG, msg: "run: RFCOM server socket start.....");
                socket = mmServerSocket.accept();
                Log.d(TAG, msg: "run: RFCOM server socket accepted connection.");
            }catch (IOException e){
                Log.e(TAG, msg: "AcceptThread: IOException: " + e.getMessage() );
            }
            if(socket != null){
                connected(socket,mmDevice);
            }
            Log.i(TAG, msg: "END mAcceptThread ");
        }
```

```
67
68          public void cancel() {
69              Log.d(TAG, msg: "cancel: Canceling AcceptThread.");
70              try {
71                  mmServerSocket.close();
72              } catch (IOException e) {
73                  Log.e(TAG, msg: "cancel: Close of AcceptThread ServerSocket failed. " + e.getMessage() );
74              }
75          }
76      }
77
78      private class ConnectThread extends Thread {
79          private BluetoothSocket mmSocket;
80
81          public ConnectThread(BluetoothDevice device, UUID uuid) {
82              Log.d(TAG, msg: "ConnectThread: started.");
83              mmDevice = device;
84              deviceUUID = uuid;
85          }
86
87          public void run(){
88              BluetoothSocket tmp = null;
89              Log.i(TAG, msg: "RUN mConnectThread ");
90              try {
91                  Log.d(TAG, msg: "ConnectThread: Trying to create InsecureRfcommSocket using UUID: "
92                          +MY_UUID_INSECURE );
93                  tmp = mmDevice.createRfcommSocketToServiceRecord(deviceUUID);
94              } catch (IOException e) {
95                  Log.e(TAG, msg: "ConnectThread: Could not create InsecureRfcommSocket " + e.getMessage());
96              }
97
98              mmSocket = tmp;
99              mBluetoothAdapter.cancelDiscovery();
100             try {
101                 mmSocket.connect();
102                 Log.d(TAG, msg: "run: ConnectThread connected.");
103             } catch (IOException e) {
104                 try {
105                     mmSocket.close();
106                     Log.d(TAG, msg: "run: Closed Socket.");
107                 } catch (IOException e1) {
108                     Log.e(TAG, msg: "mConnectThread: run: Unable to close connection in socket " + e1.getMessage());
109                 }
110                 Log.d(TAG, msg: "run: ConnectThread: Could not connect to UUID: " + MY_UUID_INSECURE );
111             }
112             connected(mmSocket,mmDevice);
113         }
114         public void cancel() {
115             try {
116                 Log.d(TAG, msg: "cancel: Closing Client Socket.");
117                 mmSocket.close();
118             } catch (IOException e) {
119                 Log.e(TAG, msg: "cancel: close() of mmSocket in Connectthread failed. " + e.getMessage());
120             }
121         }
122     }
```

```
123
124     public synchronized void start() {
125         Log.d(TAG,  msg: "start");
126         if (mConnectThread != null) {
127             mConnectThread.cancel();
128             mConnectThread = null;
129         }
130         if (mInsecureAcceptThread == null) {
131             mInsecureAcceptThread = new AcceptThread();
132             mInsecureAcceptThread.start();
133         }
134     }
135
136     public void startClient(BluetoothDevice device,UUID uuid){
137         Log.d(TAG,  msg: "startClient: Started.");
138         mProgressDialog = ProgressDialog.show(mContext, title: "Connecting Bluetooth"
139                 , message: "Please Wait...", indeterminate: true);
140
141         mConnectThread = new ConnectThread(device, uuid);
142         mConnectThread.start();
143     }
144
145     private class ConnectedThread extends Thread {
146         private final BluetoothSocket mmSocket;
147         private final InputStream mmInStream;
148         private final OutputStream mmOutStream;
149
150         public ConnectedThread(BluetoothSocket socket) {
151             Log.d(TAG,  msg: "ConnectedThread: Starting.");
152
153             mmSocket = socket;
154             InputStream tmpIn = null;
155             OutputStream tmpOut = null;
156             try{
157                 mProgressDialog.dismiss();
158             }catch (NullPointerException e){
159                 e.printStackTrace();
160             }
161
162             try {
163                 tmpIn = mmSocket.getInputStream();
164                 tmpOut = mmSocket.getOutputStream();
165             } catch (IOException e) {
166                 e.printStackTrace();
167             }
168
169             mmInStream = tmpIn;
170             mmOutStream = tmpOut;
171         }
172
```

```
173        public void run(){
174            byte[] buffer = new byte[1024];
175            int bytes;
176            while (true) {
177                try {
178                    if (mmInStream.available() > 0) {
179                        bytes = mmInStream.read(buffer);
180                        String incomingMessage = new String(buffer,  offset: 0, bytes);
181                        Log.d(TAG,  msg: "InputStream: " + incomingMessage);
182
183                        Intent incomingMessageIntent = new Intent( action: "incomingMessage");
184                        incomingMessageIntent.putExtra( name: "theMessage", incomingMessage);
185                        LocalBroadcastManager.getInstance(mContext).sendBroadcast(incomingMessageIntent);
186                    }
187                } catch (IOException e) {
188                    Log.e(TAG,  msg: "write: Error reading Input Stream. " + e.getMessage());
189                    e.printStackTrace();
190                    break;
191                }
192            }
193        }
194
195        public void write(byte[] bytes) {
196            String text = new String(bytes, Charset.defaultCharset());
197            Log.d(TAG,  msg: "write: Writing to outputstream: " + text);
198            try {
199                mmOutStream.write(bytes);
200            } catch (IOException e) {
201                Log.e(TAG,  msg: "write: Error writing to output stream. " + e.getMessage());
202                e.printStackTrace();
203            }
204        }
205
206        public void cancel() {
207            try {
208                mmSocket.close();
209            } catch (IOException e) { }
210        }
211    }
212
213    private void connected(BluetoothSocket mmSocket, BluetoothDevice mmDevice) {
214        Log.d(TAG,  msg: "connected: Starting.");
215        mConnectedThread = new ConnectedThread(mmSocket);
216        mConnectedThread.start();
217    }
218    public void write(byte[] out) {
219        ConnectedThread r;
220        Log.d(TAG,  msg: "write: Write Called.");
221        mConnectedThread.write(out);
222    }
223 }
```