ΑΝΩΤΑΤΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΠΕΙΡΑΙΑ
ΤΕΧΝΟΛΟΓΙΚΟΥ ΤΟΜΕΑ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΑΥΤΟΜΑΤΙΣΜΟΥ

ΘΕΜΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

" ΑΥΤΟΜΑΤΟ ΣΥΣΤΗΜΑ ΑΣΦΑΛΕΙΑΣ ΜΕ ΔΑΚΤΥΛΙΚΟ ΑΠΟΤΥΠΩΜΑ "

ΟΝΟΜΑΤΑ ΦΟΙΤΗΤΩΝ :

ΕΛ ΓΚΑΜΑΛ ΔΗΜΗΤΡΙΟΣ, 44602

ΜΑΤΣΙΚΑ ΣΠΥΡΙΔΟΥΛΑ , 44552

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΠΟΥΤΣΙΔΑΚΗΣ ΜΙΧΑΛΗΣ

ΑΙΓΑΛΕΩ, ΦΕΒΡΟΥΑΡΙΟΣ 2017

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Ελ Γκάμαλ Δημήτριος ,

Του Μαχμούτ , με αριθμό μητρώου 44602 φοιτητής του Τμήματος **Μηχανικών Αυτοματισμού Τ.Ε.** του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

Ο Δηλών Ημερομηνία

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Η κάτωθι υπογεγραμμένη Μάτσικα Σπυριδούλα,

Του Διονυσίου, με αριθμό μητρώου 44552 φοιτήτρια του Τμήματος **Μηχανικών Αυτοματισμού Τ.Ε.** του Α.Ε.Ι. Πειραιά Τ.Τ. πριν αναλάβω την εκπόνηση της Πτυχιακής Εργασίας μου, δηλώνω ότι ενημερώθηκα για τα παρακάτω:

«Η Πτυχιακή Εργασία (Π.Ε.) αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο του συγγραφέα, όσο και του Ιδρύματος και θα πρέπει να έχει μοναδικό χαρακτήρα και πρωτότυπο περιεχόμενο.

Απαγορεύεται αυστηρά οποιοδήποτε κομμάτι κειμένου της να εμφανίζεται αυτούσιο ή μεταφρασμένο από κάποια άλλη δημοσιευμένη πηγή. Κάθε τέτοια πράξη αποτελεί προϊόν λογοκλοπής και εγείρει θέμα Ηθικής Τάξης για τα πνευματικά δικαιώματα του άλλου συγγραφέα. Αποκλειστικός υπεύθυνος είναι ο συγγραφέας της Π.Ε., ο οποίος φέρει και την ευθύνη των συνεπειών, ποινικών και άλλων, αυτής της πράξης.

Πέραν των όποιων ποινικών ευθυνών του συγγραφέα σε περίπτωση που το Ίδρυμα του έχει απονείμει Πτυχίο, αυτό ανακαλείται με απόφαση της Συνέλευσης του Τμήματος. Η Συνέλευση του Τμήματος με νέα απόφασης της, μετά από αίτηση του ενδιαφερόμενου, του αναθέτει εκ νέου την εκπόνηση της Π.Ε. με άλλο θέμα και διαφορετικό επιβλέποντα καθηγητή. Η εκπόνηση της εν λόγω Π.Ε. πρέπει να ολοκληρωθεί εντός τουλάχιστον ενός ημερολογιακού 6μήνου από την ημερομηνία ανάθεσης της. Κατά τα λοιπά εφαρμόζονται τα προβλεπόμενα στο άρθρο 18, παρ. 5 του ισχύοντος Εσωτερικού Κανονισμού.»

Ο Δηλών Ημερομηνία

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

Κεφάλαιο 1 – Εισαγωγή

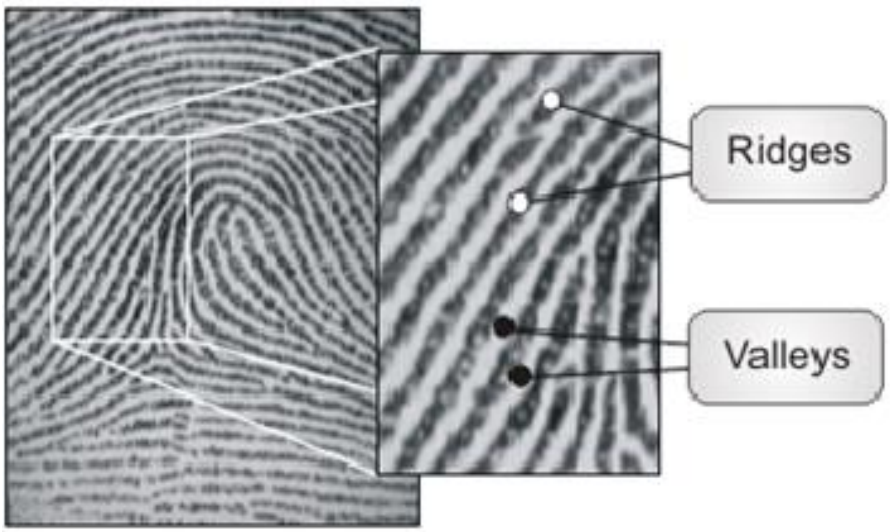
1.1. Ιστορική αναδρομή

Η χρήση των δακτυλικών αποτυπωμάτων για βιομετρική ταυτοποίηση, δηλαδή για αναγνώρισης ατόμων, ξεκινάει από τα τέλη του 19ο αιώνα. Για πρώτη φορά συστηματική μελέτη στο θέμα της ταυτοποίησης ατόμων έγινε το 1880 από τον ανθρωπολόγο Francis Galton. Ταξινόμησε τα δακτυλικά αποτυπώματα και κατηγοριοποίησε τα χαρακτηριστικά ή λεπτομέρειες τους με στόχο να μπορεί να καθορίζει πότε ταιριάζουν δυο δακτυλικά αποτυπώματα. Το 1892 ο Juan Vucetich, ένας αστυνόμος από την Αργεντινή χρησιμοποιώντας την μελέτη του Francis Galton έκανε την πρώτη χρήση ταυτοποίησης με δακτυλικά αποτυπώματα για την εξιχνίαση ενός εγκλήματος. Συγκεκριμένα η αναγνώριση έγινε από ένα δακτυλικό αποτύπωμα με αίμα που άφησε ο δολοφόνος στον τόπο του εγκλήματος. Επισήμως η χρήση δακτυλικών αποτυπωμάτων για την εξιχνίαση εγκλημάτων έγινε από τον Edward Henry της Scotland Yard το 1901 χρησιμοποιώντας το σύστημα του Francis Galton , το οποίο το εξέλιξε.

Ως βιομετρικά χαρακτηριστικά ορίζονται τα φυσικά χαρακτηριστικά ή τα γνωρίσματα εκείνα της συμπεριφοράς ενός ατόμου τα οποία μπορούν να χρησιμοποιηθούν για να αναγνωριστεί η ταυτότητά του. Η βιομετρική αναγνώριση αναφέρεται στη χρήση διαχωρίσιμων φυσικών χαρακτηριστικών (δακτυλικά αποτυπώματα, ίριδα) και χαρακτηριστικών της συμπεριφοράς (υπογραφή, φωνή) για την αναγνώριση ατόμων. Τα φυσικά χαρακτηριστικά σχετίζονται άμεσα με την συμπεριφορά ενός ατόμου με αποτέλεσμα η αναγνώριση ενός ατόμου να αποτελεί συνδυασμό και τον δύο χαρακτηριστικών. Παράδειγμα αποτελούν τα δακτυλικά αποτυπώματα τα οποία μπορεί να είναι φυσικά χαρακτηριστικά αλλά ο τρόπος με τον οποίο γίνεται η τοποθέτηση τους στην συσκευή αναγνώρισης, δηλαδή με ποιο σημείο του δακτύλου ο χρήστης θα ασκήσει την μεγαλύτερη πίεση στην επιφάνεια του αισθητήρα και με ποια γωνία, εξαρτάται από την συμπεριφορά του ατόμου.

Η φωνή μπορεί να αποτελεί ένα χαρακτηριστικό που διαμορφώνεται κυρίως από την συμπεριφορά του ατόμου, δηλαδή την διάθεσή του, εάν μιλάει δυνατά ή χαμηλά ,αλλά η βιολογική δομή του συστήματος ομιλίας ενός ατόμου που αποτελεί φυσικό χαρακτηριστικό έχει σημαντικό ρόλο στην αναγνώριση.

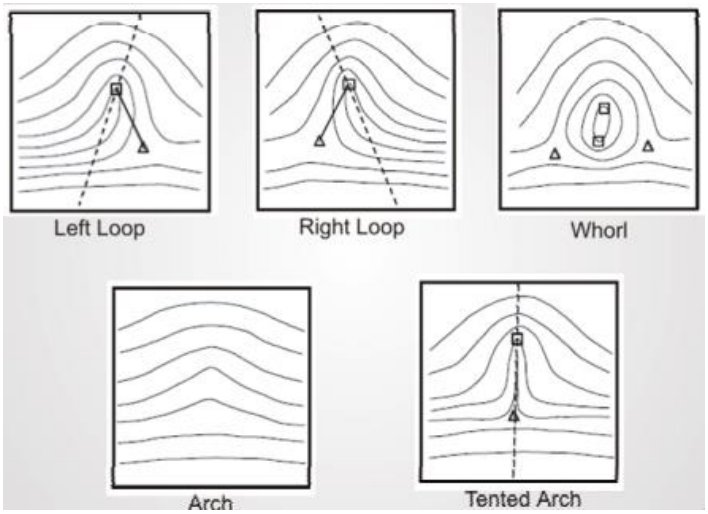
Τα χαρακτηριστικά των δακτυλικών αποτυπωμάτων καθορίζουν την μοναδικότητα και με βάση την θέση τους, το σχήμα τους και το μέγεθός τους γίνεται η αναγνώριση του ατόμου. Τα βασικότερα χαρακτηριστικά είναι οι διαδοχικές κοιλάδες (valleys) και παρυφές (ridges) της επιδερμίδας που βρίσκεται στο δακτυλικό αποτύπωμα. Συνήθως σε μια εικόνα δακτυλικού αποτυπώματος οι κοιλάδες (valleys) είναι άσπρες και οι παρυφές (ridges) μαύρες. Οι παρυφές έχουν πάχος συνήθως 100- 300μm και οι κοιλάδες 200μm.



Εικόνα 1.1(Κοιλάδες και Παρυφές δακτυλικού αποτυπώματος)

Συνήθως οι παρυφές και οι κοιλάδες βρίσκονται παράλληλα η μια στην άλλη μέχρι μια παρυφή να διακλαδωθεί σε δύο παρυφές ή να τερματίσει απότομα. Όταν αναλύουμε το δακτυλικό αποτύπωμα σε γενικό επίπεδο μπορούμε να παρατηρήσουμε μία ή δύο περιοχές στις οποίες οι παρυφές και οι κοιλάδες έχουν συγκεκριμένα σχήματα. Αυτές οι περιοχές ονομάζονται ιδιαίτερες (singular regions) και διαχωρίζονται στις κατηγορίες δέλτα σημείο (delta point) και σημείο πυρήνα (core points), σύμφωνα με την μελέτη του Juan Vucetich και του Edward Henry, και χαρακτηρίζονται από μεγάλη καμπυλότητα των παρυφών και

των κοιλάδων και απότομων τερματισμών αυτών. Συγκεκριμένα ως σημεία δέλτα χαρακτηρίζονται τα σημεία στα οποία διασταυρώνονται παρυφές και κοιλάδες με τρεις διαφορετικές διευθύνσεις όπου κάθε διεύθυνση απέχει 120^{o} από τις άλλες δύο όπως παρουσιάζεται στο παρακάτω σχήμα με το τρίγωνο.



Εικόνα 1.2(Διευθύνσεις διασταύρωσης παρυφών και κοιλάδων, Σημείο Δ)

Η συνήθης κατηγοριοποίηση των σημείων πυρήνα παρουσιάζεται στο παραπάνω σχήμα, όπου τα σημεία αυτά παριστάνονται με τετράγωνο. Η διαφοροποίηση της καμπυλότητας των παρυφών και των κοιλάδων διαμορφώνει τις εξής πέντε κατηγορίες σημείων πυρήνα.

- Αριστερός Βρόγχος (Left Loop)
- Δεξιός Βρόγχος (Right Loop)
- Δακτύλιος (Whorl)
- Αριστερός Βρόγχος (Left Loop)
- Δεξιός Βρόγχος (Right Loop)
- Δακτύλιος (Whorl)

Σε ορισμένα βιομετρικά συστήματα αναγνώρισης υπάρχει και η κατηγορία του διπλού βρόγχου η οποία διακρίνεται πολύ δύσκολα από την κατηγορία του δακτυλίου. Στο

σύστημα της παρούσας εργασίας θεωρούμε μια κατηγορία τον διπλό βρόγχο και τον δακτύλιο. Οι κατηγορίες τεντωμένο τόξο, αριστερός και δεξιός βρόγχος έχουν μόνο ένα δέλτα σημείο ενώ η κατηγορία δακτύλιος έχει δύο δέλτα σημεία. Η κατηγορία τόξο δεν έχει δέλτα σημείο και το σημείο πυρήνα είναι το ποιο δύσκολα αναγνωρίσιμο από τα υπόλοιπα. Ακολούθως παρουσιάζονται τα είδη των σημείων πυρήνα με βάση τα δακτυλικά αποτυπώματα που συλλέξαμε από έναν συγκεκριμένο αισθητήρα με μικρή επιφάνεια. Η μικρή επιφάνεια του αισθητήρα έχει αποτέλεσμα στις παρακάτω εικόνες να μην εμφανίζεται το δέλτα σημείο το οποίο για την συγκεκριμένη εφαρμογή δεν είναι απαραίτητο.

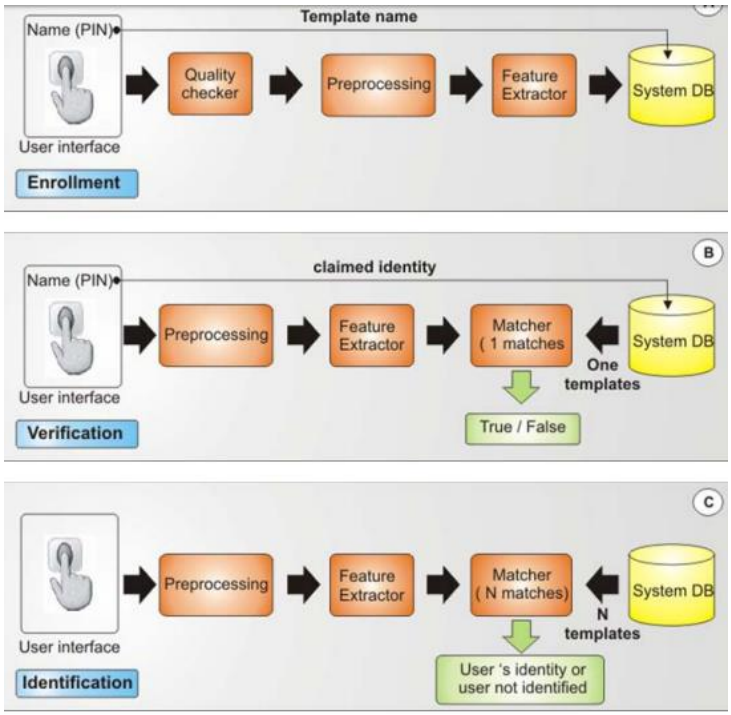
Εικόνα 1.3(Είδη δακτυλικών αποτυπωμάτων του σημείου Πυρήνα)

Ένα βιομετρικό σύστημα είναι ουσιαστικά ένα σύστημα αναγνώρισης προτύπων το οποίο αναγνωρίζει ένα άτομο καθορίζοντας την αυθεντικότητα ενός συγκεκριμένου φυσικού χαρακτηριστικού ή συμπεριφοράς του ατόμου. Κατά τον σχεδιασμό του συστήματος αυτού πρέπει να καθοριστεί πρώτα ο τρόπος με τον οποίο ένα άτομο αναγνωρίζεται. Σύμφωνα με το είδος της αναγνώρισης το σύστημα μπορεί να χωριστεί στις παρακάτω δυο κατηγορίες:

- Σύστημα ταυτοποίησης (Identification) βιομετρικών δεδομένων.
- Σύστημα εξακρίβωσης (Verification) βιομετρικών δεδομένων.

Ένα σύστημα εξακρίβωσης βιομετρικών δεδομένων, αναγνωρίζει την αυθεντικότητα της γνησιότητας της ταυτότητας ενός ατόμου συγκρίνοντας τα αποκτηθέντα από το σύστημα βιομετρικά χαρακτηριστικά με τα πρότυπα βιομετρικά χαρακτηριστικά του ατόμου με την γνήσια ταυτότητα, που έχουν αποθηκευτεί προηγουμένως στο σύστημα. Ένα σύστημα εξακρίβωσης απορρίπτει ή δέχεται ένα άτομο που ισχυρίζεται ότι έχει την συγκεκριμένη ταυτότητα σύμφωνα με τον βαθμό γνησιότητας των βιομετρικών χαρακτηριστικών του.

Ακολούθως το σύστημα ταυτοποίησης αναγνωρίζει ένα άτομο αναζητώντας σε μια μεγάλη βάση δεδομένων, με βιομετρικά χαρακτηριστικά ,την ταυτότητα του ατόμου προς αναγνώριση. Το σύστημα αυτό συγκρίνει ένα προς ένα τα αποθηκευμένα βιομετρικά χαρακτηριστικά της βάσης δεδομένων του συστήματος με τα βιομετρικά χαρακτηριστικά του ατόμου προς αναζήτηση, προκειμένου να εντοπίσει την ταυτότητα του ατόμου. Εάν τα χαρακτηριστικά του ατόμου δεν υπάρχουν στην βάση δεδομένων τότε το σύστημα αποτυγχάνει να τα εντοπίσει (fail). Σε ένα σύστημα ταυτοποίησης δεν υπάρχει ο ισχυρισμός του ατόμου προς αναγνώριση, για την γνησιότητα των βιομετρικών δεδομένων του. Ακολούθως παρουσιάζονται στο παρακάτω σχήμα ο τρόπος με τον οποίο γίνεται η εγγραφή (enrollment), η εξακρίβωση (verification) και η ταυτοποίηση (dentification).



Εικόνα 1.4(Διαδικασία εγγρφής βιομετρικών χαρακτηριστικών)

Η διαδικασία της εγγραφής (enrolment) των βιομετρικών χαρακτηριστικών ενός ατόμου στην βάση δεδομένων (System DB) στο σύστημα αναγνώρισης γίνεται και στα δυο είδη αναγνώρισης. Κατά την εγγραφή καταχωρούνται στην βάση δεδομένων του συστήματος. Κατά την διαδικασία της εγγραφής, το βιομετρικό χαρακτηριστικό του ατόμου αποτυπώνεται από κάποιον αισθητήρα βιομετρικών χαρακτηριστικών και μετατρέπεται σε ψηφιακό σήμα. Ακολούθως πραγματοποιείται ένας έλεγχος ποιότητας (Quality checker) με σκοπό να επιβεβαιωθεί ότι το συγκεκριμένο δείγμα του βιομετρικού χαρακτηριστικού μπορεί να επεξεργαστεί επιτυχώς στα επόμενα στάδια επεξεργασίας. Στο επόμενο στάδιο ακολουθεί μια προεπεξεργασία (Preprocessing) με σκοπό την βελτίωση κάποιων χαρακτηριστικών του δείγματος, ώστε να επιτευχθεί η καλύτερη εξαγωγή των χαρακτηριστικών αυτών (Feature Extractor), τα οποία στο στάδιο της σύγκρισης (Matcher) θα χρησιμοποιηθούν για την αναζήτηση από την βάση δεδομένων. Η εξαγωγή κάποιων συγκεκριμένων χαρακτηριστικών γίνεται τόσο για να μειώσει των χρόνο αναζήτησης από την βάση όσο και να αυξήσει την αξιοπιστία της αναζήτηση. Τα χαρακτηριστικά (templates) που παράγονται από το στάδιο εξαγωγής (Feature Extractor) θα χρησιμοποιηθούν για την αναγνώριση, γι’ αυτό αποθηκεύονται σε μια βάση βιομετρικών δεδομένων (System DB) μαζί με το όνομα του ατόμου (Template name) που αντιστοιχούν αυτά τα χαρακτηριστικά.

Στην περίπτωση του συστήματος εξακρίβωσης(Verification) ο χρήστης εισάγει το όνομά του ή ένα μυστικό κωδικό PIN (Personal Identification Number) και ακολούθως εισάγει το βιομετρικό του χαρακτηριστικό. Ο αισθητήρας απόκτησης βιομετρικών χαρακτηριστικών μετατρέπει το βιομετρικό χαρακτηριστικό σε ψηφιακό σήμα και εφόσον προχωρήσει στο επίπεδο ταιριάσματος (Matcher), γίνεται σύγκριση μόνο με τα χαρακτηριστικά (templates) του γνήσιου χρήστη που είναι αποθηκευμένο στην βάση δεδομένων του συστήματος, εφόσον βέβαιο ο κωδικός PIN είναι σωστός.

Στην περίπτωση της ταυτοποίησης (identification) δεν εισάγεται κωδικός ή όνομα και το σύστημα συγκρίνει τα χαρακτηριστικά (Templates) που εξήχθησαν από το βιομετρικό χαρακτηριστικό του χρήστη με όλα τα χαρακτηριστικά όλων των χρηστών (N) που είναι αποθηκευμένα στην βάση του συστήματος. Η έξοδος ενός συστήματος ταυτοποίησης είναι η ταυτότητα του χρήστη με το βιομετρικό χαρακτηριστικό που τοποθετήθηκε στην είσοδο

του συστήματος ή ένα μήνυμα που δηλώνει ότι ο χρήστης δεν βρέθηκε στην βάση δεδομένων (user not identified). Όταν οι βάσης βιομετρικών δεδομένων είναι πολύ μεγάλες χρησιμοποιούνται και τεχνικές ταξινόμησης των βιομετρικών χαρακτηριστικών σε κατηγορίες προκειμένου να ελαχιστοποιηθεί ο χρόνος αναζήτησης και η ανάγκη για μεγάλη υπολογιστική ισχύ του συστήματος αναγνώρισης.

1.2. Βιβλιογραφική επισκόπηση παρόμοιων εφαρμογών

Τα βιομετρικά συστήματα ασφαλείας είναι αυτοματοποιημένες μέθοδοι βασισμένο σε ανθρώπους από τα φυσιολογικά χαρακτηριστικά τους. Τα χαρακτηριστικά γνωρίσματα των βιομετρικών συστημάτων ασφαλείας αποτελούνται από την αναγνώριση προσώπου, τα δακτυλικά αποτυπώματα, τη γεωμετρία χεριών, τη γραφή, την ίριδα, τον αμφιβληστροειδή, την φλέβα και τη φωνή. Η τεχνολογία των βιομετρικών συστημάτων ασφαλείας γίνεται με βάση μιας εκτενούς σειράς ιδιαίτερα ασφαλούς προσδιορισμού και εξακρίβωσης προσωπικών λύσεων. Δεδομένου ότι το επίπεδο παραβιάσεων ασφαλείας και απάτης αυξάνεται, η ανάγκη για τον ιδιαίτερα ασφαλή προσδιορισμό και την επαλήθευση προσωπικών τεχνολογιών γίνεται προφανής. Τα βιομετρικά συστήματα ασφαλείας είναι σε θέση να προβλέψουν την ιδιωτικότητα εμπιστευτικών οικονομικών συναλλαγών και προσωπικών στοιχείων.

Η ανάγκη για τη χρησιμοποίηση των βιομετρικών συστημάτων ασφαλείας μπορεί να βρεθεί στην ομοσπονδία, το κράτος, τις τοπικές κυβερνήσεις, στο στρατό, και στις εμπορικές εφαρμογές. Οι επιχειρησιακές υποδομές ασφάλειας δικτύων, οι ασφαλείς ηλεκτρονικές τραπεζικές εργασίες, η επένδυση και άλλες οικονομικές συναλλαγές, λιανικές πωλήσεις, επιβολή νόμου, υγεία και κοινωνικών υπηρεσιών ωφελούνται ήδη από αυτές τις τεχνολογίες. Περισσότερες πληροφορίες για τα βιομετρικά συστήματα ασφαλείας, τις δραστηριότητες των προτύπων, τις οργανώσεις της κυβέρνησης, της βιομηχανίας και τις ερευνητικές πρωτοβουλίες στη βιομετρική τεχνολογία μπορούν να βρεθούν σε όλο αυτόν τον ιστοχώρο. Η βιομετρία είναι η στατιστική ανάλυση των

βιολογικών παρατηρήσεων και των φαινομένων. Η βιομετρία συνδέεται με τη μέτρηση της βιομετρικής τεχνολογίας: μετρήσιμα, φυσικά χαρακτηριστικά ή προσωπικά χαρακτηριστικά γνωρίσματα που χρησιμοποιούνται για να αναγνωρίσουν την ταυτότητα ή να ελέγξουν την απαιτούμενη ταυτότητα ενός προσώπου. Από το λεξικό η βιομετρία είναι «η επιστήμη που μελετά με τη βοήθεια των μαθηματικών, των στατιστικών, των πιθανοτήτων και την βιολογική παραλλαγή μέσα σε μια καθορισμένη ομάδα» .

Στα πλαίσια της εφαρμοσμένης μηχανικής ασφάλειας υπάρχουν συνήθως δύο συνδέσεις μεταξύ ενός προσώπου και μιας ταυτότητάς:

• Κάτι ξέρω (κωδικοί πρόσβασης)

• Κάτι έχω (σημεία)

Με τη βιομετρία πρέπει - θεωρητικά να είναι δυνατό να εγκατασταθεί μια τρίτη σύνδεση:

• Κάτι είμαι

Επομένως τα βιομετρικά συστήματα μπορούν να διαδραματίσουν έναν σημαντικό ρόλο στην επικύρωση ενός χρήστη. Το Aktronix απαντά εξ' ενός άλλου ορισμού που είναι βασισμένα στα γεγονότα:

Ένα πρόσωπο μπορεί να προσδιοριστεί από:

- Την κατοχή (ταυτότητας, διαβατήριο, άδεια οδήγησης, κ.λπ....)

- Τη γνώση (ενός κωδικού πρόσβασης)

- Τι είναι (η βιομετρία)

Εκείνα τα γεγονότα μας οδηγούν σε έναν καθορισμό:

«η βιομετρία επιτρέπει τον προσδιορισμό των προσώπων από το φυσιολογικό χαρακτηριστικό ή από το χαρακτηριστικό συμπεριφοράς που μπορεί να ανιχνευθεί αυτόματα». Το πρόβλημα με ένα τέτοιο καθορισμό είναι ότι η διαφορά μεταξύ της «βιομετρικής επιστήμης» που έχει πολύ διαφορετικό τρόπο της εφαρμογής και της

«βιομετρικής τεχνολογίας» που χρησιμοποιείται στην αναγνώριση των προσώπων δεν είναι πραγματικά σαφής. Τώρα, στην Ευρώπη, δεν υπάρχει κανένας νομικός καθορισμός αυτό που είναι ακριβώς η «βιομετρία».

Ο αναγνώστης δακτυλικών αποτυπωμάτων είναι το σπουδαιότερο τμήμα σε μια ηλεκτρική κλειδαριά ασφαλείας με αναγνώριση αποτυπωμάτων.

Το T5 είναι ένα σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων και επαγωγικών καρτών RFID. Χρησιμοποιείται ως αναγνώστης δακτυλικών αποτυπωμάτων ως σύστημα ελέγχου πρόσβασης και ωρομέτρησης προσωπικού. Ως σύστημα ελέγχου πρόσβασης, απαιτείται η χρήση του πίνακα ελέγχου πρόσβασης SC011. Ως σύστημα ωρομέτρησης προσωπικού, δεν απαιτείται η χρήση πίνακα ελέγχου πρόσβασης αλλά προτείνεται η χρήση με το professional πρόγραμμα ωρομέτρησης προσωπικού για την επεξεργασία των σχετικών εγγραφών και την έκδοση αναλυτικών αναφορών, καθώς και ο αναγνώστης δακτυλικών αποτυπωμάτων OA99 για την εγγραφή των δακτυλικών αποτυπωμάτων των χρηστών στο σύστημα.

Η αναγνώριση των εγγεγραμμένων χρηστών στο τερματικό T5 επιτυγχάνεται με δακτυλικά αποτυπώματα, με επαγωγική κάρτα RFID ή συνδυασμό των παραπάνω για μεγαλύτερη εγκυρότητα και ασφάλεια. Ο αναγνώστης T5, προσφέρει πολλαπλές δυνατότητες σύνδεσης με Η/Υ, πίνακα ελέγχου πρόσβασης αλλά χρησιμοποιείται και ως βοηθητικός επιπρόσθετος αναγνώστης με άλλα συστήματα ελέγχου πρόσβασης και ρολόγια καταγραφής χρονοπαρουσίας. Το σύστημα T5 είναι μικρών διαστάσεων συσκευή που τοποθετείται ακόμα και στο κάσωμα της πόρτας.

Τα τεχνικά χαρακτηριστικά παρουσιάζονται ακολούθως:

- Ρολόι καταγραφής χρονοπαρουσίας και ελέγχου πρόσβασης
- Αναγνώριση χρηστών με δακτυλικά αποτυπώματα (FP)
- Αναγνώριση χρηστών με επαγωγική κάρτα RFID (RF)
- Αναγνώριση χρηστών με επαγωγική κάρτα Mifare (προαιρετικά)

- Χωρητικότητα 1.000 χρηστών στη μνήμη
- Χωρητικότητα 50.000 εγγραφών στη μνήμη
- Αυτόνομη λειτουργία (Standalone)
- Σύνδεση με Η/Υ μέσω TCP/IP, miniUSB, RS485
- Έξοδος πρωτοκόλλου Wiegand
- Οπτικο-ακουστικά μηνύματα επιβεβαίωσης/απόρριψης
- 16 επεξεργάσιμες ομάδες χρηστών πρόσβασης
- 32 επεξεργάσιμες χρονικές ζώνες πρόσβασης
- Εποπτεία κινήσεων σε πραγματικό χρόνο (Realtime Monitoring)
- Σύνδεση με πίνακα ελέγχου πρόσβασης
- Τροφοδοσία 12V ή μέσω USB
- Τροφοδοσία μέσω δικτύου (απαιτείται συσκευή PoE)
- Επιτοίχια τοποθέτηση ή στο κάσωμα της πόρτας

Εικόνα 1.5(Συσκευή καταγραφής Δακτυλικού Αποτυπώματος)

Εικόνα 1.6(Internal view RFID ATLO-RFM-501)

1.3 Περιγραφή υπόλοιπου πτυχιακής

Στόχος της παρούσας πτυχιακής εργασίας, είναι να σχεδιαστεί και να παρουσιαστεί μια εφαρμογή βάσει της οποίας θα προγραμματιστεί μια πλακέτα Arduino για το αυτόματο κλείδωμα και ξεκλείδωμα με την χρήση δακτυλικού αποτυπώματος.

Για την επίτευξη του στόχου αυτού το υπόλοιπο της παρούσας μελέτης δομείται σε δύο κεφάλαια. Στο επόμενο κεφάλαιο παρουσιάζεται ο γενικός τρόπος λειτουργίας της εφαρμογής που προτείνεται, με διάφορα παραδείγματα, ενώ στην συνέχεια εμφανίζονται τα μέρη που θα αποτελέσουν το σύστημά μας, δηλαδή η πλακέτα Arduino, ο αισθητήρας αποτυπώματος, τα Led, τα ρελέ, η τροφοδοσία, το buzzer, ο σερβοκινητήρας και η οθόνη LCD. Στην συνέχεια παρουσιάζονται πάνω στην πλακέτα οι συνδέσεις – fritzing αλλά και μια εναλλακτική εφαρμογή παρόμοια με αυτή που προτείνεται από την παρούσα πτυχιακή εργασία, με τα αντίστοιχα εξαρτήματα που είναι απαραίτητα για την λειτουργία της. Ακολούθως, παρουσιάζεται το σενάριο λειτουργίας, δηλαδή ο προγραμματισμός που πραγματοποιήθηκε ώστε να λειτουργήσουν όλα τα εξαρτήματα της εφαρμογής με τον σωστό τρόπο. Τέλος, προτείνονται κάποιες μελλοντικές βελτιώσεις ώστε η εφαρμογή στην συνέχεια να γίνει περισσότερο ασφαλής και λειτουργική.

Κεφάλαιο 2 – Το σύστημα

2.1. Γενικός τρόπος λειτουργίας

Η χρήση συστημάτων ελέγχου πρόσβασης (Access Control), κρίνεται απαραίτητη σε εγκαταστάσεις με αυξημένες ανάγκες παρακολούθησης και καταγραφής όλων των εισόδων - εξόδων. Επιτρέπουν την πρόσβαση τόσο σε εξουσιοδοτημένα άτομα, όσο και σε επισκέπτες. Επίσης μπορούν να χρησιμοποιηθούν για την καταγραφή και επεξεργασία των ωρών εργασίας (χρονοπαρουσίας) των υπαλλήλων με χωριστούς αναγνώστες, μέσω κάρτας, μπρελόκ ή νέας τεχνολογίας βιομετρικών συστημάτων (δαχτυλικό αποτύπωμα, ίριδα ματιού κ.α.).

Το σύστημα ελέγχου πρόσβασης, με την τοποθέτηση μηχανισμών στις πόρτες και εφοδιάζοντας τους χρήστες με κάρτες :

- Επιτρέπει την είσοδο στον χρήστη σε εισόδους όπου έχει οριστεί και έχει δικαίωμα να εισέλθει.
- Πραγματοποιεί καταγραφή δεδομένων για την κίνηση εισερχομένων στον επιτηρούμενο χώρο.
- Λειτουργεί και σαν κάρτα ελέγχου για την ώρα άφιξης και αναχώρησης των εργαζομένων.

Στην τυπική του μορφή ένα σύστημα ACCESS CONTROL αποτελείται από:

- Την κεντρική μονάδα ελέγχου με δυνατότητα σύνδεσης σε Η/Υ.
- Τους τοπικούς ελεγκτές (Controllers).
- Τους αναγνώστες (Proximity, Βιομετρικοί , Smart κλπ).
- Το λογισμικό (software) διαχείρισης κινήσεων και διαβάθμισης προσβασιμότητας.
- Κάρτες απλές ή προτυπωμένες (μαγνητικές , proximity κλπ).

Οι βιομετρικοί αναγνώστες είναι συσκευές οι οποίες αναγνωρίζουν και αποθηκεύουν τα μοναδικά δακτυλικά αποτυπώματα του κάθε χρήστη και επιτρέπουν ανάλογα την πρόσβαση του στον χώρο. Η διαφορά χρήσης μεταξύ ενός βιομετρικού αναγνώστη και ενός πληκτρολογίου PIN, είναι ότι διαθέτει έναν υψηλής ποιότητας αισθητήρα ανάγνωσης και μικροεπεξεργαστή ο οποίος συγκρίνει τα αποθηκευμένα ίχνη των δακτυλικών αποτυπωμάτων, με αυτά της σάρωσης. Εάν το αποτύπωμα αναγνωριστεί ανάμεσα στα αποθηκευμένα, τότε ενεργοποιεί την ηλεκτρονική κλειδαριά για να εισέλθει το άτομο αυτό στον χώρο.

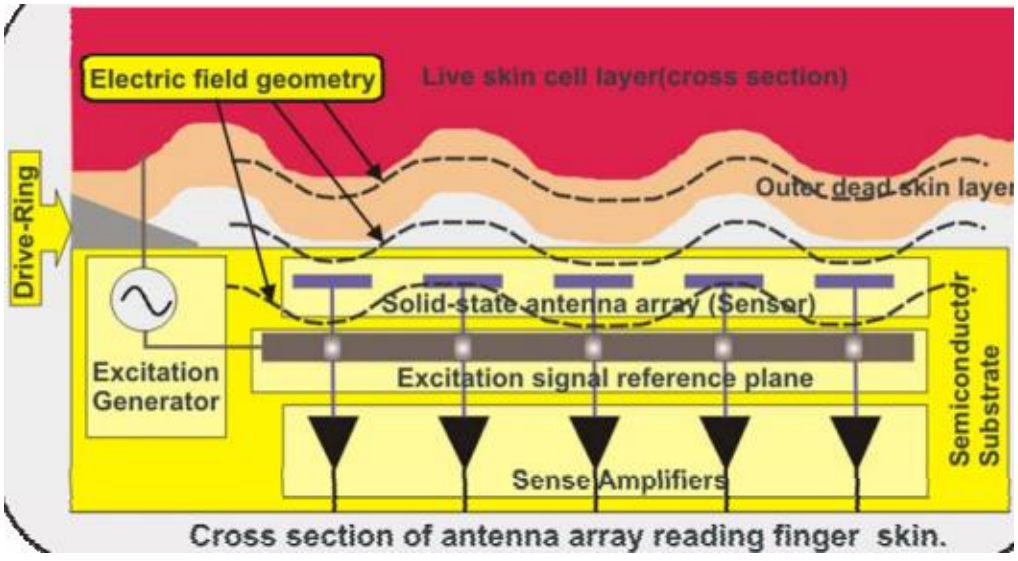
Προτού αναλυθεί το βιομετρικό σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων θα αναφερθούν οι τεχνολογίες των αισθητήρων που χρησιμοποιούνται για την καταγραφή των δακτυλικών αποτυπωμάτων με εκτενή περιγραφή στον αισθητήρα που χρησιμοποιήθηκε στην παρούσα εργασία. Η σημασία του αισθητήρα στο σύστημα αναγνώρισης δακτυλικών αποτυπωμάτων είναι μεγαλύτερη από όλα τα άλλα μέρη του συστήματος. Είναι σημαντικό λοιπόν η ποιότητα της εικόνας του δακτυλικού αποτυπώματος που θα αποκτηθεί από τον αισθητήρα να είναι μεγάλη. Εάν η ποιότητα δεν είναι ικανοποιητική, όσο τέλειος και αποτελεσματικός είναι ο αλγόριθμος επεξεργασίας και αναγνώρισης ολόκληρο το σύστημα θα είναι αναξιόπιστο.

Ακολούθως αναφέρονται κάποιες δημοφιλής τεχνολογίες αισθητήρων δακτυλικών αποτυπωμάτων.

- Πιεζοηλεκτρικοί
- Ηλεκτρικού πεδίου DC
- Οπτικοί
- Ηλεκτρο-οπτικοί
- Θερμικοί
- Υπερήχων

Ο αισθητήρας που χρησιμοποιήθηκε στην παρούσα εργασία χρησιμοποιεί τεχνολογία ημιαγωγών στερεάς κατάστασης και ανήκει στην κατηγορία των αισθητήρων ηλεκτρικού πεδίου RF. Ακολούθως στο παρακάτω σχήμα παρουσιάζεται η αρχή λειτουργία του αισθητήρα. Προτού όμως αναλυθεί η αρχή λειτουργίας του αισθητήρα θα γίνει μια συνοπτική περιγραφή της ανατομίας του δέρματος στην περιοχή του δακτυλικού αποτυπώματος.

Στο παρακάτω σχήμα παρουσιάζεται η εγκάρσια τομή του δέρματος που αποτελείται από το στρώμα των ζωντανών κυττάρων του δέρματος (Live skin cell layer) το οποίο επικαλύπτεται από το στρώμα των νεκρών κυττάρων (Outer dead skin layer) προτού το δέρμα έρθει σε επαφή με το εξωτερικό περιβάλλον. Μετά από μελέτες βρέθηκε ότι το στρώμα των ζωντανών κυττάρων του δέρματος στην περιοχή αυτή έχει μεγάλη ηλεκτρική αγωγιμότητα σε αντίθεση με το στρώμα των νεκρών κυττάρων το οποίο συμπεριφέρεται σαν ημιμονωτής. Στις ηλεκτρικά αγώγιμες αυτές ιδιότητες του δέρματος βασίζεται και η κατασκευή του αισθητήρα. Η ηλεκτρική συμπεριφορά του εξωτερικού στρώματος νεκρών κυττάρων του δέρματος ισοδυναμεί με έναν πυκνωτή ενώ το εσωτερικό στρώμα των ζωντανών κυττάρων ισοδυναμεί με ένα αγωγό.



Εικόνα 2.1(Διατομή της συστοιχίας δέρματος-αισθητήρα)

Ο συγκεκριμένος αισθητήρας διαθέτει μια γεννήτρια διέγερσης εναλλασσόμενης τάσης (Exitation Generation) RF συχνότητας με σκοπό το ρεύμα να διαπεράσει το στρώμα του δέρματος με τα νεκρά κύτταρα που ισοδυναμεί με πυκνωτή με αποτέλεσμα να κλείσει κύκλωμα μεταξύ του στρώματος δέρματος με τα ζωντανά κύτταρα και ενός επιπέδου αναφοράς του RF σήματος (Excitation signal reference plane) και βρίσκεται ακριβώς κάτω από ένα πίνακα από μικροσκοπικές επίπεδες κεραίες (solid state antenna array) ο οποίος βρίσκονται κάτω ακριβώς από την επιφάνεια του αισθητήρα που έρχεται σε επαφή με το δάκτυλο. Η RF συχνότητα επιλέγεται αρκετά χαμηλή ώστε το μήκος κύματος να μην είναι αρκετά μεγαλύτερο από τις διαστάσεις του αισθητήρα με αποτέλεσμα να μην δημιουργείται σημαντικά μεγάλη μαγνητική συνιστώσα που θα επηρέαζε το ημιστατικό πεδίο που δημιουργείται. Επίσης επιλέγεται αρκετά υψηλή ώστε να διαπερνά το στρώμα του δέρματος με τα νεκρά κύτταρα τα οποία έχουν μικρή αγωγιμότητα. Όταν ένα δάκτυλο τοποθετηθεί στην επιφάνεια του αισθητήρα κάνει ηλεκτρική επαφή με τον αισθητήρα μέσο του Drive-Ring και κλείνει κύκλωμα μεταξύ του στρώματος δέρματος με τα ζωντανά κύτταρα (Live skin cell layer) και του επιπέδου αναφοράς (Excitation signal reference plane), με αποτέλεσμα να δημιουργηθεί ένα ημιστατικό επίπεδο ηλεκτρικό πεδίο μεταξύ του στρώματος του ζωντανού δέρματος και του επιπέδου αναφοράς. Ουσιαστικά το στρώμα δέρματος με τα ζωντανά κύτταρα (Live skin cell layer) και το επιπέδου αναφοράς αποτελούν τους οπλισμούς ενός πυκνωτή, ανάμεσα στους οποίους αναπτύσσεται το ημιστατικό επίπεδο ηλεκτρικό πεδίο. Επειδή όμως ο ένας οπλισμός του πυκνωτή είναι το στρώματος του δέρματος με τα ζωντανά κύτταρα (Live skin cell layer) και το σχήμα του έχει το σχήμα τον παρυφών και των κοιλάδων του δακτυλικού αποτυπώματος, αναπτύσσεται ένα ημιστατικό ηλεκτρικό επίπεδο πεδίο το οποίο ακολουθεί την μορφή των παρυφών και των κοιλάδων ακριβώς όπως φαίνεται στο παραπάνω σχήμα.

Η μαύρες γραμμές ,οι οποίες ακολουθούν την μορφή των παρυφών και των κοιλάδων, στο σχήμα δείχνουν την γεωμετρία του πεδίου (Electric field geometry) , όπου σε κάθε μαύρη γραμμή η ένταση του πεδίου είναι ίδια. Ο πίνακα από τις μικροσκοπικές επίπεδες κεραίες (solid state antenna array) βρίσκεται μέσα στο πεδίο και καταγράφει την ένταση του πεδίου σε κάθε σημείο του επιπέδου των κεραιών. Κάθε επίπεδη κεραία από τον πίνακα κεραιών καταγράφει την ένταση του πεδίου σε εκείνο το σημείο, η οποία είναι ανάλογη με την απόσταση της επίπεδης κεραίας από την επιφάνεια του δέρματος. Η απόσταση αυτή

αντιστοιχείται σε ένα τόνο του γκρι. Δηλαδή κάθε κεραία μπορεί να αντιστοιχήσει σε ένα εικονοστοιχείο και ανάλογα με την απόστασή της από την επιφάνεια του δέρματος να δώσει έναν τόνο του γκρι. Το σήμα από κάθε κεραία διαβάζεται μέσω ενός ενισχυτή το οποίο στην συνέχεια συνθέτει την ψηφιακή εικόνα του δακτυλικού αποτυπώματος.

Ένα σημαντικό πλεονέκτημα της παραπάνω τεχνολογίας είναι η ικανότητα συλλογής των δακτυλικών αποτυπωμάτων ανεξαρτήτως τις μολύνσεις από σκόνη, λάδι ή άλλα υλικά τις οποίες μπορεί να έχει το δακτυλικό αποτύπωμα την ώρα της συλλογής του, διότι η μέτρηση γίνεται κατευθείαν στο εσωτερικό στρώμα του δέρματος, των ζωντανών κυττάρων τα οποία δεν αλλοιώνονται. Το πλεονέκτημα δεν υπάρχει σε καμία άλλη τεχνολογία συλλογής δακτυλικών αποτυπωμάτων.

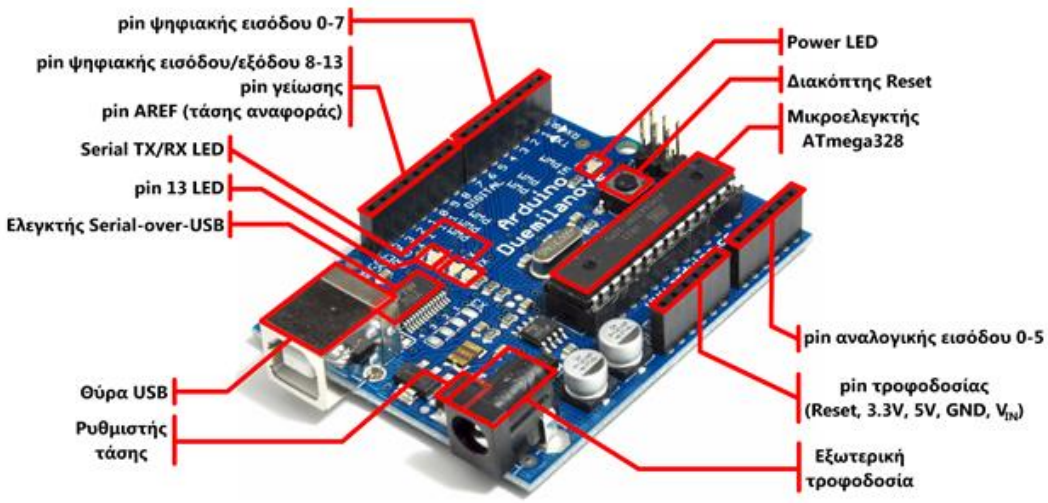
2.2. Μέρη που το αποτελούν

2.2.1. Arduino

Το Arduino είναι μια μικρή συσκευή (μικροεπεξεργαστής) που συνδέεται με USB στον υπολογιστή. Με το Arduino καλλιτέχνες, σχεδιαστές, αρχιτέκτονες, χομπίστες, μαθητές και φοιτητές μαθαίνουν προγραμματισμό και κατασκευάζουν ολόκληρα έργα για αυτοματισμούς και εφαρμογές ρομποτικής. Έτσι ειδικά τα παιδιά που ξεκινούν προγραμματισμό μαθαίνουν να αναβοσβήνουν Led σε γλώσσα Wiring που μοιάζει με c/c++ χάρη στο Arduino. Η πλακέτα του Arduino αποτελείται από έναν μικρό επεξεργαστή ανοικτού κώδικα στον οποίο μπορεί κανείς να προγραμματίσει ακόμη κι αν είναι αρχάριος μέσω του δικού του δωρεάν προγράμματος (IDE: Integrated Development Environment) που τρέχει σε Windows, Linux και MAC OS X. Στο Arduino συνδέονται Led, ροοστάτες, θύρα ethernet για να γίνει webserver και επικοινωνία μέσω bluetooth. Επειδή λογισμικό και υλικό είναι δεμένα, ευέλικτα και δοκιμασμένα, με το Arduino κατασκευάζονται εφαρμογές, οι οποίες αλληλεπιδρούν μεταξύ υπολογιστών-χρηστών-περιβάλλοντος.

Το Arduino βασίζεται στον ATmega328, έναν 8-bit RISC μικροελεγκτή, τον οποίο χρονίζει στα 16MHz. Ο ATmega328 διαθέτει ενσωματωμένη μνήμη 32Kb μνήμης Flash, από τα οποία τα 2Kb χρησιμοποιούνται από το firmware του Arduino που έχει εγκαταστήσει ήδη ο κατασκευαστής του. Το firmware αυτό που στην ορολογία του Arduino ονομάζεται bootloader είναι αναγκαίο για την εγκατάσταση των δικών προγραμμάτων στον μικροελεγκτή μέσω της θύρας USB, χωρίς δηλαδή να χρειάζεται εξωτερικός hardware programmer. Τα υπόλοιπα 30Kb της μνήμης Flash χρησιμοποιούνται για την αποθήκευση αυτών ακριβώς των προγραμμάτων, αφού πρώτα μεταγλωττιστούν στον υπολογιστή. Η μνήμη Flash, όπως και η EEPROM δεν χάνει τα περιεχόμενά της με απώλεια τροφοδοσίας ή reset. Επίσης, ενώ η μνήμη Flash υπό κανονικές συνθήκες δεν προορίζεται για χρήση runtime μέσα από τα προγράμματά , λόγω της μικρής συνολικής μνήμης που είναι διαθέσιμη σε αυτά (2Kb SRAM + 1Kb EEPROM), έχει σχεδιαστεί μια βιβλιοθήκη που επιτρέπει την χρήση όσου χώρου περισσεύει (30Kb μείον το μέγεθος του προγράμματός σε μεταγλωττισμένη μορφή).

Καταρχήν το Arduino διαθέτει σειριακό interface. Ο μικροελεγκτής ATmega υποστηρίζει σειριακή επικοινωνία, την οποία το Arduino προωθεί μέσα από έναν ελεγκτή Serial-over-USB ώστε να συνδέεται με τον υπολογιστή μέσω USB. Η σύνδεση αυτή χρησιμοποιείται για την μεταφορά των προγραμμάτων που σχεδιάζονται από τον υπολογιστή στο Arduino αλλά και για αμφίδρομη επικοινωνία του Arduino με τον υπολογιστή μέσα από το πρόγραμμα την ώρα που εκτελείται.



Εικόνα 2.2(Arduino, Είσοδοι – Έξοδοι)

Επιπλέον, στην πάνω πλευρά του Arduino βρίσκονται 14 θηλυκά pin, αριθμημένα από 0 ως 13, που μπορούν να λειτουργήσουν ως ψηφιακές είσοδοι και έξοδοι. Λειτουργούν στα 5V και καθένα μπορεί να παρέχει ή να δεχτεί το πολύ 40mA.

Ως ψηφιακή έξοδος, ένα από αυτά τα pin μπορεί να τεθεί από το πρόγραμμά σε κατάσταση HIGH ή LOW, οπότε το Arduino θα ξέρει αν πρέπει να διοχετεύσει ή όχι ρεύμα στο συγκεκριμένο pin. Με αυτόν τον τρόπο μπορούμε λόγου χάρη να ανάψουμε και να σβήσουμε ένα LED που έχουμε συνδέσει στο συγκεκριμένο pin. Αν πάλι ρυθμίσουμε ένα από αυτά τα pin ως ψηφιακή είσοδο μέσα από το πρόγραμμά , μπορούμε με την κατάλληλη εντολή να διαβάσουμε την κατάστασή του (HIGH ή LOW) ανάλογα με το αν η εξωτερική συσκευή που έχουμε συνδέσει σε αυτό το pin διοχουμεύει ή όχι ρεύμα στο pin (με αυτόν τον τρόπο λόγου χάρη μπορούμε να «διαβάζουμε» την κατάσταση ενός διακόπτη).

Τα pin 0 και 1 λειτουργούν ως RX και TX της σειριακής όταν το πρόγραμμά ενεργοποιεί την σειριακή θύρα. Έτσι, όταν λόγου χάρη το πρόγραμμά στέλνει δεδομένα στην σειριακή, αυτά προωθούνται και στην θύρα USB μέσω του ελεγκτή Serial-Over-USB αλλά και στο pin 0 για να τα διαβάσει ενδεχομένως μια άλλη συσκευή (π.χ. ένα δεύτερο Arduino στο

δικό του pin 1). Αυτό φυσικά σημαίνει ότι αν στο πρόγραμμά ενεργοποιήσουμε το σειριακό interface, χάνουμε 2 ψηφιακές εισόδους/εξόδους.

Τα pin 2 και 3 λειτουργούν και ως εξωτερικά interrupt (interrupt 0 και 1 αντίστοιχα). Με άλλα λόγια, μπορούμε να τα ρυθμίσουμε μέσα από το πρόγραμμά ώστε να λειτουργούν αποκλειστικά ως ψηφιακές είσοδοι στις οποίες όταν συμβαίνουν συγκεκριμένες αλλαγές, η κανονική ροή του προγράμματος σταματάει *άμεσα* και εκτελείται μια συγκεκριμένη συνάρτηση. Τα εξωτερικά interrupt είναι ιδιαίτερα χρήσιμα σε εφαρμογές που απαιτούν συγχρονισμό μεγάλης ακρίβειας.

Τα pin 3, 5, 6, 9, 10 και 11 μπορούν να λειτουργήσουν και ως ψευδοαναλογικές έξοδοι με το σύστημα PWM (Pulse Width Modulation), δηλαδή το ίδιο σύστημα που διαθέτουν οι μητρικές των υπολογιστών για να ελέγχουν τις ταχύτητες των ανεμιστήρων. Έτσι, μπορούμε να συνδέσουμε λόγου χάρη ένα LED σε κάποιο από αυτά τα pin και να ελέγξουμε πλήρως την φωτεινότητά του με ανάλυση 8bit (256 καταστάσεις από 0-σβηστό ως 255-πλήρως αναμμένο) αντί να έχουμε απλά την δυνατότητα αναμμένο-σβηστό που παρέχουν οι υπόλοιπές ψηφιακές έξοδοι. Είναι σημαντικό να καταλάβουμε ότι το PWM δεν είναι πραγματικά αναλογικό σύστημα και ότι θέτοντας στην έξοδο την τιμή 127, δεν σημαίνει ότι η έξοδος θα δίνει 2.5V αντί της κανονικής τιμής των 5V, αλλά ότι θα δίνει ένα παλμό που θα εναλλάσσεται με μεγάλη συχνότητα και για ίσους χρόνους μεταξύ των τιμών 0 και 5V.

Στην κάτω πλευρά του Arduino, με τη σήμανση ANALOG IN, θα βρούμε μια ακόμη σειρά από 6 pin, αριθμημένα από το 0 ως το 5. Το καθένα από αυτά λειτουργεί ως αναλογική είσοδος κάνοντας χρήση του ADC (Analog to Digital Converter) που είναι ενσωματωμένο στον μικροελεγκτή. Για παράδειγμα, μπορούμε να τροφοδοτήσουμε ένα από αυτά με μια τάση την οποία μπορούμε να κυμάνουμε με ένα ποτενσιόμετρο από 0V ως μια τάση αναφοράς Vref η οποία, αν δεν κάνουμε κάποια αλλαγή είναι προρυθμισμένη στα 5V. Τότε, μέσα από το πρόγραμμά μπορούμε να «διαβάσουμε» την τιμή του pin ως ένα ακέραιο αριθμό ανάλυσης 10-bit, από 0 (όταν η τάση στο pin είναι 0V) μέχρι 1023 (όταν η τάση στο pin είναι 5V). Η τάση αναφοράς μπορεί να ρυθμιστεί με μια εντολή στο 1.1V, ή σε όποια τάση επιθυμούμε (μεταξύ 2 και 5V) τροφοδοτώντας εξωτερικά με αυτή την τάση

το pin με την σήμανση AREF που βρίσκεται στην απέναντι πλευρά της πλακέτας. Έτσι, αν τροφοδοτήσουμε το pin AREF με 3.3V και στην συνέχεια δοκιμάσουμε να διαβάσουμε κάποιο pin αναλογικής εισόδου στο οποίο εφαρμόζουμε τάση 1.65V, το Arduino θα επιστρέψει την τιμή 512.

Τέλος, καθένα από τα 6 αυτά pin, με κατάλληλη εντολή μέσα από το πρόγραμμα μπορεί να μετατραπεί σε ψηφιακό pin εισόδου/εξόδου όπως τα 14 που βρίσκονται στην απέναντι πλευρά και τα οποία περιγράφηκαν πριν. Σε αυτή την περίπτωση τα pin μετονομάζονται από 0~5 σε 14~19 αντίστοιχα.

2.2.2. Αισθητήρας αποτυπώματος AFS8600

Η ανάγκη για την γρήγορη μεταφορά των εικόνων δακτυλικών αποτυπωμάτων (Δίκτυα αισθητήρων), την εξοικονόμηση χώρου αποθήκευσης (Χρήση ενσωματωμένων συστημάτων για την υλοποίηση αλγορίθμων επεξεργασίας και αναγνώρισης δακτυλικών αποτυπωμάτων, με μικρό αποθηκευτικό χώρο) και την βέλτιστη προεπεξεργασία των εικόνων για την πιο αξιόπιστη εξαγωγή χαρακτηριστικών από αυτές, οδήγησαν στην δημιουργία τύπων εικόνας (formats) δακτυλικών αποτυπωμάτων οι οποίες έχουν συμπιεστεί κατάλληλα με ταυτόχρονη βελτιστοποίηση των χαρακτηριστικών που θα χρησιμοποιηθούν στην αναγνώριση. Η κάρτα δακτυλικών αποτυπωμάτων AFS8600 χρησιμοποιεί αυτό τον βέλτιστο τύπο εικόνων. Συγκεκριμένα η βελτιστοποιημένη εικόνα που λαμβάνουμε από την κάρτα χρησιμοποιεί 3 bits κωδικοποίησης από τα οποία προκύπτουν τα εξής 8 επίπεδα τόνων του γκρι τα οποία έχουν κρατήσει την πληροφορία που χρειάζεται για να γίνει η βέλτιστη εξαγωγή των χαρακτηριστικών.

Η κωδικοποίηση μαζί με την προεπεξεργασία για την εξαγωγή των 8 επιπέδων του γκρί υλοποιείται από μικροεπεξεργαστή που είναι ενσωματωμένος στην κάρτα AFS8600. Σύμφωνα με της προδιαγραφές αυτού του τύπου εικόνας η προεπεξεργασία αυτή για την

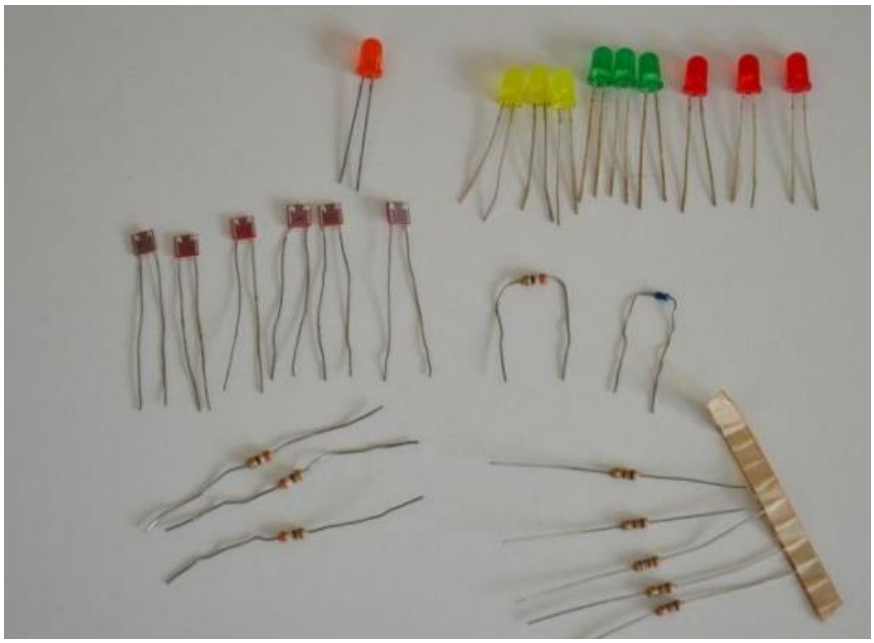
τόνωση(βελτιστοποίηση) των παρυφών και των κοιλάδων του δακτυλικού αποτυπώματος είναι ικανή ώστε στην εικόνα να υλοποιηθούν απευθείας αλγόριθμοι εξαγωγής χαρακτηριστικών.

Εικόνα 2.3(Αισθητήρας αποτυπώματος)

2.2.3. Led

Πάνω στην πλακέτα του Arduino υπάρχει ένας διακόπτης micro-switch και 4 μικροσκοπικά LED επιφανειακής στήριξης. Η λειτουργία του διακόπτη (που έχει την σήμανση RESET) και του ενός LED με την σήμανση POWER είναι μάλλον προφανής.

Τα δύο LED με τις σημάνσεις TX και RX, χρησιμοποιούνται ως ένδειξη λειτουργίας του σειριακού interface, καθώς ανάβουν όταν το Arduino στέλνει ή λαμβάνει (αντίστοιχα) δεδομένα μέσω USB. Τα LED αυτά ελέγχονται από τον ελεγκτή Serial-over-USB και συνεπώς δεν λειτουργούν όταν η σειριακή επικοινωνία γίνεται αποκλειστικά μέσω των ψηφιακών pin 0 και 1.

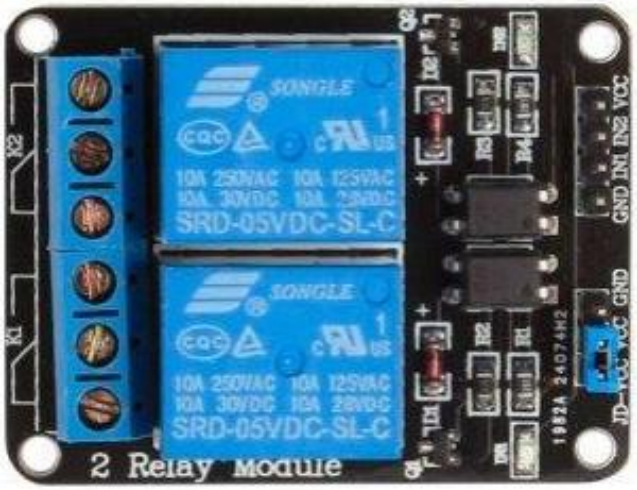


Εικόνα 2.4(Εξαρτήματα (pins και LED))

Τέλος, υπάρχει το LED με την σήμανση L. Η βασική δοκιμή λειτουργίας του Arduino είναι να του αναθέσουμε να αναβοσβήνει ένα LED (θα το δούμε αυτό στην συνέχεια όταν θα φτιάξουμε την πρώτη εφαρμογή). Οι κατασκευαστές του σκέφτηκαν να ενσωματώσουν ένα LED στην πλακέτα, το οποίο σύνδεσαν στο ψηφιακό pin 13. Έτσι, ακόμα και αν δεν έχει κανείς συνδέσει τίποτα πάνω στο φυσικό pin 13, αναθέτοντάς του την τιμή HIGH μέσα από το πρόγραμμά , θα ανάψει αυτό το ενσωματωμένο LED. Χρησιμοποιήθηκαν 2 Led, καθένα από τα οποία συνδέεται με μια αντίσταση των 220Ω σε σειρά. Η σύνδεση φαίνεται παρακάτω.

2.2.4. DC ρελέ

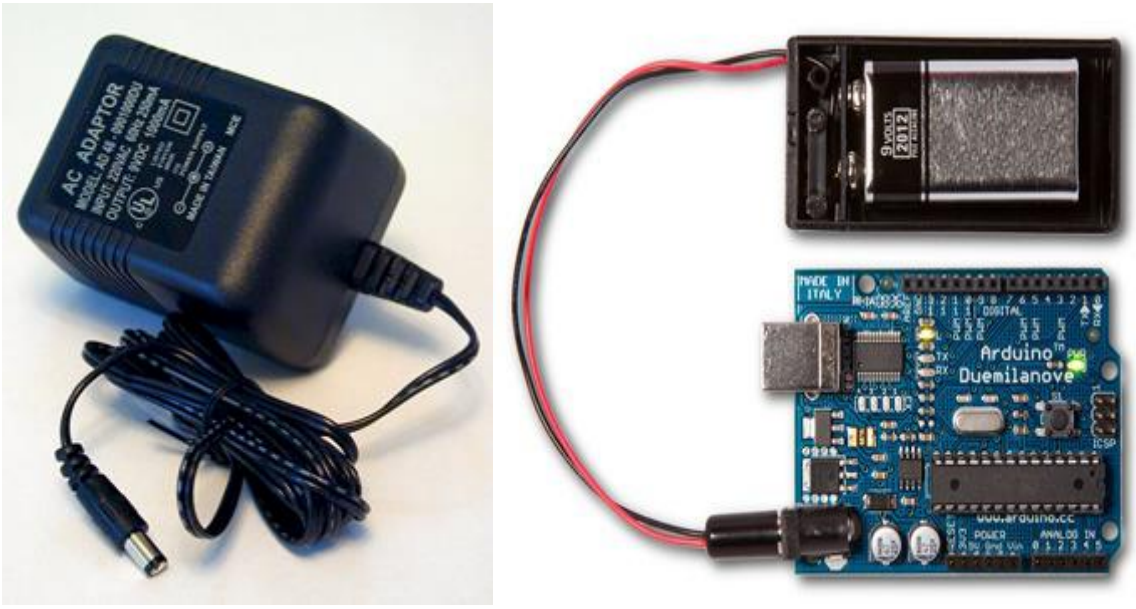
Για την συγκεκριμένη εφαρμογή με διέγερση 5V DC επιλέχθηκε έτοιμο 2 Relay Module όπως εμφανίζεται στην παρακάτω εικόνα και όχι ένας απλός DC ρελές για καλύτερη προστασία του μικροελεγκτή Arduino.



Εικόνα 2.5(Relay-Ρελέ)

2.2.5. Τροφοδοσία

Το Arduino μπορεί να τροφοδοτηθεί με ρεύμα από τον υπολογιστή μέσω της σύνδεσης USB, ή από εξωτερική τροφοδοσία που παρέχεται μέσω μιας υποδοχής φις των 2.1mm (θετικός πόλος στο κέντρο) και βρίσκεται στην κάτω-αριστερή γωνία του Arduino.



Εικόνα 2.6(Τροφοδοσία Arduino)

Για να μην υπάρχουν προβλήματα, η εξωτερική τροφοδοσία πρέπει να είναι από 7 ως 12V και μπορεί να προέρχεται από ένα κοινό μετασχηματιστή του εμπορίου, από μπαταρίες ή οποιαδήποτε άλλη πηγή DC. Δίπλα από τα pin αναλογικής εισόδου, υπάρχει μια ακόμα συστοιχία από 6 pin με την σήμανση POWER. Η λειτουργία του καθενός έχει ως εξής:

- Το πρώτο, με την ένδειξη RESET, όταν γειωθεί (σε οποιοδήποτε από τα 3 pin με την ένδειξη GND που υπάρχουν στο Arduino) έχει ως αποτέλεσμα την επανεκκίνηση του Arduino.

- Το δεύτερο, με την ένδειξη 3.3V, μπορεί να τροφοδοτήσει τα εξαρτήματά με τάση 3.3V. Η τάση αυτή δεν προέρχεται από την εξωτερική τροφοδοσία αλλά παράγεται από τον ελεγκτή Serial-over-USB και έτσι η μέγιστη ένταση που μπορεί να παρέχει είναι μόλις 50mA.

- Το τρίτο, με την ένδειξη 5V, μπορεί να τροφοδοτήσει τα εξαρτήματά με τάση 5V. Ανάλογα με τον τρόπο τροφοδοσίας του ίδιου του Arduino, η τάση αυτή προέρχεται άμεσα από την θύρα USB (που ούτως ή άλλως λειτουργεί στα 5V), από την εξωτερική τροφοδοσία αφού αυτή περάσει από ένα ρυθμιστή τάσης για να την «φέρει» στα 5V.

- Το τέταρτο και το πέμπτο pin, με την ένδειξη GND, είναι φυσικά γειώσεις.

- Το έκτο και τελευταίο pin, με την ένδειξη Vin έχει διπλό ρόλο. Σε συνδυασμό με το pin γείωσης δίπλα του, μπορεί να λειτουργήσει ως μέθοδος εξωτερικής τροφοδοσίας του Arduino, στην περίπτωση που δεν βολεύει να χρησιμοποιήσουμε την υποδοχή του φις των 2.1mm. Αν όμως έχουμε ήδη συνδεδεμένη εξωτερική τροφοδοσία μέσω του φις, μπορούμε να χρησιμοποιήσουμε αυτό το pin για να τροφοδοτήσουμε εξαρτήματα με την πλήρη τάση της εξωτερικής τροφοδοσίας (7~12V), πριν αυτή περάσει από τον ρυθμιστή τάσης όπως γίνεται με το pin των 5V.

2.2.6. Buzzer

Χρησιμοποιήθηκε για τις ανάγκες της πτυχιακής εργασίας ένα buzzer το οποίο προγραμματίστηκε κατάλληλα ώστε να βγάζει ήχο σε κάθε πέρασμα του δακτύλου, είτε είναι επιτυχής η πρόσβαση είτε όχι. Ο προγραμματισμός έγινε μέσω της γλώσσας wiring και για την αναπαραγωγή του ήχου και τονισμού του επιλέχτηκαν κατάλληλες νότες ώστε να γίνεται διακριτός ο ήχος του σωστού ή λάθος αποτυπώματος, δηλαδή ποιος θα έχει πρόσβαση και ποιος όχι.

Εικόνα 2.7(Buzzer)

2.2.7. Σερβοκινητήρας

Χρησιμοποιήθηκε ένα Μοτέρ της TowerPro Micro Servo sg 5010 mini για την προσομοίωση της επιτυχής πρόσβασης του χρήστη με συνέπεια την περιστροφή του μοτέρ και το υποτιθέμενο άνοιγμα της κλειδαριάς που δίνει πρόσβαση στην εταιρία. Σε περίπτωση που ο χρήστης δεν αναγνωριστεί επιτυχώς, το μοτέρ δεν περιστρέφεται και δεν υπάρχει πρόσβαση.

Εικόνα 2.8(Μοτέρ (servo))

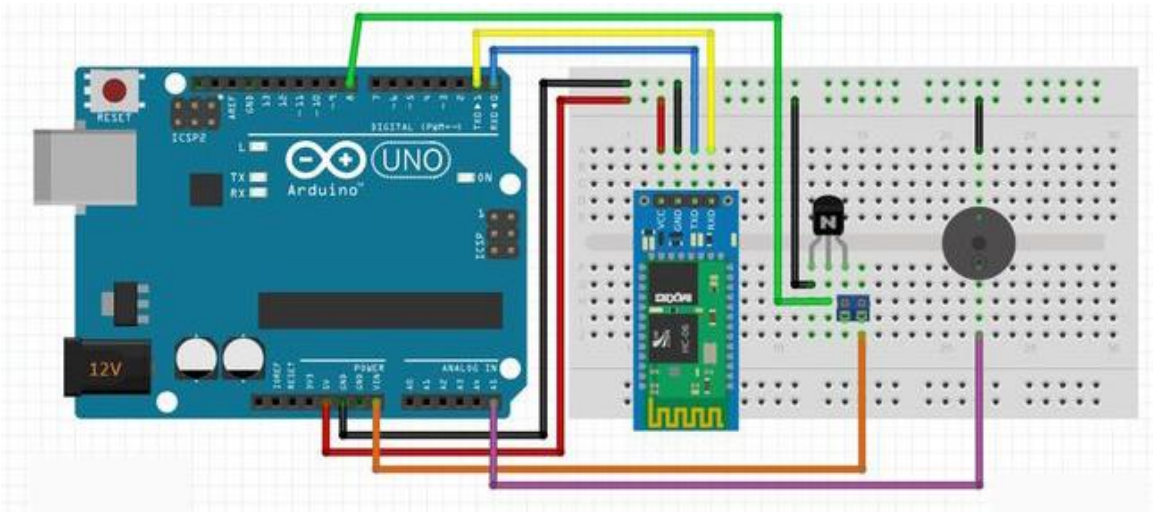
2.2.8. Οθόνη LCD

Για την ένδειξη των μηνυμάτων όπως το όνομα αυτού που εισέρχεται και ενδείξεις όπως καλωσορίσατε ή απαγορεύετε η είσοδος άλλα και για την πιο ρεαλιστική απεικόνιση του συστήματος χρησιμοποιήθηκε μια οθόνη 16x2.

Εικόνα 2.9(Οθόνη LCD 16x2)

2.3. Συνδέσεις Fritz

Παρακάτω παρουσιάζονται οι συνδέσεις (fritzing) στο κύκλωμα σχηματικά.



Εικόνα 2.10(Συνδέσεις Fritz)

Οι συνδέσεις είναι αρκετά εύκολες, ακολουθώντας το παραπάνω σχηματικό σε breadboard:

BT HC-06:

Vcc - 5V

GNG - GND

RX -TX

TX -RX

NPN Transistor:

Το pin B Βάσης στο pin 9 του Arduino

Το pin C Συλλέκτης στο 1ο pin του ακροδέκτη

Ο πομπός Ε στο GND

Το 2ο pin του ακροδέκτη θα συνδεθεί με το Arduino pin “Vin” και θα δώσει ισχύ στο ηλεκτρικό άνοιγμα της πόρτας μας (9V σε 12V).

2.4. Εναλλακτικά εξαρτήματα – εναλλακτική εφαρμογή

Μια εναλλακτική θα ήταν η εφαρμογή να πραγματοποιείται μέσω Android συστήματος. Το κύκλωμα αυτό είναι βασισμένο στο Arduino uno χρησιμοποιώντας τον μικρο ελεγκτή του, ATmega328p. Χρησιμοποιώντας αυτό το σύστημα θα είμαστε σε θέση να ξεκλειδώσουμε απ' το Android κινητό τηλέφωνο (ή tablet) την κλειδαριά σε 3 δευτερόλεπτα. Μετά τα 3 δευτερόλεπτα η κλειδαριά κλειδώνει αυτόματα. Για να την ξεκλειδώσουμε το μόνο που έχετε να κάνουμε είναι να πατήσετε ένα κουμπί απ' την Android εφαρμογή. Διαθέτει επίσης και buzzer για την αναπαραγωγή ήχου κατά την διάρκεια που η πόρτα παραμένει ανοικτή.

Τα εξαρτήματα για αυτή την εναλλακτική εφαρμογή είναι τα ακόλουθα:

- Arduino uno board
- Bluetooth module HC-06
- NPN transistor NP2222A
- 2 pin screw driver circuit
- Ηλεκτρονική κλειδαριά (12V)
- Τροφοδοτικό από 9 μέχρι 12V (max!)
- 10k αντίσταση
- Buzzer

Μόνο στην περίπτωση που θέλουμε να φτιάξουμε το δικό μας κύκλωμα θα χρειαστούμε επίσης:

- Βάση για τον atmega328
- LM7805 Voltage regulator (5V output)
- 16Mhz crystal osc
- 2x 22pF ceramic, 2x 0.22uF electrolytic πυκνωτές
- 1x 10K αντίσταση
- DC power jack
- διάτρητη πλακέτα κατασκευής κυκλωμάτων

2.5. Σενάριο λειτουργίας

Η πλακέτα στην οποία βασιστήκαμε είναι το Arduino για το οποίο χρειαστήκαμε και την Ethernet Shield του. Σε περίπτωση που το Arduino πρέπει να τοποθετηθεί σε σημείο μακριά από το router (και δεν θέλουμε να τραβάμε καλώδιο ethernet) τότε χρησιμοποιούμε ένα A/P το οποίο ρυθμίζουμε σε Client Mode.

Λοιπά πράγματα που χρησιμοποιήσαμε: breadboard, jumper wires, photocells, αντιστάσεις, μονωτική, πολύμετρο, κατσαβίδια κτλ.

Στην πιο απλή μορφή του Project, (όπου απλά ελέγχουμε 4 συσκευές/φωτιστικά από το Android), θα μας κοστίσει 23.37 (Arduino)+ 35.60 (Ethernet Shield)+ 37.72 (4x9.43) (relays)+ 10 (λοιπά, καλώδια, μονωτική ταινία κτλ)=106.69 ευρώ.

Όλη η διαδικασία είναι χωρισμένη σε επιμέρους τμήματα, αφενός για να είναι πιο εύκολο να στηθεί η τελική πλατφόρμα και αφετέρου για να είναι ευκολότερη η διαχείριση. Έτσι λοιπόν το πρώτο στάδιο είναι να γίνουν οι απαραίτητες ενέργειες όσον αφορά το hardware για να συνδεθεί ο ελεγκτής με τον αισθητήρα θερμότητας και ακολούθως να συγγραφεί ο απαραίτητος κώδικας για την καταγραφή θερμότητας στο χώρο που έχει εγκατασταθεί ο αισθητήρας.

Το τελευταίο βήμα που απομένει για τον ελεγκτή είναι να επικοινωνεί με το router ώστε να είναι εφικτή η διαχείριση των δυνατοτήτων που έχουν εγκατασταθεί μέσω της εφαρμογής που θα αναπτυχθεί.. Έτσι λοιπόν, επιτρέπεται να δημιουργήσουμε ένα HTTP server μέσω ενός shield που παρέχει η κατασκευάστρια εταιρεία, στο οποίο θα παρέχονται οι πληροφορίες από τους αισθητήρες. Συνδέεται το Arduino στον δρομολογητή με καλώδιοEthernet, στήνεται ο WebServer, και προγραμματίζεται το Arduino να δείχνει την ένδειξη από τον αισθητήρα θερμότητας. Πλέον, ανοίγοντας έναν οποιονδήποτε περιηγητή είναι εφικτή η πρόσβαση στην IP διεύθυνση που ορίστηκε στο Arduino, για να ελεγχθεί η ένδειξη της θερμοκρασίας. Το Arduino με την Ethernet shield πρέπει να συνδεθεί στο router του σπιτιού με καλώδιο Ethernet. Στην περίπτωση όμως που κάτι τέτοιο δεν είναι επιθυμητό, υπάρχει η δυνατότητα να χρησιμοποιηθεί ένα A/P σε client mode, ώστε το Arduino να αποκτήσει πρόσβαση στο δίκτυο από "απόσταση". Φυσικά πριν συνδεθεί ασύρματα το A/P σε client mode πρέπει να ληφθούν μέτρα για την ασφάλεια του ασύρματου δικτύου, καθώς δεν είναι επιθυμητό ο καθένας να έχει πρόσβαση στο αναπτυχθέν σύστημα.

Το Arduino τροφοδοτείται από την θύρα USB του υπολογιστή κατά τη διάρκεια του προγραμματισμού του. Η χρήση του όμως (αφού προγραμματιστεί) θα πρέπει να είναι ανεξάρτητη από τον υπολογιστή. Συνεπώς πρέπει να πραγματοποιηθεί η τροφοδοσία του με διαφορετικό τρόπο. Η μία επιλογή είναι να χρησιμοποιηθεί η κλασσική διεπαφή που υπάρχει σχεδόν σε όλα τα κινητά, η οποία δίνει σύνδεση USB female. Εναλλακτικά μπορεί να χρησιμοποιηθεί τροφοδοτικό DC 12V, με βύσμα 2.1mm. Όποια και από τις δύο εναλλακτικές και αν επιλεγεί, θα πρέπει να είναι ικανή να δώσει ρεύμα τουλάχιστον

500mA έως 1A, καθότι στην συνέχεια πρέπει να τροφοδοτηθούν διάφορα ηλεκτρονικά κυκλώματα από το Arduino.

Εικόνα 2.11(Τροφοδοτικά)

Η σύνδεση των relay με τις συσκευές που κάνουν χρήση 220V AC είναι μια απλή συνδεσμολογία αλλά απαιτεί μεγάλη προσοχή δεδομένου ότι μια λανθασμένη σύνδεση μπορεί να προκαλέσει τραυματισμό ή να δημιουργήσει πυρκαγιά από κάποιο βραχυκύκλωμα. Το relayσυνδέεται με τρία καλώδια στο Arduino. Το μαύρο καλώδιο συνδέεται στο PIN GND, το πράσινο στο PIN τροφοδοσίας +5V, ενώ το κόκκινο στο PIN 6 το οποίο θα λειτουργεί ως trigger. Όταν ορίζεται η κατάσταση του PIN6 ως "HIGH", το οποίο δίνει +5V, το relay κλείνει το κύκλωμα, άρα αρχίζει να λειτουργεί η συσκευή. Αντιθέτως ορίζοντας την κατάστασή του ως "LOW", το relay ανοίγει το κύκλωμα και η συσκευή απενεργοποιείται.

Για να συνδεθεί μια συσκευή που διαθέτει διακόπτη ακολουθείται η εξής διαδικασία:

- Αρχικά αποσυνδέεται η συσκευή από την τροφοδοσία.

- Στην συνέχεια ανοίγεται η θήκη του διακόπτη και αφαιρείται ο μηχανισμός.

- Έπειτα για συγκεκριμένη τοποθέτηση του φις, εντοπίζεται το καλώδιο φάσης και το neutral.

• Ακολούθως πρέπει να "παρακαμφθεί" το καλώδιο φάσης, το οποίο συνδέεται στο relay. Το καλώδιο που "έρχεται" από την πρίζα, συνδέεται στο "NO", ενώ αυτό που πηγαίνει στην συσκευή συνδέεται στο COM.

Η εγγραφή του κώδικα στο σύστημα γεφυρώνει την επικοινωνία μεταξύ του υπολογιστικού συστήματος (μέσω του λογισμικού(software), όπου στην συγκεκριμένη πτυχιακή εργασία χρησιμοποιείται η έκδοση Arduino – 1.0.5), και του υλικού(hardware), που αποτελείται από την αναπτυξιακή πλακέτα του Arduino Uno και τα περιφερειακά του. Όλοι οι τύποι των μεταβλητών που χρησιμοποιώ στο πρόγραμμα υποστηρίζονται από την παραπάνω έκδοση.

Η γλώσσα στην οποία προγραμματίστηκε το σύστημα ασφαλείας είναι η γλώσσα Wiring, μια παραλλαγή της C,C++ όπως αναφέρθηκε και στο κεφάλαιο 2. Στο πρόγραμμα χρησιμοποιούνται κάποιες βιβλιοθήκες – συναρτήσεις οι οποίες χρειάζονται για την αρχικοποίηση του κώδικα που σαν έξοδο θα έχει την σωστή τονική λειτουργία στο buzzer και επίσης την σωστή λειτουργία της οθόνης του σερβοκινητήρα. Η τονική λειτουργία του buzzer φαίνεται στο αρχείο Pitches.h που περιλαμβάνει όλες τις αρχικοποιήσεις για τις νότες που υποστηρίζει η γλώσσα wiring.Το συγκεκριμένο αρχείο κεφαλίδας ενσωματώνεται στο κυρίως πρόγραμμά και <> μέσα σε αυτό.

Στο σημείο αυτό παρουσιάζονται τα Pitches:

```
#define NOTE_B0 31

#define NOTE_C1 33

#define NOTE_CS1 35

#define NOTE_D1 37

#define NOTE_DS1 39
```

```
#define NOTE_E1 41

#define NOTE_F1 44

#define NOTE_FS1 46

#define NOTE_G1 49

#define NOTE_GS1 52

#define NOTE_A1 55

#define NOTE_AS1 58

#define NOTE_B1 62

#define NOTE_C2 65

#define NOTE_CS2 69

#define NOTE_D2 73

#define NOTE_DS2 78

#define NOTE_E2 82

#define NOTE_F2 87

#define NOTE_FS2 93

#define NOTE_G2 98

#define NOTE_GS2 104
```

```
#define NOTE_A2 110

#define NOTE_AS2 117

#define NOTE_B2 123

#define NOTE_C3 131

#define NOTE_CS3 139

#define NOTE_D3 147

#define NOTE_DS3 156

#define NOTE_E3 165

#define NOTE_F3 175

#define NOTE_FS3 185

#define NOTE_G3 196

#define NOTE_GS3 208

#define NOTE_A3 220

#define NOTE_AS3 233

#define NOTE_B3 247

#define NOTE_C4 262

#define NOTE_CS4 277
```

```
#define NOTE_D4 294

#define NOTE_DS4 311

#define NOTE_E4 330

#define NOTE_F4 349

#define NOTE_FS4 370

#define NOTE_G4 392

#define NOTE_GS4 415

#define NOTE_A4 440

#define NOTE_AS4 466

#define NOTE_B4 494

#define NOTE_C5 523

#define NOTE_CS5 554

#define NOTE_D5 587

#define NOTE_DS5 622

#define NOTE_E5 659

#define NOTE_F5 698

#define NOTE_FS5 740
```

```
#define NOTE_G5 784

#define NOTE_GS5 831

#define NOTE_A5 880

#define NOTE_AS5 932

#define NOTE_B5 988

#define NOTE_C6 1047

#define NOTE_CS6 1109

#define NOTE_D6 1175

#define NOTE_DS6 1245

#define NOTE_E6 1319

#define NOTE_F6 1397

#define NOTE_FS6 1480

#define NOTE_G6 1568

#define NOTE_GS6 1661

#define NOTE_A6 1760

#define NOTE_AS6 1865

#define NOTE_B6 1976
```

```
#define NOTE_C7 2093

#define NOTE_CS7 2217

#define NOTE_D7 2349

#define NOTE_DS7 2489

#define NOTE_E7 2637

#define NOTE_F7 2794

#define NOTE_FS7 2960

#define NOTE_G7 3136

#define NOTE_GS7 3322

#define NOTE_A7 3520

#define NOTE_AS7 3729

#define NOTE_B7 3951

#define NOTE_C8 4186

#define NOTE_CS8 4435

#define NOTE_D8 4699

#define NOTE_DS8 4978
```

Στο σημείο αυτό παρουσιάζεται ο κυρίως κώδικας της εφαρμογής με τον σχολιασμό:

```
/*

##############################################################################
###

# Μικρο-επεξεργαστής: Arduino UNO

# Γλώσσα: Wiring / C++ / Επεξεργασία / Fritzing / Arduino IDE

# Σκοπός : Arduino RFID - Σύστημα Ασφαλείας και Ελέγχου Πρόσβασης

# Operation : Χρήση RFID RC - 522 , έλεγχος της πρόσβασης των ατόμων.

##############################################################################
###

*/

// Ένταξη των βιβλιοθηκών

#include <SPI.h>

#include <RFID.h>

#include <Servo.h>

#include "pitches.h"

#include <LiquidCrystal_I2C.h>

#include <Wire.h>
```

```
// Ορίζουμε το RFID

RFID rfid(10,5);

byte MATSIKA[5] = {0x04,0xCF,0xE8,0x04,0x27};

//byte EL GAMAL[5] = {0xD5, 0x75, 0x6A, 0xD5, 0x1F};

// Εδω μπορουμε να δωσουμε προσβαση και σε αλλες καρτες

// Δηλωνουμε την LCD, τη διεύθυνση και τον τύπο της

LiquidCrystal_I2C lcd(0x27,16,2);

byte serNum[5];

byte data[5];

// Οριζουμε την μελωδία πρόσβασης και την μελωδία απόρριψης / σφάλματος

int access_melody[] = {NOTE_G4,0,NOTE_A4,0,

NOTE_B4,0,NOTE_A4,0,NOTE_B4,0, NOTE_C5,0};

int access_noteDurations[] = {8,8,8,8,8,4,8,8,8,8,8,4};

int fail_melody[] = {NOTE_G2,0,NOTE_F2,0,NOTE_D2,0};

int fail_noteDurations[] = {8,8,8,8,8,4};

// Ρύθμιση LED, Buzzer και Σέρβο-κινητήρα

int LED_access = 2;
```

```
int LED_intruder = 3;

int speaker_pin = 8;

int servoPin = 9;

// Ρύθμιση του σερβοκινητήρα

Servo doorLock;

void setup(){

 doorLock.attach(servoPin); // Προετοιμασια σερβοκινητήρα

 Serial.begin(9600); // Αρχικοποίηση της σειριακής επικοινωνίας

 lcd.init(); // προετοιμασια της LCD

 lcd.backlight();

 lcd.clear();// "Καθαρίζουμε" την LCD

 SPI.begin(); // Προετοιμασία της επικοινωνίας SPI για RFID

 rfid.init(); // Εκκίνηση RFID

 lcd.setCursor(0,0);

 lcd.print ("Arduino-RFID ");

 lcd.setCursor(0,1);

 lcd.print ("RFID ETIMO ");
```

```
 Serial.println("Sustima asfaleias me Arduino RFID:AN-MFRC522");

 Serial.println("H monada RFID ksekinise stin automati anagnosi,perimenontas gia daktiliko apotipoma");

 delay(5000);

 pinMode(LED_access,OUTPUT);

 pinMode(LED_intruder,OUTPUT);

 pinMode(speaker_pin,OUTPUT);

pinMode(servoPin,OUTPUT);

}

void loop(){

 lcd.clear();

 lcd.noBacklight();

 // Εδώ θα δημιουργήσουμε μια μεταβλητή για κάθε χρήστη

 // Όνομα_finger ή κλειδί_finger

 boolean MATSIKA_finger = true; // Το αποτύπωμα

 //boolean EL GAMAL_finger = true;

 if (rfid.isfinger()){ // Αν βρεθεί το έγκυρο αποτύπωμα
```

```
if (rfid.readfinger()){ // διαβάζει το αποτύπωμα

delay(1000);

data[0] = rfid.serNum[0]; // αποθηκεύει τον σειριακό αριθμό

data[1] = rfid.serNum[1];

data[2] = rfid.serNum[2];

data[3] = rfid.serNum[3];

data[4] = rfid.serNum[4];

}



//rfid.halt(); // RFID σε κατάσταση αναμονής

lcd.backlight();

//lcd.setCursor(0,0);

//lcd.print("ID brethike:");

Serial.print("TO APOTIPOMA VRETHIKE:");

//lcd.setCursor(0,0);

Serial.print(" ");

if(data[0] < 16){
```

```
 Serial.print("0");
 }
 Serial.print(data[0],HEX);
 if(data[1] < 16){
 Serial.print("0");
 }
Serial.print(data[1],HEX);

 if(data[2] < 16){
 Serial.print("0");
 }
 Serial.print(data[2],HEX);

 if(data[3] < 16){
 Serial.print("0");
 }
 Serial.print(data[3],HEX);
```

```
if(data[4] < 16){

Serial.print("0");

}

Serial.print(data[4],HEX);

for(int i=0; i<5; i++){

if (data[i] != MATSIKA[i]) MATSIKA_finger = false;

//if (data[i] != EL GAMAL[i]) EL GAMAL_finger = false;

// Αν δεν ειναι ένα απο τα ενεργά αποτυπώματα,βγαζει "ψευδές αποτύπωμα"

// εδώ μπορουμε να ελέγξουμε τα άλλα αποτυπώματα που επιτρέπονται, απλος πρεπει να βαλουμε ποια υπαρχουν οπως η ενεργεια παραπανω

}

Serial.println();

if (PANTELIDIS_finger){ // Αν βρεθει ένα ενεργό αποτύπωμα

lcd.setCursor(0,0);

lcd.print("Ka MATSIKA");

Serial.println("GEIA SAS KYRIA MATSIKA!"); // μήνυμα εκτύπωσης
```

```
 for (int i = 0; i < 12; i++){ // παίζει μουσική καλωσορίσματος
 int access_noteDuration = 1000/access_noteDurations[i];
 tone(speaker_pin, access_melody[i],access_noteDuration);
 int access_pauseBetweenNotes = access_noteDuration * 1.30;
 delay(access_pauseBetweenNotes);
 noTone(speaker_pin);
}
 }
 //ανάλυση των άλλων αποτυπωμάτων
 /*
 else if(EL GAMAL_finger){// θέτουμε τους άλλους χρήστες εδώ){
 lcd.setCursor(0,0);
 lcd.print("Kos EL GAMAL");
 Serial.println("GEIA SAS KYRIE EL GAMAL");
 for (int i = 0; i < 12; i++)
 {
 int access_noteDuration = 1000/access_noteDurations[i];
```

```
tone(speaker_pin, access_melody[i],access_noteDuration);

int access_pauseBetweenNotes = access_noteDuration * 1.30;

delay(access_pauseBetweenNotes);

noTone(speaker_pin);

}

}

*/

else{ // Αν το αποτύπωμα δεν αναγνωριζεται

lcd.setCursor(0,0);

lcd.print ("LATHOS ID! ");

lcd.setCursor (0,1);

lcd.print ("APAGOREBETE");

Serial.println("H KARTA DEN ANAGNORIZETAI! EPIKINONEISTE ME TON DIAXEIRISTH!"); // μήνυμα εκτύπωσης

DigitalWrite (LED_intruder, HIGH); // ανάβει το LED με το πορτοκαλι χρώμα

for (int i = 0; i < 6; i++){ // παίζει τον ηχο απορριψης του χρηστη

int fail_noteDuration = 1000/fail_noteDurations[i];
```

```
 tone(speaker_pin, fail_melody[i],fail_noteDuration);
 int fail_pauseBetweenNotes = fail_noteDuration * 1.30;
 delay(fail_pauseBetweenNotes);
 noTone(speaker_pin);
 }
 delay(1000);
 digitalWrite(LED_intruder, LOW); // Το πορτοκαλι LED σβήνει
}
 if (MATSIKA_finger){// Αν εχουμε προσθέτουμε και άλλους χρήστες
 // Μήνυμα καλωσορίσματος και δικαιώματα πρόσβασης
 lcd.setCursor(0,0);
 lcd.print("PROSBASIMOS! ");
 lcd.setCursor(0,1);
 lcd.print("KALOSORISATE!");
 Serial.println("EPITREPETAI H PROSBASH!...KALOSORISATE!");
 digitalWrite(LED_access,HIGH); // Το μπλε LED ανάβει
 doorLock.write(180); // Ανοιγμα εισόδου
```

```
delay(5000); // Καθυστερηση

doorLock.write(0); // Κλεισιμο εισόδου

digitalWrite(LED_access,LOW); // Το μπλε LED σβήνει

}

/*

if (EL GAMAL_finger){

lcd.setCursor(0,0);

lcd.print("PROSBASIMOS! ");

lcd.setCursor(0,1);

lcd.print("KALOSORISATE!");



digitalWrite(LED_access,HIGH); // Το μπλε LED ανάβει

doorLock.write(180); // Ανοιγμα εισόδου

delay(5000); // Καθυστερηση

doorLock.write(0); // Κλεισιμο εισόδου

digitalWrite(LED_access,LOW); // Το μπλε LED σβήνει

}
```

```
*/

Serial.println();

delay(500);

rfid.halt();

lcd.noBacklight();

}
```

Κεφάλαιο 3 - Μελλοντικές βελτιώσεις/ επεκτάσεις

Όπως είδαμε το σύστημα που σχεδιάστηκε είναι κατάλληλο για εφαρμογές, όπου επιθυμούμε η πρόσβαση σε ένα χώρο να γίνεται ηλεκτρονικά και ασύρματα με τη βοήθεια της τεχνολογίας του αποτυπώματος. Η τεχνική αυτή προσφέρει μεγαλύτερη αξιοπιστία και ασφάλεια σε χώρους όπου η πρόσβαση απαιτεί έλεγχο των ατόμων που έχουν εξουσιοδότηση για αποφυγή κλοπών, βανδαλισμών και άλλων παρόμοιων γεγονότων. Φυσικά το σύστημα μπορεί να αναπτυχθεί κι άλλο ή ακόμα και να τροποποιηθεί, ανάλογα με τις ανάγκες. Επίσης θα μπορούσε να εφαρμοστεί σε ένα σύστημα ασφαλείας όπου υπάρχουν πραγματικές συνθήκες στον έλεγχο εξουσιοδότησης για τα άτομα που έχουν ή όχι πρόσβαση σε κάποιο χώρο.

Μετά την περάτωση της εργασίας είμαι σε θέση να επισημάνουμε ορισμένες βελτιώσεις. Μια μελλοντική ανάπτυξη του συστήματος, θα μπορούσε να είναι η δημιουργία ενός κατάλληλου λογισμικού στον ηλεκτρονικό υπολογιστή, το οποίο θα επικοινωνεί με τον μικροελεγκτή και θα κρατάει αρχείο εισόδου των ατόμων που έχουν ζητήσει πρόσβαση σε μια κάρτα μνήμης η σε ένα σκληρό δίσκο. Επίσης το αρχείο εισόδου (βάση δεδομένων) θα μπορεί να κρατάει στατιστικά και να μας παρέχει πλήρες έλεγχο για τα άτομα που πήραν πρόσβαση από το σύστημα (Ωρα, Ημέρα, Μήνα).

Επίσης με προσθήκη ενός ακόμα αισθητήρα αποτυπώματος μπορεί να επιτευχθεί και έλεγχος εξόδου, ώστε να γνωρίζουμε την ώρα και την ημερομηνία εισόδου και εξόδου των εξουσιοδοτημένων ατόμων. Με αυτόν τον τρόπο καλύπτουμε πλήρως και την είσοδο και την έξοδο όσων έχουν πρόσβαση στο σύστημα μας.

Μια αναπτυσσόμενη στις ημέρες μας τεχνολογία επίσης η οποία αξίζει να σημειωθεί είναι η επικοινωνία κοντινού πεδίου(near field communication, NFC),που αποτελεί μια πρωτότυπη τεχνολογία συνδεσιμότητας, η οποία διαδίδεται και εξελίσσεται ραγδαία με κύριο σκοπό τη λύση αρκετών προβλημάτων, σύγχρονων αλλά και μελλοντικών. Η

λειτουργία της βασίζεται στην επαφή ή στη προσέγγιση, σε απόσταση 4 ή 5 εκατοστών της συσκευής που περιέχει το τσιπ NFC. Η τεχνολογία αυτή συνδυάζει παλαιότερες τεχνολογίες ασύρματης επικοινωνίας όπως το Bluetooth και το RFID, οι οποίες εναρμονίζονται ώστε να παρέχονται υπηρεσίες στους χρήστες στις παρακάτω ενδεικτικές περιπτώσεις:

- Έλεγχος πρόσβασης
- Ηλεκτρονικές συναλλαγές
- Ανταλλαγή και συλλογή πληροφοριών
- Νομιμότητα
- Πληρωμές
- Μεταφορές/Διαβιβάσεις
- Πιστοποιήσεις

Συμπεράσματα

Ο αρχικός στόχος που τέθηκε κατά την υλοποίηση του συστήματος επιτεύχθηκε. Υλοποιήθηκε, δηλαδή, ένα σύστημα οικιακού αυτοματισμού κλειδώματος πλήρως λειτουργικό. Επιπλέον, το σύστημα είναι πλήρως επεκτάσιμο. Με τον ίδιο τρόπο θα μπορούσε να ελέγχθει οποιαδήποτε οικιακή συσκευή που συνδέεται στα 220V του δικτύου της Δ.Ε.Η, δηλαδή, σε μια οικιακή πρίζα. Οι δυνατότητες του συστήματος βέβαια δεν περιορίζονται στον έλεγχο μόνο μίας συσκευής, αφού ο μικροελεγκτής διαθέτει πλήθος γραμμών εισόδου/εξόδου, τόσο ψηφιακών όσο και αναλογικών. Οι αναλογικές είσοδοι μπορούν να χρησιμοποιηθούν είτε σαν ψηφιακές I/O, οπότε έτσι μπορούν να ελεγχθούν και επιπλέον συσκευές, είτε σαν είσοδοι αισθητήρων αναλογικών μεγεθών που θα επιτρέπουν στο χρήστη να ελέγχει αναλογικά μεγέθη όπως πίεση, υγρασία, φωτεινότητα κ.τ.λ. Το σύστημα, συνεπώς, μπορεί να τροποποιηθεί και να ικανοποιήσει διαφορετικές ανάγκες χρηστών.

Η τροποποίηση αυτή περιλαμβάνει τρία στάδια. Το στάδιο της αλλαγής της συνδεσμολογίας του μικροελεγκτή με τις συσκευές προς έλεγχο. Το στάδιο της τροποποίησης του σχεδίου (sketch) που θα φορτωθεί στον μικροελεγκτή, καθώς και το στάδιο της τροποποίησης των τελικών εφαρμογών του χρήστη. Στο σημείο αυτό θα πρέπει να επισημανθεί ότι οι κώδικες που έχουν γραφεί σίγουρα δεν είναι βέλτιστοι οπότε κάποιος μπορεί να τους τροποποιήσει και να έχει καλύτερα αποτελέσματα. Επιπλέον, θα πρέπει να επισημανθεί και να εξεταστεί το θέμα της ασφάλειας. Η ασφάλεια της επικοινωνίας δεν αποτέλεσε αντικείμενο της παρούσας υλοποίησης. Σίγουρα ένας ειδικός στην ασφάλεια των επικοινωνιών θα βρει τρωτά σημεία στον τομέα της επικοινωνίας, όπως για παράδειγμα το ότι το password ταξιδεύει «φανερά» στη σύνδεση με πιθανό κίνδυνο υποκλοπής.

Θα πρέπει παρόλα αυτά να τονιστεί ότι οι προαναφερθείσες βελτιώσεις και επεκτάσεις δεν αυξάνουν (παρά μόνο ελάχιστα ίσως) το κόστος του συστήματος, το οποίο δεν ξεπέρασε τα 70€, χρησιμοποιώντας παντού καινούρια υλικά. Αυτός ήταν και ένας επιπλέον στόχος της παρούσας διπλωματικής, η ανάπτυξη δηλαδή ενός πλήρως λειτουργικού συστήματος

οικιακού αυτοματισμού με το μικρότερο δυνατό κόστος. Συνοψίζοντας, η βελτίωση των κωδίκων που έχουν γραφεί (π.χ. μέσω της ανάπτυξης ενός ολοκληρωμένου πρωτοκόλλου επικοινωνίας των συσκευών του τελικού χρήστη με τον μικροελεγκτή), καθώς και το θέμα της ασφάλειας της επικοινωνίας αποτελούν τα σημεία μελλοντικής ανάπτυξης του συστήματος που υλοποιήθηκε. Έχοντας ως βάση τον επιτυχημένο απομακρυσμένο έλεγχο συσκευών που παρέχει το συγκεκριμένο σύστημα, μπορεί πλέον κάποιος να το επεκτείνει, να το βελτιώσει και σίγουρα να το κάνει πιο ασφαλές με απώτερο στόχο τη λειτουργικότητα, τη βελτίωση της καθημερινότητας του ανθρώπου και τελικά την πρόοδο της επιστήμης.

Βιβλιογραφία

1. Kim, J., Brewer, P., & Bernhard, B. (2008). Hotel customer perceptions of biometric door locks: Convenience and security factors. Journal of Hospitality & Leisure Marketing, 17(1-2), 162-183.
2. Smith, A. D. (2005). Exploring the acceptability of biometrics and fingerprint technologies. International Journal of Services and Standards, 1(4), 453-481.
3. Zhang, S., Janakiraman, R., Sim, T., & Kumar, S. (2006, January). Continuous verification using multimodal biometrics. In International Conference on Biometrics (pp. 562-570). Springer Berlin Heidelberg.
4. Jo, J. G., Seo, J. W., & Lee, H. W. (2007, August). Biometric digital signature key generation and cryptography communication based on fingerprint. In International Workshop on Frontiers in Algorithmics (pp. 38-49). Springer Berlin Heidelberg.
5. You, L., Zhang, G., & Zhang, F. (2011). A cryptographic key binding method based on fingerprint features and the threshold scheme. International Journal of Advancements in Computing Technology, 3(4), 21-31.
6. Thian Song, O., Teoh Beng Jin, A., & Connie, T. (2007). Personalized biometric key using fingerprint biometrics. Information Management & Computer Security, 15(4), 313-328.
7. Chen, H., Sun, H., & Lam, K. Y. (2007, November). Key management using biometrics. In Data, Privacy, and E-Commerce, 2007. ISDPE 2007. The First International Symposium on (pp. 321-326). IEEE.
8. Feng, Q., Su, F., & Cai, A. (2008). Fingerprint-based key binding/recovering scheme based on fuzzy vault. Journal of Electronics (China), 25(3), 415-421.
9. Gangi, R. R., & Gollapudi, S. S. (2013). Locker opening and closing system using RFID fingerprint password and GSM. International Journal of Emerging Trends & Technology in Computer Science, 2(2).
10. Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. (2015, December). Fingerprint Biometric based Access Control and Classroom Attendance Management System. In India Conference (INDICON), 2015 Annual IEEE (pp. 1-6). IEEE.

11. Liu, Y. (2008). Identifying legal concerns in the biometric context. J. Int'l Com. L. & Tech., 3, 45.
12. Hemalatha, A. (2011). A Secured Biometric Attendance System (Thumsec System) With Access Lock Control.
13. Yaakob, M. K. B., Jamia'an, M. B., Ramli, N. I. B. N., Elias, M. R. B., & Zulkifli, A. B. (2013). Embedded Door Lock System Using Biometric Technology (EDLS).