Ατομική Διπλωματική Εργασία

SMART HOMES APPLICATION AND INTERNET OF THINGS

USING MAIXPY DOCK TOOL KIT

Μενέλαος Αρτεμίου

Πανεπιστήμιο Κύπρου

Τμήμα Πληροφορικής

Μάιος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

SMART HOMES APPLICATION AND INTERNET OF THINGS

USING MAIXPY DOCK TOOL KIT

Μενέλαος Αρτεμίου

Επιβλέπων Καθηγητής

Αντρέας Πιτσιλλίδης

Η Ατομική Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Μάιος 2020

Ευχαριστίες

Με αφορμή την υλοποίηση της παρούσας διπλωματικής εργασίας, θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου κ. Αντρέα Πιτσιλλίδη, καθηγητή του Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου, για την καθοδήγηση και την εμπιστοσύνη που έδειξε σε κάθε μας συνεργασία.

Το πιο θερμό ευχαριστώ το οφείλω στην οικογένειά μου για την στήριξη και τη βοήθεια που μου παρείχε για την εκπλήρωση και περάτωση αυτού του επιστημονικού τίτλου σπουδών.

Επίσης, θα ήθελα να ευχαριστήσω ιδιαιτέρως το σύντροφό μου, για την υπομονή και τη στήριξη των προσπαθειών και των κόπων μου.

Περίληψη

Η τεχνολογική πρόοδος γνωρίζει ραγδαία ανάπτυξη τα τελευταία χρόνια σε διάφορους τομείς, επιτρέποντας τη δημιουργία νέων τεχνολογικών προϊόντων τα οποία χρησιμοποιούνται σε καθημερινή βάση. Μια βασική παράμετρος στη διαβίωση μας είναι ο τομέας της ασφαλείας και της προστασίας των προσωπικών μας περιουσιών. Για τη διατήρηση της ασφάλειας τους εκτός από τη χρήση ισχυρών φυσικών κλειδαριών τεχνολογικά δεν χρησιμοποιούμε κάτι άλλο από ένα κλειδί. Η μέθοδος αυτή έχει πολλά αρνητικά, σε αρκετές περιπτώσεις δεν είμαστε τόσο ασφαλείς όσο νομίζουμε. Θεωρητικά οι περισσότερες θύρες ασφαλείας είναι απαραβίαστες, μέχρι του σημείου που μας κλαπεί το κλειδί. Επιπρόσθετα με τους συνεχόμενα αυξανόμενους ρυθμούς που ζούμε εξάγεται η ανάγκη για αυτοματισμούς που θα βοηθούν την καθημερινότητα μας. Ένα αυτοματοποιημένο σύστημα μας απαλλάσσει από την ανάγκη να έχουμε στην κατοχή μας κλειδιά για να εισέλθουμε ή να εξέλθουμε από το σπίτι μας, χωρίς να επιτρέπουμε σε ανεπιθύμητα άτομα να έχουν πρόσβαση στην περιουσία μας.

Η παρούσα διπλωματική εργασία μελετά ένα συγκεκριμένο τομέα της τεχνολογίας ο οποίος είναι τα "Έξυπνα Σπίτια". Στόχος αυτής της εργασίας είναι η ανάπτυξη ενός ολοκληρωμένου συστήματος ταυτοποίησης, το οποίο θα αντικαταστήσει τις παραδοσιακές κλειδαριές. Στόχος του συστήματος είναι να έχει το χαμηλότερο δυνατό κόστος, έτσι ώστε να είναι προσιτό σε όλο το κόσμο, χωρίς να διακυβεύεται η ασφάλεια της περιουσίας του. Οι χρήστες μέσω του συστήματος θα έχουν την δυνατότητα να επιλέγουν τα άτομα τα οποία, θα έχουν πρόσβαση στο σύστημα. Παράλληλα το σύστημα θα λειτουργεί και ως σύστημα ασφαλείας αφού μόλις εντοπίσει άνθρωπο κοντά στην πόρτα θα καταγράφει το πρόσωπο του. Το σύστημα θα λειτουργεί με αναγνώριση προσώπου και θα το ταυτοποιεί κάνοντας χρήση αλγορίθμων, μηχανικής μάθησης και νευρωνικών δικτύων.

Περιεχόμενα

Κεφάλαιο 1 **Εισαγωγή**

1.1: Γενική Περίληψη

Τα τελευταία χρόνια παρατηρείται μια ραγδαία αύξηση της τεχνολογίας σε διάφορους τομείς, ταυτόχρονη ανάπτυξη γνωρίζει και η εύρεση τεχνικών για να αυτοματοποιηθούν διάφορες καθημερινές ασχολίες, λόγω του ρυθμού ζωής της εποχής στης οποίας ζούμε. Μια εκ των σημαντικότερων αναγκών είναι η ικανότητα να μπορεί ο κάθε άνθρωπος να προστατεύσει την είσοδο στην περιουσία του σε μη εξουσιοδοτημένα από τον ίδιο άτομα. Η αρχή αυτή δεν περιορίζεται σε ατομικό επίπεδο(π.χ. υποκλοπή του κλειδιού εισόδου στο σπίτι), αλλά επεκτείνεται τόσο σε εμπορικό και κυβερνητικό επίπεδο(π.χ. παραβίαση δικλίδων ασφαλείας, συνήθως κάποιου κωδικού που δίνει τη δυνατότητα πρόσβασης σε μη εξουσιοδοτημένα άτομα). Όπως γίνεται αντιληπτό ο αντίκτυπος είναι μεγάλος και οι λύσεις σε ένα τέτοιο ζήτημα πρέπει να παρέχουν την μέγιστη ασφάλεια και να ελαχιστοποιεί τον τρόπο με το οποίο κάποιος επιτήδειος θα επιχειρήσει να παραβιάσει τους μηχανισμούς ασφαλείας της εφαρμογής.

Σε ένα τέτοιο σημαντικό ζήτημα μια νέα τάση η οποία ονομάζεται Internet of Things μπορεί να παρέχει κάποιες εξειδικευμένες λύσεις. Προσεγγίζοντας το πρόβλημα αυτό μπορεί να γίνει χρήση διαφόρων αισθητήρων και συσκευών όπως και χρήση τεχνολογιών για αυτοματοποιημένα συστήματα ικανά να παίρνουν αποφάσεις. Για τη λήψη των αποφάσεων μπορεί να εφαρμοστεί και κάποιου είδους αλγόριθμος τεχνίτης νοημοσύνης και μηχανικής μάθησης.

1.2: Περιγραφή και Κίνητρο

Αντιλαμβανόμαστε από τα λεγόμενα πιο πάνω, ότι υπάρχει αυξημένη ανάγκη εύρεσης τεχνικών αντικατάστασης των παραδοσιακών τρόπων ταυτοποίησης οι οποίες σε συγκεκριμένες περιπτώσεις ευνοούσαν την παραβίαση τους, ενώ ταυτόχρονα απαιτούσαν από το χρήστη συνήθως να έχει ένα token(κλειδί) ή να θυμούνται κάποιο κωδικό ασφαλείας. Οι δύο αυτές πρακτικές δεν είναι οι καταλληλότερες στο κομμάτι λειτουργικότητας αφού στην token based προσέγγιση(ανάγκη κατοχής κλειδιού ή κάρτας) το token μπορεί να κλαπεί και να χρησιμοποιηθεί από τον καθένα, ενώ πιθανόν είναι να το χάσουμε ή να ξεχαστεί κάπου. Η password based προσέγγιση(ανάγκη κατοχής κωδικού ασφαλείας) ο οποίος επίσης είναι εύκολο να κλαπεί, επίσης απαιτεί από τον χρήστη να τον θυμάται δυσκολεύοντας τους έτσι περαιτέρω. Αυτό έχει ως αποτέλεσμα πολλοί χρήστες να τους καταγράφουν σε χαρτί όπου και αυτό είναι εξίσου εύκολο να κλαπεί ή να χαθεί. Αναλύοντας τις απαιτήσεις οι οποίες αναλύθηκαν αντιλαμβανόμαστε το κύριο κίνητρο για το θέμα της εργασίας.

Πρέπει να παρέχει στο χρήστη τη δυνατότητα ταυτοποίησης με ελάχιστο περιθώριο σφάλματος. Επιπρόσθετα δεν θα πρέπει να περιορίζεται από περιβαλλοντικές συνθήκες όπως σκοτάδι αφού θα είναι δικλείδα ασφαλείας μεταξύ του χώρου του οποίου θέλουμε να προστατεύσουμε και των εξωτερικών παρατηρητών. Επιπρόσθετα το σύστημα το οποίο θα αναπτυχθεί θα πρέπει να είναι όσο πιο οικονομικό γίνεται δίνοντας τη δυνατότητα σε εταιρίες και ιδρύματα(π.χ. πανεπιστήμια) να το χρησιμοποιήσουν για όλους τους σημαντικούς χώρους, για παράδειγμα μπορεί να εγκατασταθεί στα εργαστήρια της πληροφορικής έτσι ώστε να επιτρέπετε η είσοδος μόνο σε φοιτητές της πληροφορικής, ενώ παράλληλα θα λειτουργεί και σαν σύστημα ασφαλείας αφού θα καταγράφει τις προσπάθειες εισόδου στους χώρους αυτούς.

1.3: Στόχος της εργασίας και Συνεισφορά

Ο στόχος λοιπόν αυτής της διπλωματικής εργασίας είναι να δημιουργηθεί ένα σύστημα το οποίο θα έχει το λιγότερο δυνατό κόστος και να παρέχει την μέγιστη δυνατή ασφάλεια. Το σύστημα αυτό δίνει την δυνατότητα σε χώρους όπου φυλάσσονται ευαίσθητα δεδομένα μεγαλύτερη ασφάλεια απαλλάσσοντας τους παράλληλα από την ανάγκη δημιουργίας απαραβίαστων κλειδαριών και κωδικών ασφαλείας.

Για τον σχεδιασμό τέτοιου συστήματος θα γίνει χρήση βιομετρικών χαρακτηριστικών συγκεκριμένα η σχηματομορφή του προσώπου και τα χαρακτηριστικά του. Το σύστημα το οποίο έχει υλοποιηθεί μέσα από αυτή την εργασία είναι ευέλικτο, έχει χαμηλό κόστος και μπορεί εύκολα να επεκταθεί προσθέτοντας καινούριους αισθητήρες, παρέχοντας έτσι τη δυνατότητα στους χρήστες να καλύψουν τις ανάγκες τους. Κάθε υπομονάδα έχει την δική της οθόνη η οποία αλληλοεπιδρά με τον χρήστη δίνοντας του τις απαραίτητες πληροφορίες για να ακολουθήσει την διαδικασία με ακρίβεια και σαφήνεια.

1.4: Δομή Εργασίας

Η διπλωματική εργασία θα ακολουθήσει την ακόλουθη δομή:

Κεφάλαιο 1 **Εισαγωγή**

Σε αυτό το κεφάλαιο έχουμε μια γενική εισαγωγή για την ραγδαία ανάπτυξη της τεχνολογίας καθώς και για την τελευταία τάση του Internet of Things και του Smart Home. Στη συνέχεια αναφερόμαστε στα κίνητρα που μας ώθησαν να αναπτύξουμε ένα τέτοιο σύστημα και τι αναμένουμε από αυτό. Ακολούθως περιγράφεται ο στόχος και η συνεισφορά της εργασίας, τελειώνοντας καταγράφεται η δομή που θα έχει η εργασία αυτή.

Κεφάλαιο 2 Γνωστικό Υπόβαθρο

Σε αυτό το κεφάλαιο γίνονται περιγραφές για κάποιους όρους και τεχνολογίες που έχουν χρησιμοποιηθεί για την υλοποίηση αυτής της εργασίας. Υπάρχουν αναφορές για το Internet of Things, το Smart Home, τα Face Recognition Systems, όπως επίσης για το υλικό και λογισμικό που χρησιμοποιήθηκε για την ολοκλήρωση της διπλωματικής.

Κεφάλαιο 3 **Μεθοδολογία**

Σε αυτό το κεφάλαιο γίνεται μια περιγραφή για τις επιλογές που έχουν γίνει σχετικά με το υλικό και το λογισμικό που έχουν χρησιμοποιηθεί καθώς και το λόγο τον οποίον έχουν επιλεχτεί να χρησιμοποιηθούν σε αυτή την εργασία. Παράλληλα περιγράφεται και η προσέγγιση, ως προς την υλοποίηση του συστήματος.

Κεφάλαιο 4 **Αξιολόγηση**

Σε αυτό το κεφάλαιο γίνεται μια περιγραφή για την λήψη αποτελεσμάτων, όπως και για την μεθοδολογία που ακολουθήθηκε για να καταλήξουμε, εάν το σύστημα επιτελεί τον τελικό του σκοπό.

Κεφάλαιο 5 **Σύνοψη**

Σε αυτό το κεφάλαιο καταγράφονται τα συμπεράσματα από την ανάπτυξη αυτού του συστήματος, τα μελλοντικά σχέδια όπου θα μπορούσε να χρησιμοποιηθεί και οι περιορισμοί που είχαμε κατά την προσαρμογή του.

Κεφάλαιο 2: **Γνωστικό Υπόβαθρο**

2.1: Internet of Things

Ο όρος “Internet of Things” αδιαμφησβήτητα αποτελεί δικαίως ένα από τα πιο πολυσυζητημένα τεχνολογικά θέματα του 21ου αιώνα. Η ιδέα αυτή έχει τις ρίζες της την δεκαετία του 1990 όπου διάφοροι επιστήμονες οραματίζονταν ένα κόσμο όπου οι υπολογιστές θα συνυπήρχαν με τους ανθρώπους διευκολύνοντας τους στην καθημερινότητα τους. Το 1991 ο Mark Weiser εκδίδει την μελέτη "The Computer of the 21st Century"[1] όπου αναφέρεται στον όρο “ubiquitous computing” όπου οι άνθρωποι εκτός από του παραδοσιακού τύπου υπολογιστές(laptop, stationary computer) θα αλληλοεπιδρούν με καθημερινά αντικείμενα όπως ψυγεία, γυαλιά οράσεως κ.α. Στην προσπάθεια ένταξης της ιδέας αυτής εκείνη τη εποχή στηρίζουν διάφοροι ακαδημαϊκοί οργανισμοί όπως: UbiComp, PerCom[2] και IEEE οι οποίοι περιέγραψαν την ιδέα αυτή σαν μια μεταφορά μικρών ποσών από δεδομένα έτσι ώστε να ενοποιήσουν και να αυτοματοποιήσουν το κόσμο γύρω μας. Ο όρος “Internet of Things” πιθανότατα επινοήθηκε από τον Kevin Ashton το 1999, ο οποίος πίστευε ότι η ταυτοποίηση μέσω ραδιοσυχνοτήτων(RFID) είναι αναγκαία τεχνολογία αφού θα επιτρέπει στους υπολογιστές να διαχειριστούν τις διεργασίες.

Στην σύγχρονη εποχή ο όρος IoT αναφέρεται σε ένα οικοσύστημα το οποίο αποτελείται από συσκευές οι οποίες είναι συνδεδεμένες στο διαδίκτυο συλλέγοντας δεδομένα. Ακολούθως τα δεδομένα τα οποία έχουν ληφθεί χρησιμοποιούνται για την παροχή λύσεων. Περιοχές οι οποίες υποβοηθούνται της τεχνολογίας αυτής αφορούν τομείς της εκπαίδευσης, υγείας και ασφάλειας των πολιτών, καθώς και σε διάφορες πτυχές της

καθημερινής μας ζωής. Υπολογίζεται ότι μέχρι το 2020 θα υπάρχουν 50 δισεκατομμύρια συσκευές οι οποίες θα είναι συνδεδεμένες με το διαδίκτυο.

Όπως γίνεται αντιληπτό οι τομείς οι οποίοι επηρεάζονται είναι αρκετοί, με αποτέλεσμα να είναι μια αρκετά σύνθετη τεχνολογία η οποία αποτελείται από τρία επίπεδα, το καθένα συμβάλει αυτόνομα ή και συνεργατικά με τα υπόλοιπα για την επίλυση τις διεργασίας το οποίο προορίζεται.

Figure 2.1.1: Internet of things

Αρχιτεκτονική IoT

Όπως προαναφέρθηκε η αρχιτεκτονική του IoT αποτελείται από τρία επίπεδα:

"Things"

Όπου απαρτίζονται οι συνδεδεμένες συσκευές υπεύθυνες για αλληλεπίδραση και συλλογή δεδομένων με το περιβάλλον και συνήθως είναι διαφόρων τύπων αισθητήρες. Καίριοι τομείς που επηρεάζονται:

Έξυπνα Σπίτια

Αποτελεί τον τομέα με την υψηλότερη απήχηση αφού εκτός του ότι είναι από τους πιο διαδεδομένους και ανεπτυγμένους τομείς, είναι και αυτός που επηρεάζει άμεσα και τους περισσότερους ανθρώπους. Η ενσωμάτωση αισθητήρων σε διάφορα σημεία αναφοράς(για παράδειγμα αισθητήρας θερμοκρασίας, αισθητήρας διαρροών νερού, υγραερίου κ.λ.π.) προσφέρουν πρόληψη και ασφάλεια από τυχών ατυχήματα και ζημιές, διευκολύνουν την διαβίωση, παρέχουν μεμακρυσμένο τρόπο ελέγχου και παρακολούθησης διαφόρων σημείων στο σπίτι, κάνοντας τη διαβίωση μας σε αυτό ποιοτικότερη. Επιπρόσθετα συμβάλλουν περεταίρω στην ασφάλεια και διαφύλαξη της προσωπικής περιουσίας μας

προειδοποιώντας μας για τυχόν παραβάσεις (και σε κάποιες περιπτώσεις και τον εισβολέα, ότι είμαστε ενήμεροι για την παρουσία του με πιθανό αποτέλεσμα τη φυγή του) εξασφαλίζοντας στοιχεία για υποβοήθηση εύρεσης του δράστη ή για την καταδίκη του. Η χρήση τέτοιων αισθητήρων εκτός από αποτρεπτικό παράγοντα σε επίδοξους διαρρήκτες αποτελεί και τρόπο ελέγχου κατοικίδιων και ανθρώπων τρίτης ηλικίας ή με αναπηρίες για διαπίστωση σε πραγματικό χρόνο σε ποια κατάσταση βρίσκονται.

Figure 2.1.2: Τομέας

Υγεία

Ο τομέας της υγείας επίσης γνωρίζει τεράστια ανάπτυξη καθώς αισθητήρες έχουν τοποθετηθεί σε fitbits και smartwatch οι οποίοι παρακολουθούν και ενημερώνουν ασθενείς και ιατρικό προσωπικό για διάφορες ζωτικές λειτουργίες ενώ άλλες προσεγγίσεις ειδοποιούν σωστικά συνεργεία σε περίπτωση που αντιληφθούν ότι ο χρήστης βρίσκεται σε κάποια επικίνδυνη κατάσταση (χαρακτηριστικό παράδειγμα αποτελεί η πτώση ενός ποδηλάτη σε γκρεμό και το smartwatch έστειλε αυτόματα στίγμα θέσης στα σωστικά συνεργεία βοηθώντας έτσι στην έγκαιρη εύρεση και διάσωση του).

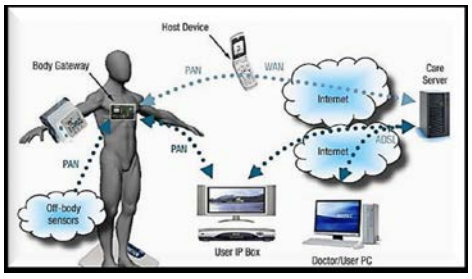


Figure 2.1.3: Τομέας Υγείας

Μεταφορές και Διακίνηση

Η χρήση αισθητήρων μπορεί να μειώσουν δραστικά την κυκλοφοριακή συμφόρηση, αφού θα ενημερώνουν τους οδηγούς για τυχόν ατυχήματα, οδικά έργα ή άλλες πηγές

καθυστερήσεων στο οδικό δίκτυο προτείνοντας τους εναλλακτικές διαδρομές σε πραγματικό χρόνο. Επίσης θα παρέχονται άλλες χρήσιμες πληροφορίες όπως χώροι στάθμευσης, διανυκτερεύοντες υπηρεσίες, διευκολύνοντας έτσι την καθημερινότητα. Η χρήση αισθητήρων μπορεί να βοηθήσει και στα Μέσα Μαζικής Μεταφοράς παρέχοντας ακριβέστερες πληροφορίες για τον χρόνο άφιξης των μέσων. Παρόλα αυτά ο πιο σημαντικός τομέας στο χώρο αυτό είναι η αυτοματοποιημένη οδήγηση αφού η πληθώρα δεδομένων που συλλέγονται από αισθητήρες σε αυτοκίνητα αυτή τη στιγμή θα διευκολύνει τη συντομότερη εφαρμογή του μέτρου. Άμεσο συνεπακόλουθο της εφαρμογής θα είναι λιγότερες οδικές συγκρούσεις και περεταίρω μείωση της κυκλοφοριακής συμφόρησης αφού δεν θα υφίσταται η ανάγκη οδικών σημάνσεων όταν όλα τα αυτοκίνητα θα είναι σε θέση να κινούνται αυτόνομα, αφού θα επικοινωνούν άμεσα μεταξύ τους και οι αποφάσεις προτεραιότητας και διασταυρώσεων θα παίρνονται από κοινού μέσω ίδιου κώδικα οδήγησης που θα ακολουθούν.

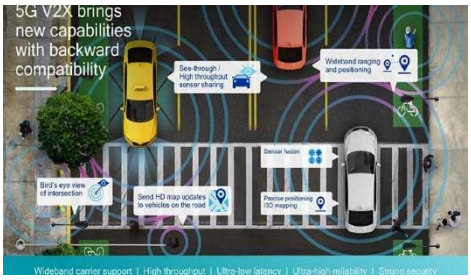


Figure 2.1.4: Τομέας Μεταφορών και Διακίνησης

Άμυνα

Εφαρμογές υπάρχουν και για στρατιωτική χρήση, αφού η χρήση αισθητήρων για παρακολούθηση βιομετρικών συστημάτων καθώς και παροχή χρήσιμων πληροφοριών για το πεδίο της μάχης, θα ελαττώσουν τις απώλειες στρατιωτών. Επιπρόσθετα η χρήση αισθητήρων για αναγνώριση και επιτήρηση στόχων θα μειώσει περισσότερο με τη σειρά του την θνησιμότητα των μαχών και θα δώσει σημαντικό προβάδισμα στις χώρες που χρησιμοποιούν τις τεχνολογίες αυτές.

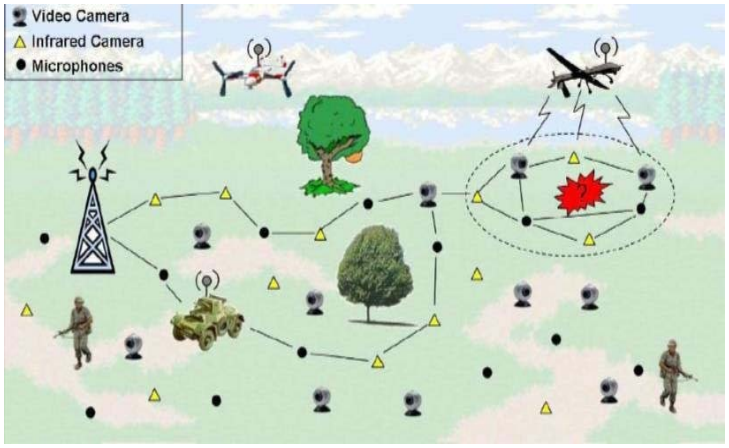


Figure 2.1.5: Τομέας Άμυνας

"Communication and Networking"

Όπου απαρτίζεται ο τρόπος μεταφοράς των δεδομένων που συλλέχθηκαν από το προηγούμενο επίπεδο στο επόμενο για την αποθήκευση και επεξεργασία τους.

Sensors-Devices to Gateway (Networking)

Σε αυτό το υπερεπίπεδο απαρτίζεται ο εξοπλισμός ο οποίος είναι υπεύθυνος για την ενσύρματη και ασύρματη επικοινωνία από τους αισθητήρες στα Gateways.

Gateway to ISP-Data Center (Communication)

Σε αυτό το υπερεπίπεδο απαρτίζεται ο εξοπλισμός ο οποίος είναι υπεύθυνος για την ενσύρματη και ασύρματη επικοινωνία από τα Gateways προς το Cloud για την μεταφορά δεδομένων στα αποθηκευτικά συστήματα.

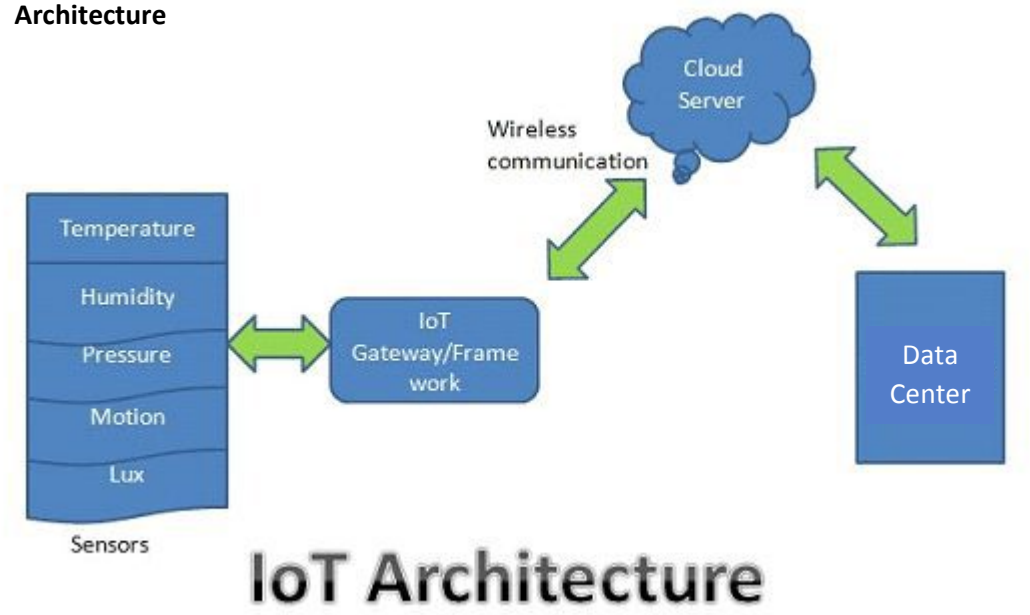
"Calculation and Storage"

Όπου απαρτίζεται από την αποθήκευση και επεξεργασία των δεδομένων.

Big Data Analysis

Τα δεδομένα από το προηγούμενο επίπεδο επεξεργάζονται σε πραγματικό χρόνο μέσω αλγορίθμων big data analysis.

Figure 2.1.6: IoT Architecture



2.2: Smart Home:

Smart Home ορίζεται η εξόπλιση του οικιακού περιβάλλοντος με τεχνολογίες και αισθητήρες οι οποίες θα υποβοηθούν τον άνθρωπο στην καθημερινή του διαβίωση διευκολύνοντας την καθημερινότητά του. Μέσω εφαρμογής παρέχεται στο χρήστη η δυνατότητα να ελέγχει την κατάσταση των αισθητήρων, διάφορες μετρήσεις ακόμη και να ενημερώνεται για τις αλλαγές που πιθανόν να έχουν οι καταστάσεις των αισθητήρων. Οι εφαρμογές αυτές παρέχουν την δυνατότητα λειτουργιών όπως αυτοματοποιήσεις, απομακρυσμένου χειρισμού διαφόρων τύπων(φωνητικές εντολές, menu διεπαφών κ.α.). Για την επικοινωνία και αποστολή δεδομένων έχουν υλοποιηθεί διαφορά πρωτόκολλα ανάλογα με τις συνθήκες τις οποίες καλούνται να λειτουργήσουν(π.χ. μακροχρόνια χρήση χωρίς παροχή ενέργειας, έκθεση τους σε εξωτερικές συνθήκες κ.α.) καθώς και τις διεργασίες τις οποίες καλούνται να επιτελέσουν. Βασικότερες εκ των οποίων είναι Bluetooth, WiFi, ZigBee, MQTT, CoAP, DDS, NFC, Cellular, AMQP, LoRaWAN το καθένα διαθέτει τα δικά του πλεονεκτήματα και μειονεκτήματα και χρησιμοποιείται αναλόγως της εφαρμογής και της διεργασίας που θα εκτελεί.

Όπως προαναφέρθηκε η ανάπτυξη εφαρμογών για έξυπνο σπίτι βρίσκονται στην ακμή τους, αφού έχουν την πιο άμεση επίδραση στην ποιότητα ζωής των ανθρώπων. Κυριότερες εφαρμογές είναι:

Σύστημα ελέγχου-Ασφαλείας

Η εγκατάσταση αισθητήρων κίνησης σε πιθανά σημεία παραβάσεων(παράθυρα και θύρες) μπορεί να ανιχνεύσει τις προσπάθειες αυτές και να ληφθούν μέτρα σε πραγματικό χρόνο(ειδοποίηση χρήστη και αστυνομίας, ενεργοποίηση συναγερμού κ.α.). Επιπρόσθετα η προσθήκη συσκευών καταγραφής ήχου και εικόνας(cameras), παρέχει την δυνατότητα στο χρήστη παρακολούθησης της περιουσίας του τόσο για λόγους ασφάλειας όσο και αν υπάρχουν ευπαθείς ομάδες στο σπίτι(π.χ. ηλικιωμένοι, μικρά παιδία) τα οποία χρειάζονται επιτήρηση για να βεβαιώνεται ανά πάσα στιγμή για τη σωματική τους ακεραιότητα. Μια πιο εξειδικευμένη χρήση των καμερών είναι και η χρήση τους για αντικατάσταση των συμβατικών κλειδαριών με “smart locks”, ακολουθώντας τη λογική της ταυτοποίησης μέσω ανθρώπινων χαρακτηριστικών(κυρίως προσώπου). Η τελευταία εφαρμογή θέλει ιδιαίτερο χειρισμό καθώς το σύστημα πρέπει να βρίσκεται σε θέσει να δίνει πρόσβαση μόνο στα εξουσιοδοτημένα άτομα. Παρόλα αυτά θα είναι πολύ χρήσιμο αφού μπορεί να απαλείψει πλήρως την ανάγκη μεταφοράς κλειδιών και επίσης δίνει τη δυνατότητα παρακολούθησης και καταγραφής του ατόμου που επιχειρεί να εισέλθει καθώς και επιπλέον πληροφορίες όπως ημερομηνία και ώρα. Η εφαρμογή αυτή εκτός από σπίτια έχει εφαρμογές και σε άλλους χώρους όπως εταιρίες, κυβερνητικοί οργανισμοί, στρατόπεδά κ.α. αυξάνοντας την ασφάλεια αφού όπως προαναφέρθηκε (νοουμένου ότι θα λειτουργεί άψογα) δεν θα υπάρχει τρόπος να έχει πρόσβαση μη εξουσιοδοτημένα άτομα με το επιπλέον πλεονέκτημα της καταγραφής αρχείου (πιθανόν και ειδοποίησης) για επιτυχής και ανεπιτυχής προσπάθειες.

Συσκευές ανίχνευσης ατόμων

Συστήματα τέτοιου είδους υπάγονται στον τομέα της ασφάλειας αφού μπορούν να χρησιμοποιηθούν για άτομα με άνοια τα όποια εάν απομακρυνθούν από το οικείο περιβάλλον υπάρχει πιθανότητα να χαθούν ή να πάθουν κάτι. Για το λόγο αυτό πρέπει να ειδοποιηθεί κάποιος νωρίς σε περίπτωση που αρχίζουν να απομακρύνονται. Επίσης μπορεί να εφαρμοστεί σε

κρατούμενους σωφρονιστικών ή και άλλων ιδρυμάτων σε περίπτωση που επιχειρήσουν ή έχουν αποδράσει να εντοπιστούν έγκαιρα.

Σύστημα ελέγχου φωτισμού-φωτοαισθητήρων

Αρχικά δίνεται η δυνατότητα της εξ αποστάσεως ελέγχου του φωτισμού, έτσι ακόμη και αν βρισκόμαστε μακριά, για τον εξωτερικό παρατηρητή φαίνεται ότι κάποιος είναι στο σπίτι κάνοντας πιθανούς διαρρήκτες να το ξανασκεφτούν πριν επιχειρήσουν διάρρηξη. Επιπρόσθετα συμβάλει και στην εξοικονόμηση ενέργειας αφού μπορούμε να ελέγξουμε(ή ακόμη και να ειδοποιηθούμε) ότι υπάρχει ανοικτό κάποιο φως στο σπίτι. Επίσης φωτοαισθητήρες μπορούν να χρησιμοποιηθούν για τον έλεγχο κουρτινών, για παράδειγμα να ανοίγουν ελάχιστο λίγο πριν το ξυπνητήρι και τελείως μετά από αυτό(νοουμένου ότι υπάρχει φως από τον ήλιο) βοηθώντας μας να ξυπνήσουμε ευκολότερα. Μια άλλη εφαρμογή είναι να ανοίγουν για να ζεσταθεί το σπίτι όταν ανιχνεύσουν φως κατά την χειμερινή περίοδο, ενώ αντίθετα να κλείνουν το καλοκαίρι για να διατηρούν δροσερό το σπίτι(η εφαρμογή αυτή μπορεί να συνεργάζεται και με κάποιο αισθητήρα θερμοκρασίας)

Σύστημα ελέγχου θερμοκρασίας

Η χρήση ειδικών θερμοστατών παρέχει τη δυνατότητα τόσο μεμακρυσμένου ελέγχου του κλιματιστικού, αλλά δίνει και την δυνατότητα στο ίδιο το σύστημα να κρατάει τη θερμοκρασία σε επιθυμητά επίπεδα. Με αυτό τον τρόπο δεν γίνεται αλόγιστη χρήση των κλιματιστικών, βοηθώντας στην εξοικονόμηση ενέργειας.

Συστήματα για κήπους

Μέσω ειδικών αισθητήρων θα ελέγχονται αυτόματα παράμετροι που επηρεάζουν την ανάπτυξη των φυτών όπως υγρασία και pH εδάφους και θα ενημερώνει τους χρήστες για τυχόν ενέργειες που θα πρέπει να κάνει(να τοποθετήσει περισσότερο λίπασμα) και αν μπορεί να ειδοποιήσει άλλα συστήματα να προβούν σε ενέργειες(να αυξηθεί η ροή νερού από το σύστημα ποτίσματος)

Έξυπνες ηλεκτρικές συσκευές

Οι συσκευές αυτές ουσιαστικά έχουν σκοπό να αυτοματοποιήσουν και να διευκολύνουν την καθημερινή μας ζωή. Για παράδειγμα έξυπνες καφετιέρες και τοστιέρες μπορούν να έχουν έτοιμο το πρωινό μας τη στιγμή που βρισκόμαστε στην κουζίνα χωρίς την

παρέμβαση μας. Το ψυγείο και τα ράφια μπορούν να μας ενημερώνουν ή να προσθέτουν στη λίστα αγορών μας αντικείμενα τα οποία θα εξαντληθούν σύντομα.

Τεχνίτη νοημοσύνη και μηχανική μάθηση

Οι πιο πάνω εφαρμογές εκτός από τον χειροκίνητο χειρισμό τους μπορούν να εμπλουτιστούν με αλγορίθμους τεχνίτης νοημοσύνης και μηχανικής μάθησης έτσι ώστε να αναγνωρίζουν μοτίβα και να παίρνουν αποφάσεις για περεταίρω διευκόλυνση και αύξηση του βιοτικού επιπέδου. Για παράδειγμα αισθητήρας θερμοκρασίας μπορεί να αντιληφθεί ποια είναι η ιδανική για το χρήστη θερμοκρασία ανάλογα με τις καιρικές συνθήκες και ο χρήστης να μην χρειάζεται πλέον να χειρίζεται το κλιματιστικό, ο θερμοσίφωνας να αντιληφθεί πια χρονική στιγμή της μέρα ο χρήστης κάνει μπάνιο και να προνοήσει ώστε να υπάρχει ζεστό νερό χωρίς παρέμβαση από το χρήστη, όπως επίσης το προαναφερθέν σύστημα ταυτοποίησης-ασφαλείας να ανιχνεύσει ύποπτες κινήσεις ατόμου προειδοποιώντας και προλαμβάνοντας απόπειρες διάρρηξης κ.α.

Πλεονεκτήματα

Όπως έγινε αντιληπτό υπάρχουν πολλές εφαρμογές οι οποίες θα αυτοματοποιήσουν και θα βοηθήσουν στην αύξηση του βιοτικού επιπέδου. Η δυνατότητα ελέγχου διαφόρων παραμέτρων της ζωής του καθώς και η παροχή του αισθήματος ασφάλειας στο χρήστη θα παρέχουν μια καλύτερη ποιότητα ζωής όπως επίσης θα βοηθήσουν σημαντικά στην εξοικονόμηση ενέργειας.

Μειονεκτήματα

Παρόλες τις διευκολύνσεις που παρέχονται εγκυμονούν και αρκετοί κίνδυνοι. Αρχικά υπάρχει η πιθανότητα το σύστημα να προσβληθεί από hackers, οι οποίοι αποκτώντας πρόσβαση στο σύστημα μπορούν να προβούν σε κακόβουλες ενέργειες (απενεργοποίηση συναγερμού, ενεργοποίηση κλιματιστικού και φωτιστικών κ.α.). Επιπρόσθετα για τον έλεγχο των λειτουργειών απαιτείται πρόσβαση στο διαδίκτυο όπου εκτός από κακόβουλες επιθέσεις(man in the middle), εξαρτόμαστε(συνήθως) από ένα πάροχο ο οποίος λόγο του ότι οι εντολές για κάποια διεργασία έχουν σαν ενδιάμεσο σταθμό(για επεξεργασία και αποθήκευση) τα data center του παρόχου. Έτσι οι εταιρίες έχουν πρόσβαση στα προσωπικά μας δεδομένα. Τέλος, εξαιτίας του ότι οι τεχνολογίες αυτές είναι σχετικά καινούργιες και

ακόμη βρίσκονται στο στάδιο της έρευνας και ανάπτυξης έχουν υψηλό κόστος και για ένα ολοκληρωμένο σύστημα απαιτούνται μεγάλα ποσά χρημάτων.

2.3: Face Recognition System:

Η τεχνολογία αναγνώρισης προσώπου επιτρέπει την ταυτοποίηση και επαλήθευση ενός ατόμου από μια ψηφιακή εικόνα ή ενός πλαισίου βίντεο(video frame) από κάποια πηγή. Για τη διαδικασία της ταυτοποίησης χρησιμοποιούνται επιλεγμένα χαρακτηριστικά του προσώπου από μια δεδομένη εικόνα. Επιπρόσθετα μπορεί να γίνει χρήση βιομετρικής τεχνίτης νοημοσύνης η οποία αναλύοντας μοτίβα με βάση τις υφές και το σχήμα του προσώπου μπορεί να προσδιορίσει μοναδικά έναν άνθρωπο.[3][4][5] Αρχικά η τεχνολογία αυτή είχε μόνο υπολογιστικές εφαρμογές, στη συνέχεια όμως επεκτάθηκε σε διάφορους τεχνολογικούς τομείς όπως κινητές πλατφόρμες και ρομποτική. Τέτοια συστήματα χρησιμοποιούνται για έλεγχο πρόσβασης σε συστήματα ασφαλείας και ανήκουν στην ομάδα ταυτοποίησης μέσο βιομετρικών χαρακτηριστικών(π.χ. δακτυλικά αποτυπώματα ή συστήματα αναγνώρισης ίριδας ματιών).[6] Παρόλο που παρέχουν χαμηλότερη προστασία σε σχέση με άλλα βιομετρικά συστήματα, παρατηρείται ευρεία χρήση τους λόγω της ανέπαφους και μη επεμβατικής πολιτικής την οποία ακολουθεί. Επιπρόσθετα η χρήση τέτοιων συστημάτων επιτρέπει παρακολούθηση βίντεο(video surveillance), αυτοματοποιημένη καταγραφή περιστατικών και πληροφοριών όπως επίσης προηγμένη αλληλεπίδραση ανθρώπου-υπολογιστή αφού επιτρέπει έλεγχο διεργασιών μέσω νευμάτων και κινήσεων του προσώπου.

Figure 2.3.1: Face Recognition

State of the Art Techniques for face acquisition: Η διαδικασία αναγνώρισης προσώπου αποτελείται από δύο στάδια. Αρχικά εξάγουμε τα χαρακτηριστικά και επιλέγουμε ποια είναι κατάλληλα για την κατηγοριοποίηση. Στη συνέχεια χρησιμοποιώντας τα επιλεγμένα χαρακτηριστικά και αξιοποιώντας κάποιες τεχνικές κατηγοριοποιούμε τα δεδομένα. Οι σημαντικότερες εκ των οποίων είναι:

"Traditional"

Μια πρώτη προσέγγιση είναι ο προσδιορισμός των χαρακτηριστικών που διαφοροποιούνται από άνθρωπο σε άνθρωπο. Τα κυριότερα εκ των οποίων είναι η σχετική θέση, το μέγεθος ή / και το σχήμα των ματιών, της μύτης, των ζυγωματικών και της γνάθου, και στη συνέχεια να αναλυθούν μέσω αλγορίθμων για τη λήψη απόφασης, συγκρίνοντας τα με άλλες εικόνες με αντίστοιχες ιδιότητες.[7] Άλλοι αλγόριθμοι ανιχνεύουν χρήσιμα χαρακτηριστικά μέσω μιας συλλογής από εικόνες, συμπιέζοντας την εικόνα. Στη συνέχεια συγκρίνουν την επιθυμητή εικόνα με τα χαρακτηριστικά που έχουν αποθηκευτεί.[8] Λόγω της πληθώρας τρόπων κατηγοριοποίησης υπήρξαν διάφορες προσπάθειες κατάταξης των αλγορίθμων σε ομάδες. Η πρώτη προσέγγιση είναι ο διαχωρισμός τους σε γεωμετρικούς, οι οποίοι εξετάζουν διακριτά χαρακτηριστικά στις εικόνες που αναλύουν και φωτομετρικούς οι οποίοι εφαρμόζουν μια στατιστική ανάλυση των τιμών (που εξάγει από την εικόνα) και συγκρίνοντας τις τιμές αυτές με πρότυπα για εξάλειψη διακυμάνσεων. Η δεύτερη προσέγγιση είναι ο διαχωρισμός τους σε ολιστικούς οι οποίοι προσπαθούν να ταυτοποιήσουν το πρόσωπο σαν ένα ενιαίο σύνολο, ενώ οι αλγόριθμοι με βάση χαρακτηριστικά(feature-based models) υποδιαιρεί την εικόνα σε μικρότερα κομμάτια αναλύοντας το καθένα ξεχωριστά, λαμβάνοντας υπόψη και τη χωρική διάταξη του κομματιού σε σχέση με τα υπόλοιπα. Οι κύριες αρχές που χρησιμοποιούν οι περισσότεροι αλγόριθμοι συμπεριλαμβάνουν eigenfaces[9], linear discriminant analysis[10], elastic bunch graph matching χρησιμοποιώντας Fisherface algorithm[11], το κρυφό μοντέλο

Markov[12], multilinear subspace learning[13] χρησιμοποιώντας tensor representation[14] και neuronal motivated dynamic link matching[15].

"Three-Dimensional recognition" [16]

Η τρισδιάστατη τεχνική αναγνώρισης προσώπου, είναι μια προσέγγιση η οποία κάνει χρήση 3D sensors για να καταγράψει πληροφορίες για το σχήμα του προσώπου. Αυτές οι πληροφορίες όπως και πριν χρησιμοποιούνται για εντοπισμό διακριτικών χαρακτηριστικών στην επιφάνεια ενός προσώπου, όπως το περίγραμμα των ματιών, τη μύτη και το πηγούνι. Το πλεονέκτημα χρήσης τρισδιάστατων αισθητήρων για εντοπισμό χαρακτηριστικών πλεονεκτεί στον τομέα φωτισμού αφού δεν επηρεάζεται από αλλαγές στον φωτισμό. Επίσης παρέχει την δυνατότητα αναγνώρισης προσώπου υπό γωνία. Μεγάλο ενδιαφέρον εκδηλώνεται και στο ερευνητικό πεδίο ανάπτυξης καλύτερων 3D αισθητήρων οι οποίοι δίνουν πιο ακριβή δεδομένα. Γενικότερα τα τρισδιάστατα σημεία δεδομένων από ένα πρόσωπο βελτιώνουν σε μεγάλο βαθμό την ακρίβεια της αναγνώρισης προσώπου, αφού δίνουμε στο σύστημα περισσότερα δεδομένα με μεγαλύτερη σημαντικότητα. Παρόλα αυτά οι αισθητήρες αυτοί έχουν αυξημένο κόστος. Μια μέθοδος η οποία προσεγγίζει τη λειτουργία αυτών των αισθητήρων είναι η χρήση τριών καμερών που δείχνουν σε διαφορετικές γωνίες. μια κάμερα θα δείχνει προς τα εμπρός του θέματος, η δεύτερη προς τα πλάγια και η τρίτη σε γωνία. Όλες αυτές οι κάμερες θα λειτουργούν μαζί, ώστε να παρακολουθεί το πρόσωπο ενός θέματος σε πραγματικό χρόνο και να μπορεί να εντοπίζει και να αναγνωρίζει το πρόσωπο.[17]

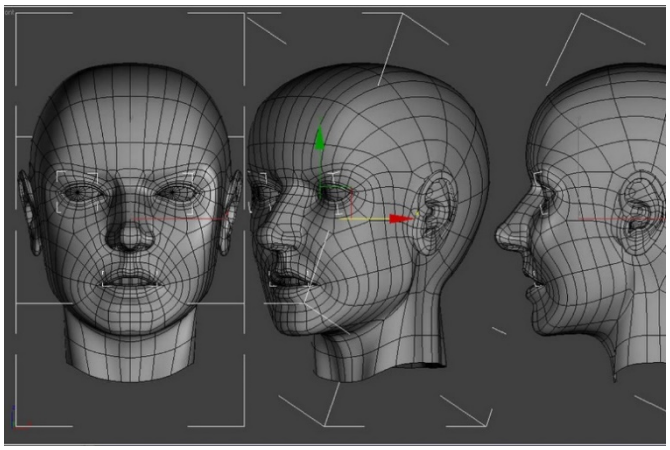


Figure 2.3.2: 3-D Face Recognition

“Thermal cameras”

Η χρήση θερμικών καμερών είναι ακόμη μια εξιδεικευμένη τεχνολογία, η οποία επιτρέπει ανίχνευση προσώπου αγνοώντας παράλληλα τυχόν αντικείμενα(γυαλιά, καπέλα ή μακιγιάζ) που μπορεί να φέρει ο άνθρωπος.[18] Επιπρόσθετα δεν έχουν την ανάγκη επιπλέον φωτισμού για συνθήκες χαμηλής ορατότητας που έχουν οι συμβατικές κάμερες.[19] Ταυτόχρονα δεν υπάρχει βάση δεδομένων για τέτοιου είδους φωτογραφίες, και υπάρχει επαρκής έρευνα στο συγκεκριμένο πεδίο αν και τα αποτελέσματα τη δεδομένη στιγμή είναι αρκετά καλά.

Figure 2.3.3: Thermal Face Recognition

Applications: Η αναγνώριση προσώπου βρίσκει χρήση σε αρκετές εφαρμογές του μοντέρνου κόσμου.

Mobile platforms

“Social media”

Οι πλατφόρμες κοινωνικών μέσων έχουν υιοθετήσει δυνατότητες αναγνώρισης προσώπου για να διαφοροποιήσουν τις λειτουργίες τους προκειμένου να προσελκύσουν μια ευρύτερη βάση χρηστών εν μέσω σκληρού ανταγωνισμού από διαφορετικές εφαρμογές. Οι κινούμενοι φακοί οι οποίοι χρησιμοποίησαν τεχνολογία αναγνώρισης προσώπου, έφεραν επανάσταση και επαναπροσδιόρισαν το selfie, επιτρέποντας στους χρήστες να προσθέσουν φίλτρα για να αλλάξουν τον τρόπο εμφάνισής τους.

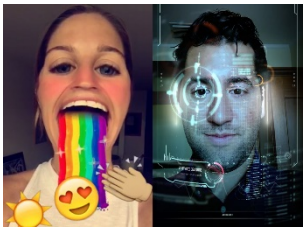


Figure 2.3.4: Social Media Application

“ID Verification”

Η αναδυόμενη χρήση της αναγνώρισης προσώπου είναι στη χρήση υπηρεσιών επαλήθευσης ταυτότητας. Πολλές εταιρείες εργάζονται τώρα στην αγορά για να παρέχουν αυτές τις υπηρεσίες σε τράπεζες, ICO και άλλες ηλεκτρονικές επιχειρήσεις.[20] Η τεχνολογία αυτή πρέπει να είναι σε θέση να αναγνωρίζει αλλαγές στην εμφάνιση ενός χρήστη και να λειτουργεί με καπέλα, κασκόλ, γυαλιά και πολλά γυαλιά ηλίου, γένια και μακιγιάζ. Επιπρόσθετα θα πρέπει να ταυτοποιεί και στο σκοτάδι χωρίς εξωτερική πηγή φωτός. Υλοποιήσεις τέτοιας εφαρμογής κάνουν χρήση ενός ειδικού υπέρυθρου φλας που ρίχνει αόρατο υπέρυθρο φως στο πρόσωπο του χρήστη για να διαβάσει σωστά τα σημεία του προσώπου του.[21][22] Πρωτεργάτης τέτοιων εφαρμογών είναι η εταιρία “Apple” η οποία υλοποίησε την πιο πάνω λογική για να αντικαταστήσει την βιομετρική ταυτοποίηση μέσω δακτυλικών αποτυπωμάτων.

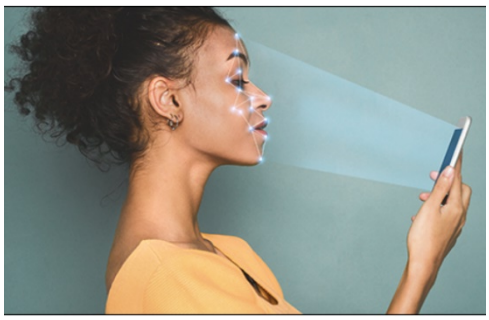


Figure 2.3.5: ID Verification

Security Services: Πάρα πολλές χώρες ανά το παγκόσμιο έχουν αναπτύξει εφαρμογές για να εκμεταλλευτούν εφαρμογές σχετικά με αυτό τον τομέα, μερικές ενδιαφέρουσες προσεγγίσεις αναφέρονται πιο κάτω. Στην Αυστραλία η Αυστραλιανή Δύναμη Συνόρων και η Τελωνειακή Υπηρεσία της Νέας Ζηλανδίας, έχουν δημιουργήσει ένα αυτοματοποιημένο σύστημα επεξεργασίας συνόρων, το οποίο χρησιμοποιεί αναγνώριση προσώπου συγκρίνοντας το πρόσωπο του ταξιδιώτη με τα δεδομένα στο μικροτσίπ του ηλεκτρονικού διαβατηρίου. [23] Παρόμοια πολιτική εφαρμόζει και ο Καναδάς στους χώρους των αεροδρομίων του συγκρίνοντας το πρόσωπο με την φωτογραφία διαβατηρίου του ατόμου.[24] Στο αεροδρόμιο του Παναμά ένα σύστημα παρακολούθησης σε ολόκληρο το αεροδρόμιο χρησιμοποιεί εκατοντάδες κάμερες αναγνώρισης ζωντανών προσώπων για εντοπισμών καταζητούμενων. Η Κίνα και Ηνωμένες Πολιτείες Αμερικής αδιαμφισβήτητα

τηρούν ίσως τις πιο αυστηρές πολιτικές σε αυτό το θέμα με την κυβέρνηση της Αμερικής να κατέχει ένα από τα μεγαλύτερα συστήματα αναγνώρισης προσώπου στον κόσμο με βάση δεδομένων 117 εκατομμυρίων Αμερικανών ενηλίκων, με φωτογραφίες που συνήθως προέρχονται από φωτογραφίες άδειας οδήγησης.[25] Το FBI έχει επίσης θεσπίσει το πρόγραμμα αναγνώρισης επόμενης γενιάς για να συμπεριλάβει την αναγνώριση προσώπου, καθώς και πιο παραδοσιακά βιομετρικά στοιχεία όπως δακτυλικά αποτυπώματα και σαρώσεις ίριδας, τα οποία μπορούν να τραβήξουν τόσο από ποινικές όσο και από αστικές βάσεις δεδομένων.[26] Η Κίνα έχει αναπτύξει τεχνολογία αναγνώρισης προσώπου και τεχνητής νοημοσύνης στο Xinjiang.[27] Η τεχνολογία αυτή επιτρέπει την ταυτοποίηση ατόμων που φορούν χειρουργικές μάσκες ή μάσκες σκόνης, χρησιμοποιώντας αποκλειστικά μάτια και μέτωπα.

Figure 2.3.6: Security Services

Advantages over Other Biometric Systems

Συγκριτικά με τα υπόλοιπα βιομετρικά συστήματα το βασικότερο πλεονέκτημα ενός συστήματος αναγνώρισης προσώπου είναι η ικανότητα του για μαζική ταυτοποίηση ατόμων. Επιπρόσθετα δεν απαιτείται η συναίνεση από τους ίδιους για την διαδικασία της ταυτοποίησης. Σωστές υλοποιήσεις τέτοιων συστημάτων βρίσκονται σε δημόσιους χώρους και επιτελούν την εργασία αυτή χωρίς να γίνονται αντιληπτά από τους περαστικούς [28]

Disadvantages over other biometric systems

Ωστόσο συγκρινόμενο με άλλες βιομετρικές τεχνικές, η αναγνώριση προσώπου είναι λιγότερο αξιόπιστη και αποτελεσματική. Ο κυριότερος λόγος είναι ότι επηρεάζεται από πολλούς ευμετάβλητους παράγοντες όπως ο φωτισμός, η έκφραση, η στάση κατά τη διαδικασία λήψης του προσώπου. Ως άμεση συνέπια, η αναγνώριση προσώπου μεταξύ όλων των βιομετρικών συστημάτων, έχει τα υψηλότερα ποσοστά ψευδούς αποδοχής(false positive) και απόρριψης(false negative), θέτοντας αρκετά ερωτηματικά στον ερευνητικό τομέα εάν είναι άξιο εμπιστοσύνης. Επιπρόσθετα παρόλη την ικανότητα αναγνώρισης σε

υψηλής ανάλυσης σε μετωπικές φωτογραφίες, όσο χαμηλώνει η ανάλυση και αλλάζει η γωνία λήψης (δηλαδή όσο πλησιάζουμε σε φωτογραφίες profile) μειώνεται η ικανότητα και η αξιοπιστία του αλγορίθμου.

Figure 2.3.7: False Rejection and False Acceptance Rate

Anti-Facial Recognition Systems

Αρκετοί ερευνητές και εταιρίες προσπαθούν να επινοήσουν τρόπους έτσι ώστε να δυσκολεύουν ή να αδρανοποιούν πλήρως τέτοια συστήματα. Η πρώτη προσέγγιση επινοήθηκε από Ιάπωνες ερευνητές του Εθνικού Ινστιτούτου Πληροφορικής. Δημιούργησαν γυαλιά τα οποία χρησιμοποιούν σχεδόν υπέρυθρο φως για να κάνουν το πρόσωπο κάτω από αυτό μη αναγνωρίσιμο για να αναγνωρίσει το λογισμικό. Η λειτουργία τους στηρίζεται στη διαταραχή του φωτός στην περιοχή του προσώπου εμποδίζοντας τα λογισμικά αναγνώρισης να το ανιχνεύσουν με επιτυχία.[29][30][31][32] Η δεύτερη προσέγγισή είναι η χρήση μοτίβων μακιγιάζ, έτσι ώστε να εμποδίζουν τους αλγόριθμους που χρησιμοποιούνται για την ανίχνευση ενός προσώπου, γνωστός ως εκθαμβωτική όραση του υπολογιστή.[33][34]

Figure 2.3.8: Anti-Facial Recognition Systems

Controversies

Privacy violations

Οργανισμοί σχετικοί με τα δικαιώματα των πολιτών εκφράζουν ανησυχία ότι η ιδιωτική ζωή διακυβεύεται με τη χρήση τεχνολογιών παρακολούθησης. Ορισμένοι φοβούνται ότι θα μπορούσε να οδηγήσει σε μια «κοινωνία συνολικής επιτήρησης», με την κυβέρνηση και άλλες αρχές να έχουν τη δυνατότητα να γνωρίζουν τον τόπο και τις δραστηριότητες όλων των πολιτών όλο το 24ωρο. Υπάρχουν αρκετά παραδείγματα εταιριών και οργανισμών(κυβερνητικών και μη) οι οποίοι έχουν καταχραστεί δικαιώματα της ανθρώπινης ελευθέριας στο βωμό του κέρδους.[35][36] Παραδείγματα τέτοιων ενεργειών είναι η χρήση αναγνώρισης προσώπου για εύρεση άλλων προσωπικών δεδομένων του ατόμου όπως φωτογραφίες στα μέσα κοινωνικής δικτύωσης, συμπεριφορά στο Διαδίκτυο, μοτίβα ταξιδιού κ.λ.π. Επιπλέον, τα άτομα έχουν περιορισμένη ικανότητα αποφυγής ή αναστολής της αναγνώρισης προσώπου, εκτός εάν κρύβουν τα πρόσωπά τους και το χειρότερο είναι πως οι καταναλωτές ενδέχεται να μην καταλαβαίνουν ή να γνωρίζουν για ποιο λόγο χρησιμοποιούνται τα δεδομένα τους, γεγονός που τους αρνείται τη δυνατότητα να συναινέσουν στον τρόπο με τον οποίο κοινοποιούνται τα προσωπικά τους στοιχεία.[37][38] Αυξημένη ανησυχία από τους καταναλωτές παρατηρείται για εταιρίες που χρησιμοποιούν την τεχνολογία αναγνώρισης προσώπου ως μέσο ταυτοποίησης στα κινητά τηλέφωνα. Πιο συγκεκριμένα ανησυχούν για τυχών χρήση των δεδομένων τους για χρήση μαζικής παρακολούθησης του κοινού. Σχετικοί οργανισμοί αναφέρουν εφόσον ζούμε σε μια ελεύθερη κοινωνία, θα πρέπει να είμαστε σε θέση να βγαίνουμε στο κοινό χωρίς να φοβόμαστε να ταυτοποιηθούμε και να παρακολουθούμαστε. Οι άνθρωποι ανησυχούν ότι με την αυξανόμενη επικράτηση της αναγνώρισης προσώπου, θα αρχίσουν να χάνουν την ανωνυμία τους.

Imperfect Technology in Law Enforcement

Πολλές κυβερνήσεις ανά το παγκόσμιο έχουν ενσωματώσει λογισμικό αναγνώρισης προσώπου στο νομικό πλαίσιο της κάθε χώρας. Συγκεκριμένα οι Κινεζικές αρχές εντόπισαν και συνέλαβαν χρησιμοποιώντας ένα τέτοιο σύστημα είκοσι πέντε καταζητούμενους ο ένας εκ των οποίων είχε διαφύγει από τις αρχές για δέκα χρόνια. Άλλες μελέτες δείχνουν αδυναμία ακριβείας εντοπισμού για άτομα με σκουρόχρωμο χρώμα προσώπου. Επιπρόσθετα τέτοια συστήματα έχουν μεγαλύτερες δυσκολίες για ταυτοποίηση

γυναικών παρά αντρών. Μετά από μελέτες διαφόρων ερευνητών σε τρία διαφορετικά εμπορικά συστήματα διαπιστώθηκε σφάλμα ακρίβειας της τάξης του 23,8% έως 36%, ενώ για τους άνδρες με ανοιχτόχρωμο δέρμα ήταν μεταξύ 0,0 και 1,6%. Τα συνολικά ποσοστά ακρίβειας για τον εντοπισμό ανδρών (91,9%) ήταν υψηλότερα από ό, τι για τις γυναίκες (79,4%), και κανένα από τα συστήματα δεν ταιριάζει σε μια μη δυαδική κατανόηση του φύλου.[39][40][41] Αυτό έχει αμφιταλαντευόμενα συμπεράσματα σχετικά με την αξιοπιστία τέτοιων συστημάτων στη λήψη αποφάσεων και αν είναι πρέπων να χρησιμοποιούνται. Οι ειδικοί εκφράζουν τις ανησυχίες τους ότι η τεχνολογία αυτή μπορεί πραγματικά να βλάπτει τις κοινότητες που η αστυνομία ισχυρίζεται ότι προσπαθούν να προστατεύσουν.[42][43]

2.4: Hardware

Sipeed MaixyPy M1W Dock

Για την λήψη της φωτογραφίας και την αλληλεπίδραση με τον χρήστη γίνεται χρήση του MaixyPy M1W Dock της Sipeed. Το kit αυτό είναι εξοπλισμένο με το Kendryte K210 Processing Unit (a 64-bit dual-core RISC-V CPU with hardware FPU, FFT, sha256 and convolution accelerator) σχεδιασμένο για AIoT (AI+IOT) εφαρμογές. Επιπρόσθετα διαθέτει μια οθόνη LCD 2.4 inches με ανάλυση 320x240 pixels. Διαθέτει επίσης 2MP camera για την λήψη φωτογραφιών και βίντεο. Η εσωτερική του μνήμη είναι σχετικά μικρή, διαθέτει θύρα επέκτασης μέσω micro SD κάρτας, όλο το kit τροφοδοτείται μέσω θύρας USB-C ενώ υποστηρίζει σύνδεση στο διαδίκτυο μέσω εξωτερικής WIFI κεραίας. Τα πιο πάνω περιλαμβάνονται στη συσκευασία κατά την αγορά του kit, παρόλα αυτά παρέχει 40 pins για σύνδεση πιο εξειδικευμένων αισθητήρων (π.χ. θερμοκρασίας υγρασίας κ.λ.π). Για τον προγραμματισμό του χρησιμοποιεί τη γλώσσα προγραμματισμού MicroPython η οποία είναι μια παραλλαγή της γλώσσας Python 3, περιλαμβάνοντας ένα μικρό υποσύνολο της τυπικής βιβλιοθήκης Python και είναι βελτιστοποιημένη για εκτέλεση σε μικροελεγκτές και σε περιορισμένα περιβάλλοντα.

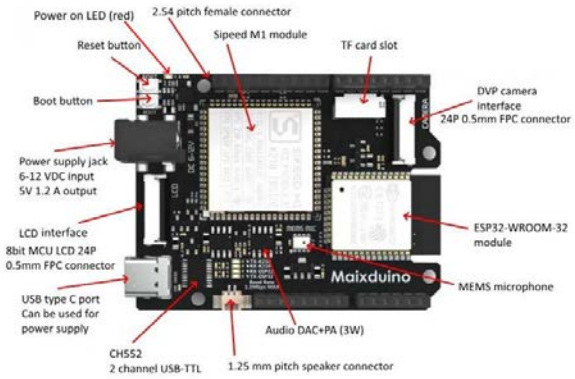


Figure 2.4.1: MaixyPy Main Components

2.5: Software

Take the Picture and Respond

kFlash_Gui

Αυτό το λογισμικό χρησιμοποιείται για εισαγωγή έτοιμων modules καθώς και του IDE του MaixyPy το οποίο επιτρέπει τον προγραμματισμό του Hardware και αναλύεται πάρα κάτω.

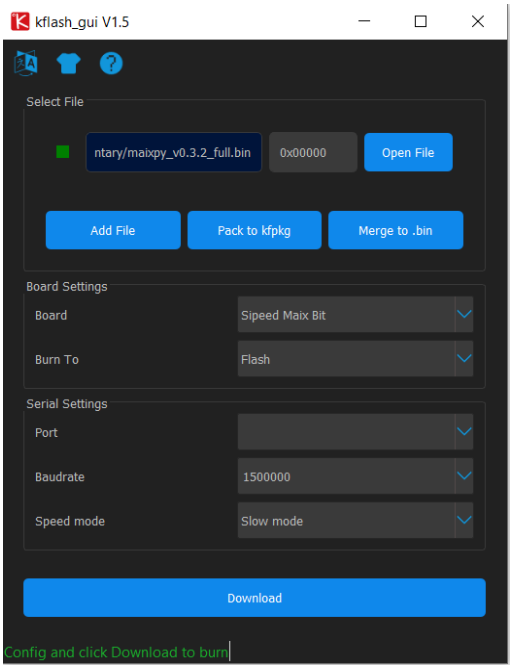


Figure 2.5.1: Kflash Interface

MaixyPy_IDE

Το IDE χρησιμοποιείται κυρίως για τον προγραμματισμό του Hardware, έναντι του notepad επειδή παρέχει και άλλες δυνατότητες όπως άμεση προβολή στην οθόνη την λαμβάνει η κάμερα, καθώς και το ιστόγραμμα (histogram) της εικόνας σε διάφορα φάσματα φωτός όπως RGB, Grayscale, LAB, YUV. Επιπρόσθετα παρέχει επιπλέον εργαλεία για machine vision και video για περεταίρω επεξεργασία.

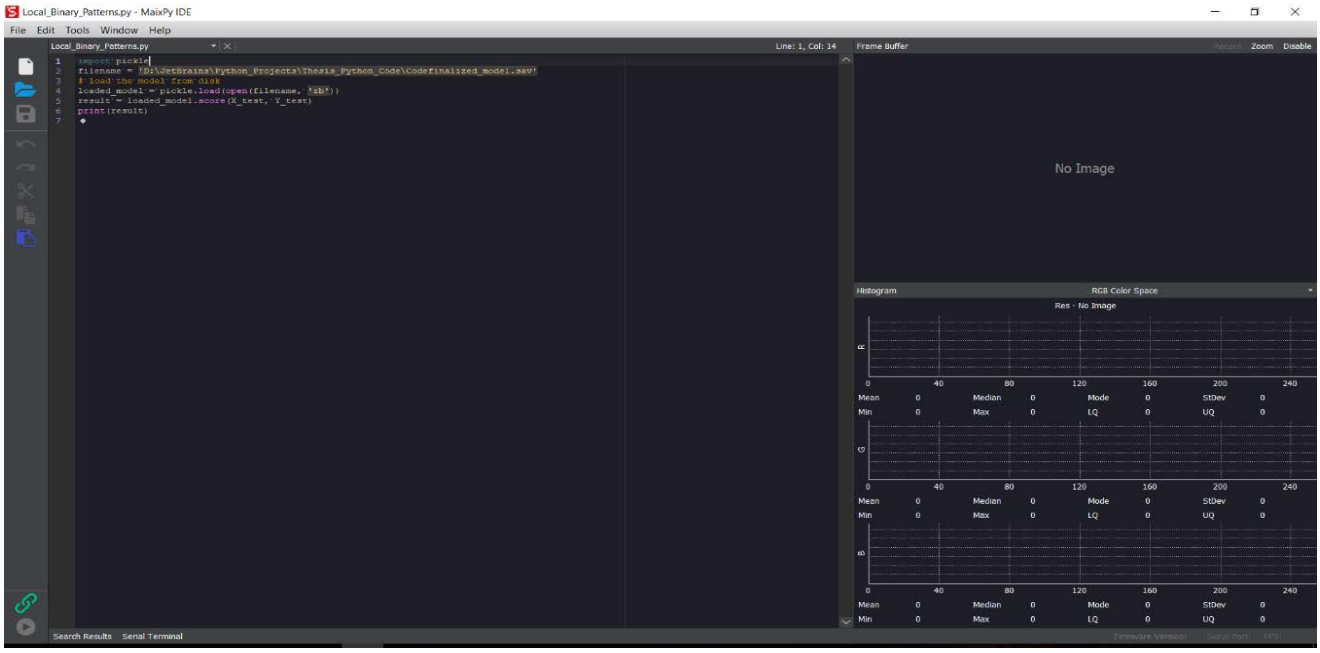


Figure 2.5.2: MaixyPy IDLE Interface

MicroPython

Η MicroPython είναι η γλώσσα με την οποία μπορούμε να αλληλοεπιδρούμε και να ελέγχουμε τους αισθητήρες του kit. Αποτελεί μια λιτή και αποτελεσματική εφαρμογή της γλώσσας προγραμματισμού Python 3 που περιλαμβάνει ένα μικρό υποσύνολο της τυπικής βιβλιοθήκης Python και είναι βελτιστοποιημένη για εκτέλεση σε μικροελεγκτές και σε περιορισμένα περιβάλλοντα. Η MicroPython στοχεύει να είναι όσο το δυνατόν πιο συμβατή με τη Python για να επιτρέπει μεταφορά κώδικα με ευκολία από την επιφάνεια εργασίας σε έναν μικροελεγκτή ή ενσωματωμένο σύστημα.

Data Manipulation

Python

Η Python είναι μια interpreted, high-level, general-purpose programming language. Οι γλωσσικές δομές και η αντικειμενοστραφή προσέγγιση στοχεύουν να βοηθήσουν τους προγραμματιστές να γράψουν σαφή, λογικό κώδικα για μικρά και μεγάλα έργα. Οι interpreters Python είναι διαθέσιμοι για πολλά λειτουργικά συστήματα. Μια παγκόσμια κοινότητα προγραμματιστών αναπτύσσει και διατηρεί το CPython, μια εφαρμογή αναφοράς ανοιχτού κώδικα. Ένας μη κερδοσκοπικός οργανισμός, το Python Software Foundation, διαχειρίζεται και κατευθύνει πόρους για την ανάπτυξη Python και CPython.

2.6: Algorithms Used in Thesis

Feature Extraction: Για την εξαγωγή των χαρακτηριστικών από την εικόνα χρησιμοποιήθηκε ο αλγόριθμος Local Binary Patterns, αφού μετά από μελέτη σχετικών βιβλιογραφιών θα επέφερε τα καλύτερα αποτελέσματα για τις συνθήκες και τα δεδομένα με τα οποία θα έχουμε.[44]

"Local Binary Patterns"

Ο αλγόριθμος υλοποιεί μια απλή αλλά αποτελεσματική πολιτική για εξαγωγή των χαρακτηριστικών συγκρίνοντας τις τιμές σε μια γειτονία από pixels σε σχέση με το κέντρο της γειτονίας. Η χρήση μιας τέτοιας πολιτικής επιφέρει πολλά πλεονεκτήματα σε σχέση με άλλους αλγορίθμους. Το κυριότερο πλεονέκτημα είναι ότι χρειάζεται ελάχιστο χρόνο για την επεξεργασία της εικόνας και την εξαγωγή των χαρακτηριστικών. Επιπλέον αφού συγκρίνει γειτονικά pixels με το κεντρικό επηρεάζεται ελάχιστα από τις συνθήκες φωτισμού όταν ο φωτισμός είναι παράλληλος με το πρόσωπο. Παρόλα αυτά εάν το φως έχει μεγάλη απόκλιση από τον οριζόντιο άξονα ως προς το πρόσωπο, ίσως δώσει λιγότερα χρήσιμα χαρακτηριστικά.[45][46][47]

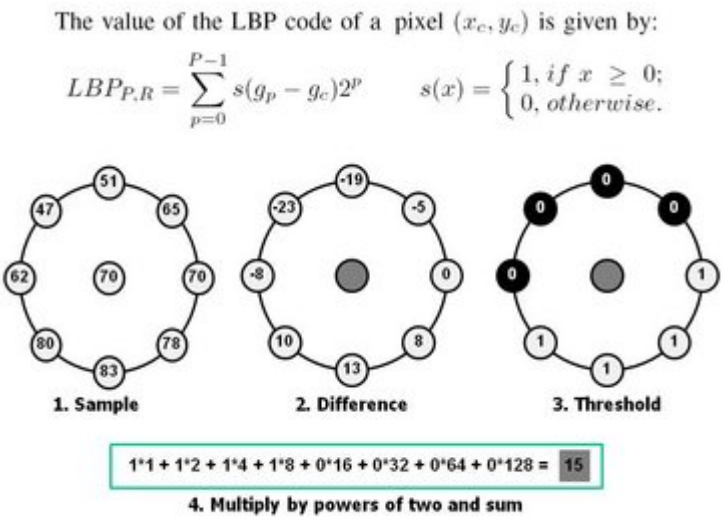


Figure 2.6.1: LBP computation

Feature Selection and Validation: Για την εξαγωγή των χαρακτηριστικών τα οποία θα ωφελήσουν περισσότερο τον αλγόριθμο να κατηγοριοποιήσει σωστά τις φωτογραφίες χρησιμοποιήθηκαν οι ακόλουθοι αλγόριθμοι. Ο λόγος χρήσης των συγκεκριμένων

αλγορίθμων είναι ότι καλούμαστε να τα επιλύσουμε ένα πρόβλημα κατηγοριοποίησης(Classification)[48] και όχι ομαδοποίησης(Clustering)[49], επειδή τα δεδομένα (εικόνες) καλούμαστε να επιλέξουμε εμείς αν επιτρέπεται ή όχι η πρόσβαση τους. Επιπρόσθετα οι συγκεκριμένοι αλγόριθμοι λειτουργούν εξίσου καλά ανεξάρτητα με την ποσότητα των δεδομένων εκπαίδευσης τους.[50]

"K Nearest Neighbors"

Ο K Nearest Neighbors(KNN) χρησιμοποιείται για την αναγνώριση προτύπων(στην προκειμένη περίπτωση χαρακτηριστικών προσώπου) και αποτελεί μια μη παραμετρική μέθοδο. Ταξινομεί το αντικείμενο έτσι ώστε να αντιστοιχεί στην τάξη πιο κοινή μεταξύ των k πλησιέστερων γειτόνων του.[51][52]

"Stochastic Gradient Descent"

Ο Stochastic Gradient Descent(SGD) αποτελεί μια βελτιωμένη έκδοση του αλγορίθμου Gradient Descent(GD) και είναι μια επαναληπτική μέθοδος για εύρεση βέλτιστων τιμών των κλάσεων. Προσφέρει εξαιρετικά αποτελέσματα ειδικά σε εφαρμογές μεγάλων δεδομένων, αφού μειώνει τον υπολογιστικό φόρτο, επιτυγχάνοντας ταχύτερες επαναλήψεις παρέχοντας όμως παράλληλα ελαφρώς χαμηλότερο ρυθμό σύγκλισης. [53][54]

"Support Vector Classification"

Ο Support Vector Classification(SVC) ανήκει στην κλάση των Support Vector Machines(SVM). Τέτοιου είδους αλγόριθμοι χρησιμοποιούνται για να αναλύουν δεδομένα που χρησιμοποιούνται για την ταξινόμηση και την ανάλυση παλινδρόμησης. Ένα μοντέλο SVM είναι μια αναπαράσταση των παραδειγμάτων ως σημεία στο διάστημα, χαρτογραφημένα έτσι ώστε τα παραδείγματα των ξεχωριστών κατηγοριών να διαιρούνται με ένα σαφές κενό που είναι όσο το δυνατόν ευρύτερο. Στη συνέχεια, νέα παραδείγματα χαρτογραφούνται στον ίδιο χώρο και προβλέπεται να ανήκουν σε μια κατηγορία με βάση τα χαρακτηριστικά που διαθέτουν.[55][56]

Κεφάλαιο 3: **Μεθοδολογία**

3.1: Hardware

Στόχος είναι να επιλεγεί ένα σύστημα το οποίο θα λειτουργεί αυτόνομα όλη την μέρα. Επιπλέον το σύστημα πρέπει να έχει χαμηλό κόστος έτσι ώστε να είναι προσιτό στην αγορά του. Για την υλοποίηση επιλέξαμε το MaixyPy M1W Dock της Sipeed, αφού έχει χαμηλό κόστος, ενώ συμπεριλαμβάνει εκτός των άλλων μια οθόνη για την αλληλεπίδραση του με τον χρήστη.

Figure 3.1.1: MaixyPy Kit

Sipeed MaixyPy M1W Dock

Για την υλοποίηση του συστήματος λήψης φωτογραφιών και την αλληλεπίδραση με το χρήστη χρησιμοποιήθηκε το MaixyPy M1W Dock της Sipeed. Αποτελεί ένα εξαιρετικό kit το οποίο περιλαμβάνει αρκετά περιφερικά και έναν ισχυρό επεξεργαστή ο οποίος έχει παράλληλα χαμηλή κατανάλωση. Οι φωτογραφίες που θα χρησιμοποιηθούν για την εκπαίδευση του συστήματος λήφθηκαν όλες στον ίδιο χώρο με κλειστά παράθυρα και πόρτες, με τεχνητό φως έτσι ώστε όλες οι φωτογραφίες να έχουν τις ίδιες πηγές φωτός και να φωτίζονται από τις ίδιες κατευθύνσεις το ίδιο. Το dock σταθεροποιήθηκε και όλες οι φωτογραφίες πάρθηκαν από την ίδια απόσταση. Τέλος, αφού χρησιμοποιήθηκε η ίδια κάμερα οι φωτογραφίες είχαν όλες την ίδια ποιότητα εικόνας και τις ίδιες αναλογίες. Για κάθε άτομο ξεχωριστά πάρθηκαν διαφόρου τύπου φωτογραφίες στην προσπάθεια να προσομοιωθούν οι συνθήκες φωτισμού, η γωνία με την οποία θα κοιτάζουν, τον αισθητήρα και την πιθανότητα να έχουν κάποιο αξεσουάρ(π.χ. γυαλιά οράσεως). Συγκεκριμένα πάρθηκαν τρείς φωτογραφίες σε συνθήκες ικανοποιητικού φωτισμού αριστερά, ευθεία και

δεξιά. Στη συνέχεια μειώθηκε ο φωτισμός στο ελάχιστο και επαναλάβαμε την ίδια διαδικασία. Τέλος, οι δύο προηγούμενες προσεγγίσεις επαναλήφθηκαν με τη διαφορά ότι το άτομο φορούσε γυαλιά οράσεως. Έτσι, συνολικά για κάθε άτομο συλλέξαμε δώδεκα φωτογραφίες και για τα δεδομένα εκπαίδευσης χρησιμοποιήθηκαν τέσσερα άτομα(δύο άντρες και δύο γυναίκες). Για τα δεδομένα ελέγχου-επαλήθευσης δεν τηρήθηκε η διατήρηση σταθερών συνθηκών για να ελέγξουμε την ικανότητα του συστήματος να αναγνωρίζει και να ταυτοποιεί εικόνες με περισσότερο θόρυβο. Να σημειωθεί χρησιμοποιήθηκαν έξι άτομα αφού έγινε εισαγωγή δύο καινούργιων προσώπων για να παρατηρήσουμε την συμπεριφορά του για άτομα τα οποία δεν έχουν ακόμα καταγραφεί. Επιπρόσθετα έγινε και προσπάθεια προσομοίωσης κακόβουλων επιθέσεων. Σε ένα υποθετικό σενάριο όπου επιτήδειοι ανακαλύπτουν τα πρόσωπα που έχουν πρόσβαση στο σύστημα και επιχειρούν να το παραβιάσουν. Πρόθεση μας είναι η υλοποίηση του χειρότερου δυνατού σεναρίου όπου ο hacker έχει στη κατοχή του την ίδια φωτογραφία που χρησιμοποίησε ο χρήστης για να εισάγει την ταυτότητα του στο σύστημα, μέσο των δεδομένων εκπαίδευσης. Έτσι στα δεδομένα ελέγχου-επαλήθευσης εκτυπώθηκε η φωτογραφία σε χαρτί και αποθηκεύτηκε στο κινητό, στη συνέχεια εκτέθηκαν στην κάμερα για να γίνει προσομοίωση της προσπάθειας παράβασης του συστήματος με αυτό το τρόπο.

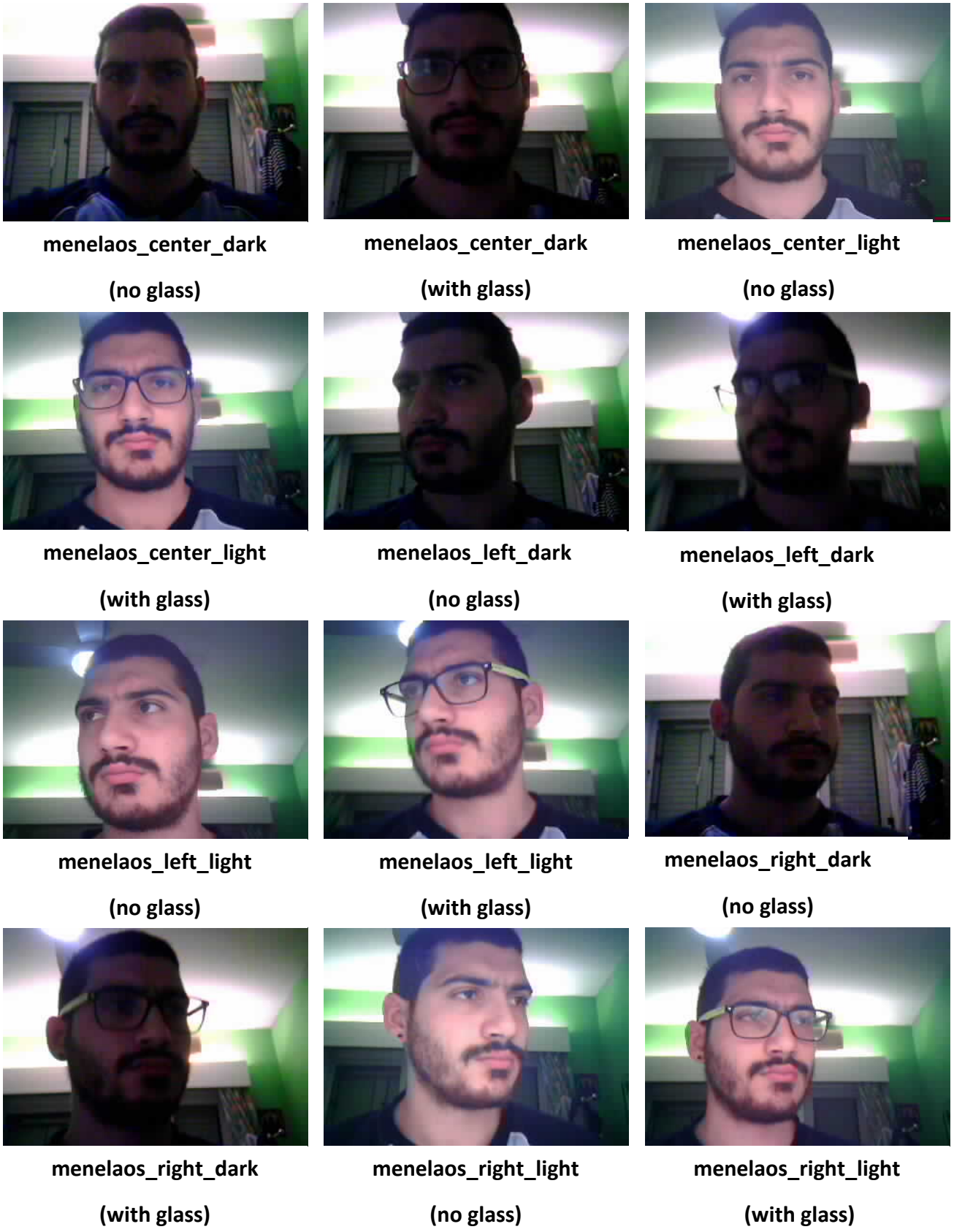


Figure 3.1.1: Training Data Sample

3.2: Software

Take the Picture and Respond

kFlash_Gui

Η εταιρία Sipeed παρέχει ένα repository στο οποίο η ίδια τοποθετεί αναβαθμίσεις στο λογισμικό του hardware καθώς και χρήσιμα modules τα οποία εκτελούν συγκεκριμένες εργασίες που δεν είναι σε θέση οι χρήστες να ορίσουν, κυρίως στην επικοινωνία μεταξύ chipset και περιφερικών συστημάτων-αισθητήρων. Για να είναι σε θέση να λειτουργήσει το hardware θα πρέπει μέσω το εργαλείου αυτού να γίνει "burned" το λειτουργικό σύστημα που χρησιμοποιεί στην μνήμη "flash". Επιπρόσθετα επιτρέπει και την χρήση IDE περιβάλλοντος εργασίας το οποίο παρέχει άμεσα επιπλέον πληροφορίες στον προγραμματιστή τις οποίες δεν μπορεί να τις παρέχει ο προγραμματισμός μέσω ενός shell.

MaixyPy_IDE

Το IDE το οποίο παρέχεται από την εταιρία μέσα από το repository, παρέχει ένα γραφικό περιβάλλον το οποίο εκτός από τις επιπλέον πληροφορίες που παρέχει, διευκολύνει την ανάπτυξη λογισμικού σε σύγκριση με την ανάπτυξη κώδικα σε shell. Αφού γίνουν οι απαραίτητες προεργασίες εγκατάστασης από το λογισμικό kFlash_Gui προχώρησα στην εξοικείωση του γραφικού περιβάλλοντος και της γλώσσας προγραμματισμού MicroPython έγινε η συγγραφή προγραμμάτων για την επικοινωνία μεταξύ chipset-sensor και περιφερικών συστημάτων, όπως και την επεξεργασία και αποθήκευση των δεδομένων. Στην συνέχεια δημιουργήθηκε το πρόγραμμα το οποίο είναι αδρανές περιμένοντας να εντοπίσει κάποιο πρόσωπο("Find_Face_and_Take_Picture_SD.py"). Μόλις εντοπίσει το πρόσωπο προβάλει ένα τετράγωνο πλαίσιο γύρω από το πρόσωπο του χρήστη έτσι ώστε να τον πληροφορεί ότι τον εντόπισε. Μόλις ενημερώσει τον χρήστη ότι εντοπίστηκε το πρόσωπο του, τον ενημερώνει να παραμείνει ακίνητος κοιτώντας ευθεία. Μετά το πέρας κάποιων δευτερολέπτων (μεταβλητή η οποία αλλάζει μέσω του προγράμματος) τον βγάζει φωτογραφία και την αποθηκεύει στον προεπιλεγμένο χώρο αποθήκευσης(Micro Sd ή την εσωτερική Flash Memory). Όταν αποθηκευτεί ο επιθυμητός όγκος φωτογραφιών εκπαίδευσης με τις κατάλληλες συνθήκες όπως περιγράφεται στην ενότητα 3.1: Hardware(Figure:Training Data Sample) οι φωτογραφίες μεταφέρονται στον υπολογιστή για επεξεργασία, εξαγωγή χαρακτηριστικών και δημιουργία του μοντέλου ταυτοποίησης. Τέλος αναπτύχθηκε πρόγραμμα ("demoAuthentication.py") το οποίο είναι αδρανές

περιμένοντας να εντοπίσει κάποιο πρόσωπο. Μόλις εντοπίσει το πρόσωπο προβάλει ένα τετράγωνο πλαίσιο γύρω από το πρόσωπο του χρήστη έτσι ώστε να τον ενημερώσει ότι τον εντόπισε. Μόλις ενημερώσει τον χρήστη ότι εντοπίστηκε το πρόσωπο του, τον ενημερώνει να παραμείνει ακίνητος κοιτώντας ευθεία. Μετά το πέρας κάποιων δευτερολέπτων (μεταβλητή η οποία αλλάζει μέσω του προγράμματος) τον βγάζει φωτογραφία και περιμένει το αποτέλεσμα της ταυτοποίησης μέσω κλίσης κάποιας συνάρτησης. Μόλις λάβει το αποτέλεσμα ενημερώνει τον χρήστη εάν του επιτρέπεται ή αν του απαγορεύεται η είσοδος με ένα μήνυμα στην οθόνη του συστήματος.

Data Manipulation

Python

Κατόπιν οι φωτογραφίες μεταφέρονται στην Python για εξαγωγή των χαρακτηριστικών από την εικόνα, την επιλογή των χρήσιμων χαρακτηριστικών και την δημιουργία του μοντέλου ταυτοποίησης.

*Feature Extraction**:*** Για την εξαγωγή των χαρακτηριστικών από την εικόνα έγινε χρήση του αλγορίθμου "Local Binary Patterns" και αποτελεί το πρώτο στάδιο στη διαδικασία ταυτοποίησης, εξάγοντας τα χαρακτηριστικά κάνοντας χρήση του προγράμματος "Local_Binary_Input(Auto_Input)" το οποίο παρουσιάζει στο χρήστη την εικόνα του, στη συνέχεια ζητείται να διευκρινίσει εάν έχει πρόσβαση στο σύστημα. Στη συνέχεια παρουσιάζει στο χρήστη την εικόνα (figure LBP_Program) μετατοπισμένη στο φάσμα του γκρίζου(Grayscale), την εικόνα όπως μετατρέπεται μετά τη χρήση του αλγορίθμου LBP και τον πίνακα ιστογραμμάτων(histograms).

Local Binary Patterns: Ο αλγόριθμος υλοποιεί μια απλή αλλά αποτελεσματική πολιτική για εξαγωγή των χαρακτηριστικών συγκρίνοντας τις τιμές σε μια γειτονιά από pixels σε σχέση με το κέντρο της γειτονίας. Μπορεί να ξεχωρίζει με σχετική ευκολία ακμές(σημάδια, χαμόγελο, σούφρωμα κ.α.), ενώ επηρεάζεται σε λιγότερο βαθμό(σχετικά με άλλους αλγορίθμους) από την ποσότητα φωτός που υπάρχει στο περιβάλλον. Η σημαντικότερη παράμετρος στον συγκεκριμένο αλγόριθμο η οποία είναι άμεσα εμπλεκόμενη με την λεπτομέρεια των χαρακτηριστικών είναι η ακτίνα της γειτονίας(πόσα pixel θα χρησιμοποιούνται ανά γειτονία). Στην εφαρμογή επιλέχτηκαν τα οκτώ pixel που θα δώσουν και την καλύτερη λεπτομέρεια. Ο αριθμός των pixel επηρεάζει άμεσα την λεπτομέρεια αφού ορίζει τον αριθμό των συγκρίσεων με το κεντρικό και το σύνολο των χαρακτηριστικών που θα παραχθούν. Με την ρύθμιση γειτονίας στο οκτώ και τις διαστάσεις που παράγονται από το Sipeed MaixyPy M1W Dock(320*240 pixels σε τεχνολογία QVGA) έχουμε 256 χαρακτηριστικά τα οποία θα επεξεργαστούν και θα αναλυθούν για να επιλεχθούν τα ιδανικότερα. Ο τρόπος λειτουργείας του αλγορίθμου είναι επαναληπτικός για κάθε γειτονία παράγει ένα αριθμό. Ο τρόπος δημιουργίας του αριθμού αναφέρεται πιο κάτω μαζί με την τρόπο λειτουργίας του αλγορίθμου.

Φάση 1: Διαχωρισμός της εικόνας σε κομμάτια(δημιουργεί ένα grid αναλόγως των διαστάσεων της εικόνας)

Φάση 2: Για κάθε κομμάτι επιλέγει σειριακά 9 pixel σε μια διάταξη τύπου τετραγώνου 3x3

Φάση 3: Συγκρίνει το κάθε pixel με το κεντρικό

Φάση 4: Εάν έχει μεγαλύτερη ή ίση τιμή τοποθετεί ‘1’ στο αντίστοιχο pixel

Φάση 5: Εάν όχι τοποθετεί ‘0’

Φάση 6: Κατασκευάζουμε τον αντίστοιχο 3x3 πίνακα και τοποθετούμε τα 0 και 1 στις ανάλογες θέσεις

Φάση 7: Ξεκινώντας από όποιο κελί επιθυμούμε κινούμενοι κυκλικά παράγουμε έναν 8 bit αριθμό

Φάση 8: Μόλις τελειώσουν όλες οι συγκρίσεις παράγουμε έναν αριθμό $\sum_{n=0}^{n=7} i*(2^n)$

Φάση 9: Επαναλαμβάνει τις φάσεις(2-6) μέχρι να ολοκληρωθούν όλα τα κομμάτια

Μόλις ολοκληρωθεί η πιο πάνω διαδικασία παίρνουμε τους αριθμούς που παράξαμε και τους χρησιμοποιούμε για να αναπαραστήσουμε την εικόνα μέσω ιστογραμμάτων (histograms).

Σημειώνεται ότι για να είναι εφικτός ο έλεγχος των pixel μετατρέπουμε την φωτογραφία σε grayscale έτσι ώστε να μπορούμε να ελέγξουμε ως προς 1 τιμή και όχι 3 που έχει η έγχρωμη φωτογραφία(RGB).

Με τον τρόπο αυτό μετατρέπουμε ένα χώρο πολλαπλών διαστάσεων (θόρυβος) σε χώρο χαμηλών διαστάσεων (χρήσιμα δεδομένα)

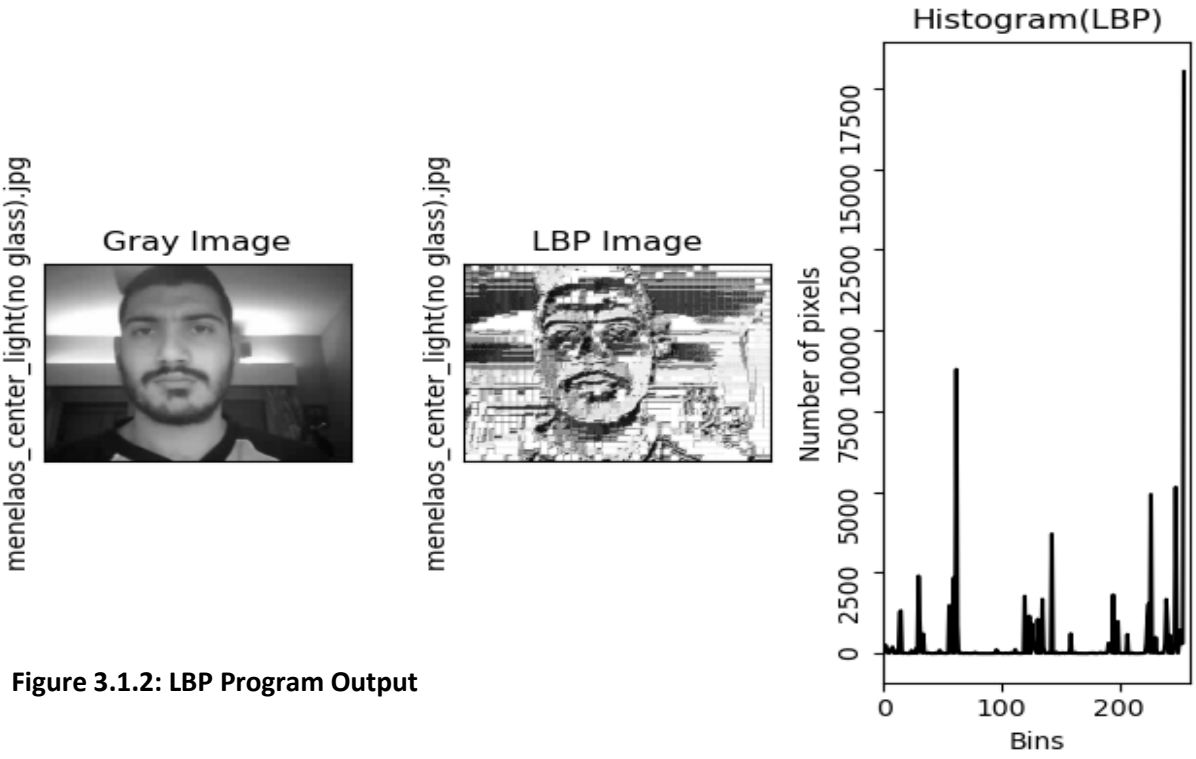


Figure 3.1.2: LBP Program Output

Feature Selection and Validation: Στη συνέχεια μέσω του προγράμματος "Dimensionality_redaction" επιχειρούμε να μειώσουμε τις διαστάσεις του προβλήματος αφού 256 πεδία για κάθε εικόνα θα κάνουν τη διαδικασία της ταυτοποίησης πολύ αργή. Επιπρόσθετα υπάρχουν πεδία που δεν ωφελεί να υπάρχουν αφού έχουν τις ίδιες τιμές για σχεδόν όλες τις εικόνες(είναι τα πεδία που αφορούν περιοχές στην φωτογραφία εκτός του προσώπου), εξ ορισμού οι τιμές αυτές δεν πρέπει να συμπεριληφθούν στην διαδικασία της ταυτοποίησης και αφαιρούνται. Τα πεδία θα αφαιρεθούν νοουμένου ότι ξεπεράσουν κάποιο κατώφλι ίδιων τιμών για ένα συγκεκριμένο πεδίο. Το κατώφλι αυτό ορίστηκε στο 75% (δηλαδή ένα το 75% ή περισσότερο των τιμών έχουν παρόμοιο εύρος τιμής), αφαιρείται το πεδίο αυτό από όλες τις εικόνες. Συγκεκριμένα αφαιρέθηκαν δεκαπέντε πεδία στη φάση αυτή. Ακολούθως κανονικοποιούμε τα δεδομένα(normalize data[Normalization]) αλλάζοντας την κλίμακα των δεδομένων μας από θετικούς φυσικούς αριθμούς σε άκαιρες τιμές από το μηδέν μέχρι ένα. Η διαδικασία αυτή είναι απαραίτητη αφού η διακύμανση μεταξύ τον ακατέργαστων δεδομένων (πεδίων) είναι μεγάλες, αυτό έχει σαν αποτέλεσμα να εμποδίζουν τους αλγορίθμους μάθησης να βρουν το μοτίβο, εάν δεν επιτελεστεί κανονικοποιήση στα δεδομένα. Έπειτα ακολουθεί το πιο χρονοβόρο στάδιο το οποίο είναι η επιλογή των χαρακτηριστικών με βάση προβλέψεις από τους αλγόριθμους που επιλέξαμε. Πριν εκκινήσουμε την διαδικασία διαχωρίζουμε τα δεδομένα που έχουμε σε δεδομένα εκπαίδευσης και δεδομένα ελέγχου-επαλήθευσης. Στην συνέχεια εφαρμόζουμε και συγκρίνουμε μεταξύ τους τις τεχνικές "Forward Checking" και "Backward Checking" για την εύρεση των πιο χρήσιμων χαρακτηριστικών. Ουσιαστικά στο "Forward Checking" ξεκινούμε με ένα ελάχιστο αριθμό χαρακτηριστικών (για το συγκεκριμένο πρόβλημα επιλέχτηκε το πέντε) και εφαρμόζουμε επαναληπτικά τον αλγόριθμο που επιλέξαμε, προσθέτοντας ένα στοιχείο στο τέλος της κάθε επανάληψης μέχρι να φτάσουμε στον μέγιστο αριθμό στοιχείων. Στόχος είναι η εύρεση του συνδυασμού που θα επιφέρει την υψηλότερη ακρίβεια. Στο "Backward Checking" ακολουθούμε την ίδια διαδικασία με την διαφορά ότι ξεκινούμε με όλα τα στοιχεία και σε κάθε επανάληψη αφαιρούμε ένα στοιχείο. Να σημειωθεί ότι επιθυμούμε μεν την μέγιστη δυνατή ακρίβεια, αλλά η χρήση υπερβολικά μεγάλου αριθμού στοιχείων θα επιβραδύνει την διαδικασία. Έτσι επιλέγουμε το μικρότερο δυνατό πλήθος στοιχείων, που θα έχει την ακρίβεια στη οποία επιθυμούμε για την εφαρμογή. Με το πέρας του προγράμματος έχει δημιουργηθεί

ένα αρχείο με τις καλύτερες υλοποιήσεις για τον κάθε αλγόριθμο. Συνολικά περιέχει δεκατέσσερις υλοποιήσεις αφού υπάρχουν δώδεκα υλοποιήσεις για τον K Nearest Neighbors Algorithm (όσες είναι και το μέγιστο πλήθος των γειτόνων) και από μια για Stochastic Gradient Descent και Support Vector Classification αντίστοιχα. Τέλος τα επιλεγόμενα χαρακτηριστικά εκπαίδευσης (training data) και ελέγχου(testing data)μεταφέρονται στο αρχείο "Classifiers.py" για το στάδιο της εκπαίδευσης και αξιολόγησης. Τα χαρακτηριστικά που επιλέχθηκαν δοκιμάστηκαν από όλους τους αλγορίθμους για να ανακαλύψουμε ποιος συνδυασμός επιφέρει τα καλύτερα αποτελέσματα. Συνολικά υλοποιήθηκαν 196 συνδυασμοί (14 διαφορετικές προβλέψεις * 14 διαφορετικούς αλγόριθμους), από τους οποίους αναλύθηκαν για να διαπιστώσουμε εάν απέδωσαν το αναμενόμενο. Πιο κάτω παρατίθεται ο τρόπος λειτουργίας των συγκεκριμένων αλγορίθμων.

K Nearest Neighbors Algorithm: Ο αλγόριθμος αυτός θα χρησιμοποιηθεί τόσο στην ανάλυση των δεδομένων όσο και στην ταυτοποίηση. Ο αλγόριθμος K-Nearest Neighbors υλοποιεί μια απλή λογική για κατηγοριοποίηση των δεδομένων:

Φάση 1: Αρχίζουμε με ένα σύνολο από δεδομένα τα οποία είναι διαχωρισμένα σε διάφορες κατηγορίες. (Τα δεδομένα τα οποία χρησιμοποιούμε έχουν πλήθος πέντε, αυτό συνεπάγεται ότι η αναπαράσταση τους δεν είναι εφικτή αφού δεν μπορούμε να αναπαραστήσουμε δεδομένα πέραν του τρισδιάστατου χώρου)

Φάση 2: Τοποθετούμε το νέο στοιχείο στον ίδιο χώρο με τα γνωστά δεδομένα

Φάση 3: Ανάλογα με το πλήθος που έχουμε επιλέξει αναζητούμε τους κοντινότερους γείτονες για το νέο στοιχείο

Φάση 4: Όταν οι k κοντινότεροι γείτονες(στοιχεία) εντοπιστούν, τότε το στοιχείο κατηγοριοποιείται ανάλογα με την κλάση που ανήκουν η πλειοψηφία των k γειτονικών στοιχείων

Φάση 5: Επαναλαμβάνει τις φάσεις(2-4) μέχρι να κατηγοριοποιηθούν όλα στοιχεία

Stochastic Gradient Descent: Ο αλγόριθμος αυτός θα χρησιμοποιηθεί τόσο στην ανάλυση των δεδομένων όσο και στην ταυτοποίηση. Ο αλγόριθμος Stochastic Gradient Descent υλοποιεί μαθηματικό μοντέλο (Εξισώσεις και παραγώγους για υπολογισμό γραμμής, επιφάνειας ή υπερεπιφάνειας) για την κατηγοριοποίηση των δεδομένων:

Φάση 1: Αρχίζουμε με ένα σύνολο από δεδομένα τα οποία αναπαριστούμε στο χώρο. (Τα δεδομένα τα οποία χρησιμοποιούμε έχουν πλήθος πέντε, αυτό συνεπάγεται ότι η αναπαράσταση τους δεν είναι εφικτή αφού δεν μπορούμε να αναπαραστήσουμε δεδομένα πέραν του τρισδιάστατου χώρου)

Φάση 2: Υπολογίζουμε τις παραγώγους ως προς τα στοιχεία που έχουμε

Φάση 3: Υπολογίζουμε τις συναρτήσεις σφάλματος

Φάση 4: Υπολογίζουμε τις νέες τιμές για τα δεδομένα μας

Φάση 5: Επαναλαμβάνει τις φάσεις(2-4) μέχρι να κατηγοριοποιηθούν όλα στοιχεία

Όταν ολοκληρωθεί η διαδικασία και βρεθεί η βέλτιστη γραμμή, επιφάνεια ή υπερεπιφάνεια (αυτό εξαρτάται από το μέγεθος του προβλήματος) τα δεδομένα βρίσκονται στο μέγιστο βαθμό κατηγοριοποίησης.

Ο αλγόριθμος αυτός προϋποθέτει το πρόβλημα να είναι γραμμικά διαχωρίσιμο, με τον όρο αυτό εννοούμε ότι όταν αναπαραστήσουμε τα σημεία στο χώρο να μπορούν να διαχωριστούν από μια γραμμή, επιφάνεια ή υπερεπιφάνεια(ανάλογα πάντα με τις διαστάσεις που έχει ο χώρος στον οποίο βρισκόμαστε)

Support Vector Classification: Ο αλγόριθμος αυτός θα χρησιμοποιηθεί τόσο στην ανάλυση των δεδομένων όσο και στην ταυτοποίηση. Ο αλγόριθμος Support Vector Classification προσπαθεί να υπολογίσει την βέλτιστη γραμμή, επιφάνεια ή υπερεπιφάνεια(ανάλογα με το μέγεθος των δεδομένων) για την κατηγοριοποίηση των δεδομένων:

Φάση 1: Αρχίζουμε από το δεδομένα μας στην αρχική τους διάσταση(στο πρόβλημα που έχουμε είναι πέντε οι διαστάσεις)

Φάση 2: Μέσω μαθηματικών μοντέλων(kernel functions έγινε χρήση του RBF)αναγάγουμε τα δεδομένα σε υψηλότερη διάσταση (στο πρόβλημα που έχουμε θα αναχθούν τα δεδομένα στην έκτη διάσταση)

Φάση 3: Χρησιμοποιούμε των αλγόριθμο Support Vector Classification για εύρεση υπερεπιφάνειας

Φάση 4: Διαχωρίζουμε τα στοιχεία ανάλογα σε ποια πλευρά της υπερεπιφάνειας βρίσκονται

Κεφάλαιο 4: **Αξιολόγηση**

Εισαγωγή

Ο λόγος ανάπτυξης της συγκεκριμένης εφαρμογής είναι η αντικατάσταση των υφιστάμενων (παραδοσιακών ή μη) συστημάτων ασφαλείας, με ένα "έξυπνο" σύστημα το οποίο θα απαλλάσσει το χρήστη από την ενεργή ενασχόλησή του στο ξεκλείδωμα, χωρίς να διακυβεύεται η ασφάλεια της περιουσίας του. Αντιλαμβανόμαστε ότι το επίπεδο ακρίβειας του αλγορίθμου πρέπει να είναι το υψηλότερο δυνατόν και να ελαχιστοποιεί τα false negative, αλλά κυρίως τα false positive. Σημαντικός παράγοντας αποτελεί και ο χρόνος απόκρισης του αλγορίθμου αφού στην χειρότερη περίπτωση επιθυμούμε να παίρνει τόσο χρόνο όσο χρειάζεται για να ξεκλειδώσει με παραδοσιακά(key, token, pin) ή άλλα βιομετρικά(ίριδα, δακτυλικό αποτύπωμα) συστήματα. Απαραίτητη θεωρείται και η αξιολόγηση της ανθεκτικότητας τέτοιων συστημάτων σε προσπάθειες παραβίασης των πρωτοκόλλων ασφαλείας τους.

4.1: Παραδοσιακά Συστήματα

Σύμφωνα με το επιστημονικό πεδίο της Αλληλεπίδρασης Ανθρώπου-Υπολογιστή(HCI: Human Computer Interaction), παραδοσιακά συστήματα αποτελούν τα συστήματα όπου για την ταυτοποίηση των χρηστών στηρίζονται στο τι γνωρίζει ο χρήστης(Knowledge-based Methods[57]), όπως για παράδειγμα ένα pin ή κωδικό. Επίσης άλλες μέθοδοι παραδοσιακών συστημάτων είναι η ταυτοποίηση μέσω ειδικών αντικειμένων-συσκευών(Token-based Methods[58]), ή την χρήση κάποιου κλειδιού .

Knowledge-Based Methods

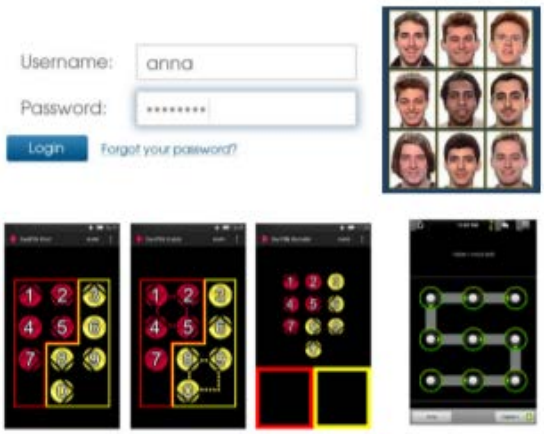
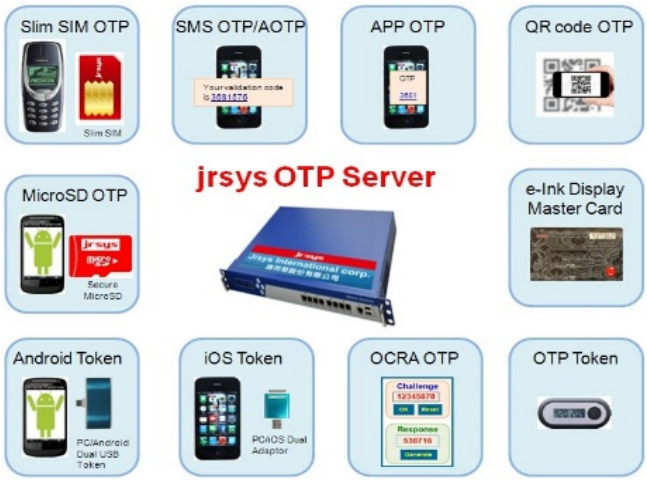


Figure 4.1.1: Knowledge-Based Methods

Token-Based Methods (Smart)



Token-Based Methods (Traditional)

Figure 4.1.2: Token-Based Methods

4.1.1: Knowledge-based Methods

Μειονεκτήματα

Σε τέτοιου είδους συστήματα ο χρήστης πρέπει να θυμάται ένα συνθηματικό για να μπορέσει να ταυτοποιηθεί. Παρόλα αυτά στην εποχή την οποία ζούμε υπάρχουν πάρα πολλοί κωδικοί τους οποίους ένας άνθρωπος καλείται να θυμάται(emails, κινητό τηλέφωνο, υπολογιστής κ.λ.π.), έτσι οι περισσότεροι χρήστες δεν χρησιμοποιούν κωδικούς με ισχυρή προστασία(η ανάμιξη κεφαλαίων, πεζών γραμμάτων, αριθμών και συμβόλων που συμβάλλουν στην δημιουργία ενός ισχυρού κωδικού), έτσι διευκολύνουν την προσπάθεια επιτήδειων στην παραβίαση συστημάτων. Η χρήση ισχυρού κωδικού έχει το μειονέκτημα ότι καθυστερεί την διαδικασία της ταυτοποίησης, αφού συνήθως έχουν μεγάλο πλήθος από ψηφία και ο χρήστης πρέπει να πληκτρολογεί κάθε φορά που εισέρχεται στο χώρο. Επιπρόσθετα είναι αρκετά συχνό φαινόμενο η κλοπή των συνθηματικών και η χρήση τους από μη εξουσιοδοτημένα πρόσωπα. Επιπρόσθετα τα συστήματα αυτά (ειδικά σε συστήματα που χρησιμοποιούν pin) είναι εφικτή η παραβίαση τους με επιθέσεις brute-force[59], man-in-the-middle[60] κ.λ.π. Τέλος επιτήδειοι μπορούν να έχουν πρόσβαση στο συνθηματικό, εκμεταλλευόμενοι τεχνικών όπως το “phishing”[61] και το “shoulder-surfing”[62].

Πλεονεκτήματα

Νοουμένου ότι έγινε υλοποίηση της νεότερης τεχνολογίας ασύμμετρης κρυπτογραφίας[63] και δημιουργήθηκε ένας ισχυρός κωδικός, τα συστήματα αυτά παρέχουν μεγάλο βαθμό ασφάλειας. Επιπρόσθετα μετά την πληκτρολόγηση του συνθηματικού η διαδικασία της ταυτοποίησης είναι σύντομη συνήθως μερικά milliseconds. Επιπρόσθετα οι πιθανότητες false positive και false negative είναι μηδαμινές.

4.1.2: Token-based Methods

Μειονεκτήματα

Σε τέτοιου είδους συστήματα, ο χρήστης πρέπει να έχει μαζί του την συσκευή ή το αντικείμενο που τον ταυτοποιεί. Οπότε μπορεί να μη χρειάζεται να θυμάται έναν περίπλοκο κωδικό, εάν ξεχάσει το μέσο το οποίο τον ταυτοποιεί, δεν υπάρχει τρόπος να ταυτοποιηθεί. Οι επιτήδειοι μπορεί να μην έχουν κάποιο συνθηματικό να υποκλέψουν, αλλά συνήθως οι συσκευές αυτές χρησιμοποιούν κάποια ειδική συχνότητα και μοτίβο αποστολής (συνήθως), για να επικοινωνήσουν με τα τερματικά για την ταυτοποίηση. Με την γνώση αυτή και τις κατάλληλες συσκευές υποκλοπής συχνοτήτων, επιτήδειοι μπορούν να υποκλέψουν την συχνότητα, άρα και την ταυτότητα μας.

Πλεονεκτήματα

Συστήματα τα οποία είναι υλοποιημένα με τέτοια λογική ταυτοποιούν τον χρήστη με μεγάλη ακρίβεια ενώ και αυτά έχουν μηδαμινές πιθανότητες για false positive και false negative κατά την ταυτοποίηση. Η διαδικασία της ταυτοποίησης είναι επίσης σύντομη, με το επιπλέον πλεονέκτημα ότι δεν υφίσταται πλέον ο χρόνος πληκτρολόγησης του συνθηματικού(τα συστήματα αυτά έχουν την λογική tap and go), επιταχύνοντας περαιτέρω την διαδικασία.

4.2: Βιομετρικά Συστήματα

Σε βιομετρικού τύπου συστήματα ο χρήστης δεν χρειάζεται γνώση κάποιου συνθηματικού ή να έχει στην κατοχή του κάποιο αντικείμενο ή συσκευή. Για την ταυτοποίηση του χρησιμοποιεί σημεία στο ανθρώπινο σώμα τα οποία ταυτοποιούν μοναδικά τους

ανθρώπους. Χαρακτηριστικότερα σημεία αποτελούν η ίριδα, τα δακτυλικά αποτυπώματα και το πρόσωπο. Ο λόγοι για τους οποίους η ίριδα και τα δακτυλικά αποτυπώματα διαφέρουν (ακόμη και για τα ομοζυγωτικά δίδυμα), είναι οι διακυμάνσεις στις ορμόνες τους κατά την περίοδο της κύησης. Για τα χαρακτηριστικά του προσώπου ευθύνονται κυρίως γενετικοί λόγοι και για αυτό τα ομοζυγωτικά δίδυμα έχουν τόσες ομοιότητες

Biometric-Based Methods

Figure 4.1.3: Biometric-Based Methods

4.2.1: Biometric-based Methods

Μειονεκτήματα

Σε βιομετρικού είδους συστήματα παρατηρείται συνήθως ελάχιστα χαμηλότερο επίπεδο ασφάλειας, από συστήματα που υλοποιούνται με τις προαναφερθείσες μεθόδους. Ο λόγος είναι ότι αποτελεί σχετικά καινούργια μέθοδος ταυτοποίησης, σε σχέση με τα τις άλλες μεθόδους. Επιπρόσθετα η διαδικασία εισαγωγής χρηστών στο σύστημα, έχει μεγαλύτερη διάρκεια.

Πλεονεκτήματα

Εν αντιθέσει με τις προηγούμενου τύπου μεθόδους, μόλις εισαχθεί ο χρήστης στο σύστημα, απαλλάσσεται από την ανάγκη ενεργής ενασχόλησης στη διαδικασία ταυτοποίησης. Ουσιαστικά όλο το σύστημα είναι αυτοματοποιημένο και ο χρήστης δεν

χρειάζεται να θυμάται κάποιο συνθηματικό, ή να έχει στην κατοχή του κάποια συσκευή ή αντικείμενο. Το μέσο για την ταυτοποίηση αποτελεί ένα μέρος από το σώμα του. Επιπρόσθετα εάν εξαιρεθεί η διαδικασία εισαγωγής του στο σύστημα, η διαδικασία της ταυτοποίησης είναι εύκολη και γρήγορη.

4.3: Σύστημα Ταυτοποίησης με χρήση MaixyPy M1W Dock

Εισαγωγή

Το σύστημα το οποίο θα αναπτυχθεί θα κάνει χρήση βιομετρικών μεθόδων, συγκεκριμένα θα αναλύει τα χαρακτηριστικά του προσώπου. Η επιλογή αυτή έγινε ώστε να μην υπάρχει το φαινόμενο της υποκλοπής, του μέσου ταυτοποίησης. Παράλληλα, θα λειτουργεί και σαν σύστημα ασφαλείας αφού θα καταγράφει τις προσπάθειες ταυτοποίησης. Το σύστημα διαθέτει το επιπλέον πλεονέκτημα της προσαρμοστικότητας, αφού δεδομένου ότι υπάρχει η βάση με τα άτομα επιλέγουμε (μέσω της εκπαίδευσης του αλγορίθμου), ποια άτομα θα έχουν πρόσβαση.

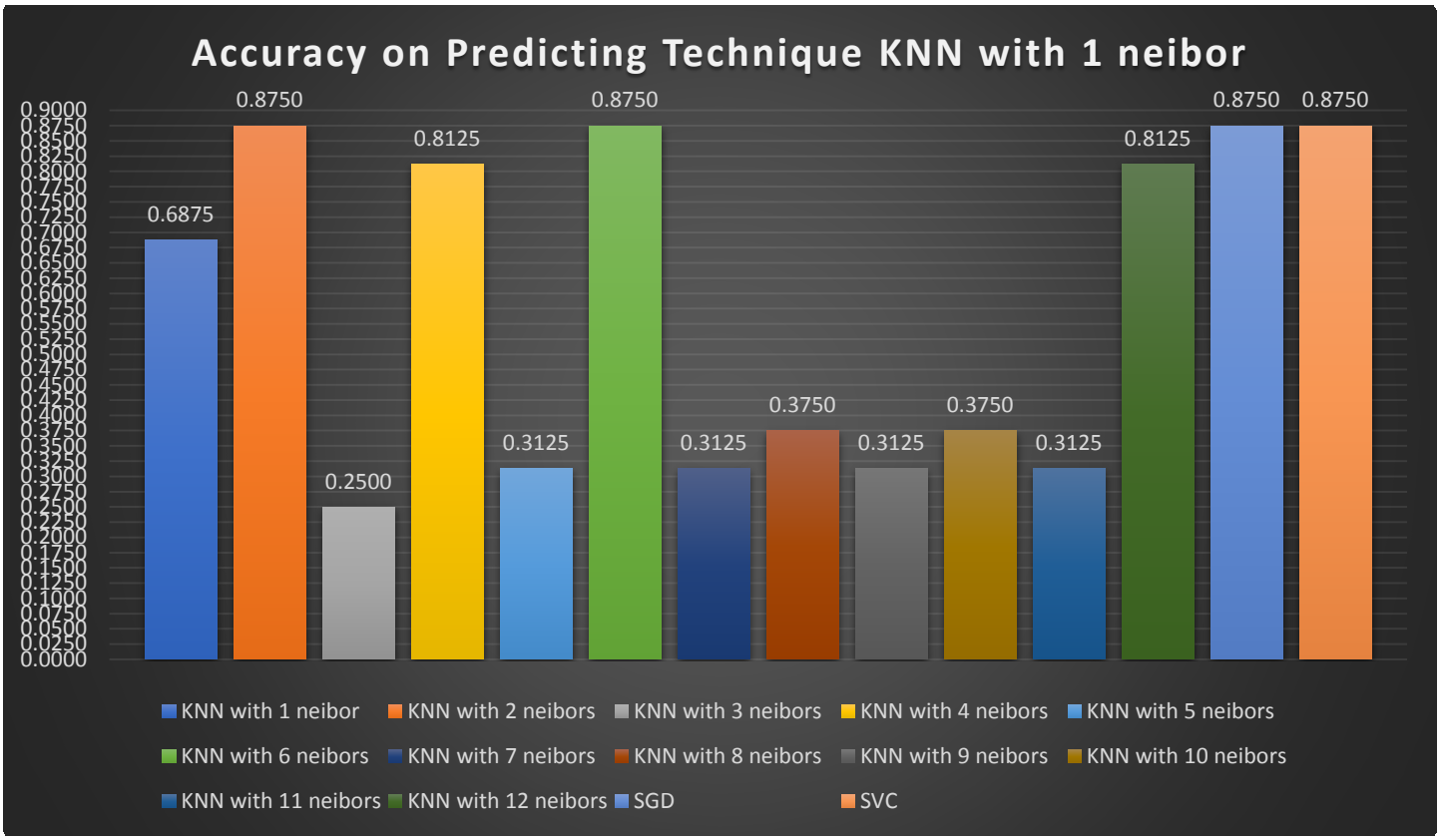
Μεθοδολογία Αξιολόγησης Αλγορίθμων

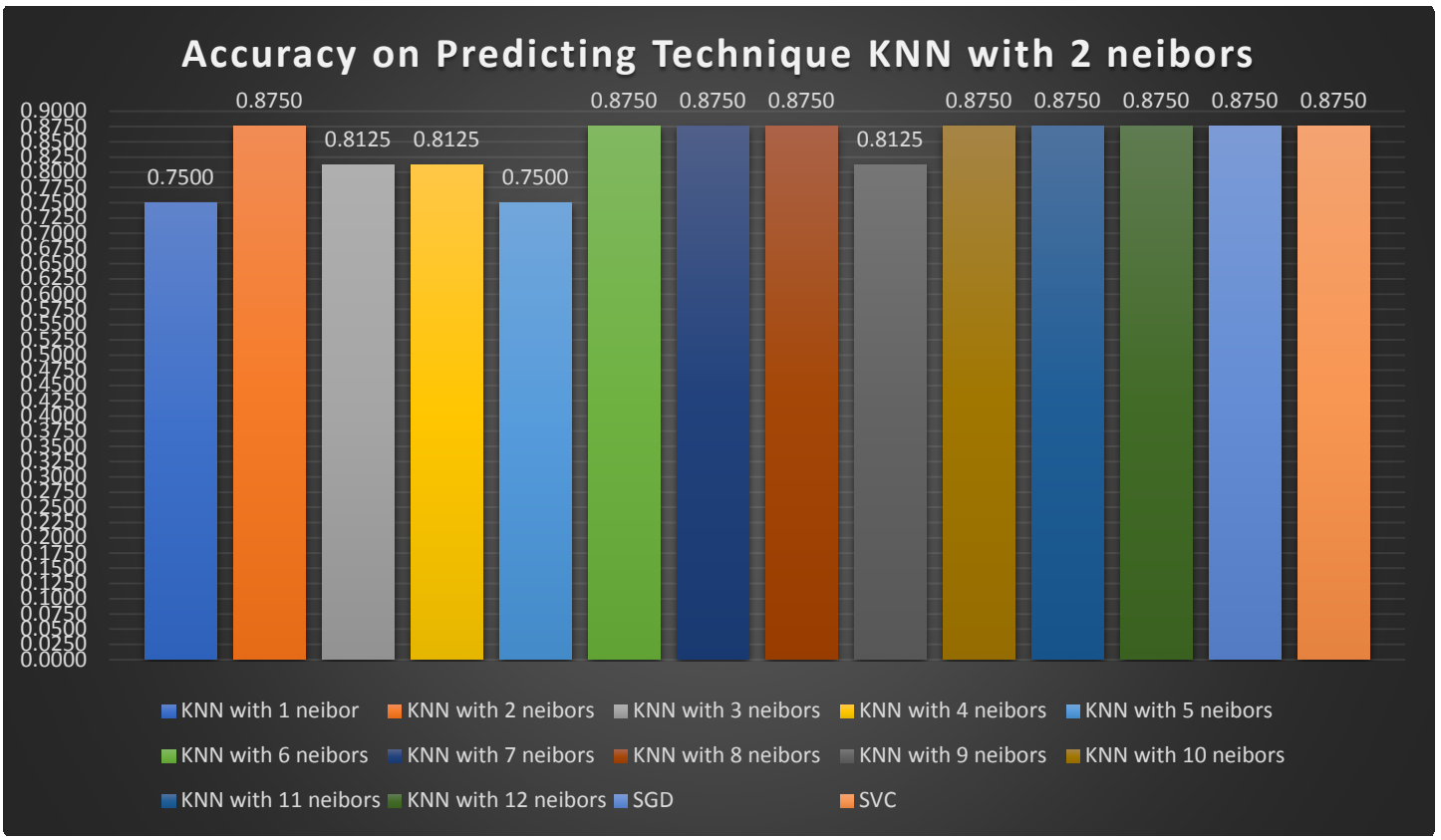
Για την αξιολόγηση των αλγορίθμων, το κάθε αποτέλεσμα λήφθηκε δέκα φορές, στη συνέχεια αφαιρέθηκαν τυχόν outliers και υπολογίστηκε ο μέσος όρος. Η προσέγγιση αυτή ακολουθήθηκε για να αφαιρεθούν τυχόν ανωμαλίες στα αποτελέσματα. Ακολούθως τα τελικά αποτελέσματα αναλύθηκαν και τοποθετήθηκαν σε γραφήματα. Αξίζει να αναφερθεί ότι κατά την παραγωγή των προβλεφθέντων χαρακτηριστικών ο κάθε αλγόριθμος υπολογίζει πόση ακρίβεια(Accuracy) αναμένουμε εάν χρησιμοποιηθεί ο αλγόριθμος αυτός. Κατά την αξιολόγηση ελέγχθηκαν διάφορες παράμετροι δίνοντας ιδιαίτερη έμφαση στην ορθότητα και χρόνο ταυτοποίησης των αλγορίθμων. Αρχικά ελέγχθηκε η ακρίβεια κάθε συνόλου από χαρακτηριστικά με κάθε αλγόριθμο για να διαπιστωθεί εάν η εκτιμώμενη ακρίβεια συμβαδίζει με την πραγματική. Στη συνέχεια κάθε αλγόριθμος ελέγχθηκε πόσο καλό σύνολο από χαρακτηριστικά παρήγαγε(ελέγχοντας το σύνολο που παρήγαγε τι ακρίβεια είχαν οι άλλοι αλγόριθμοι), όπως επίσης πόσο καλός είναι στην ταυτοποίηση(ελέγχοντας τα υπόλοιπα σύνολα που παρήχθησαν από άλλους αλγορίθμους πόσο καλά τα ταυτοποιεί). Τέλος ελέγχθηκε η ταχύτητα ελέγχου των αλγορίθμων.

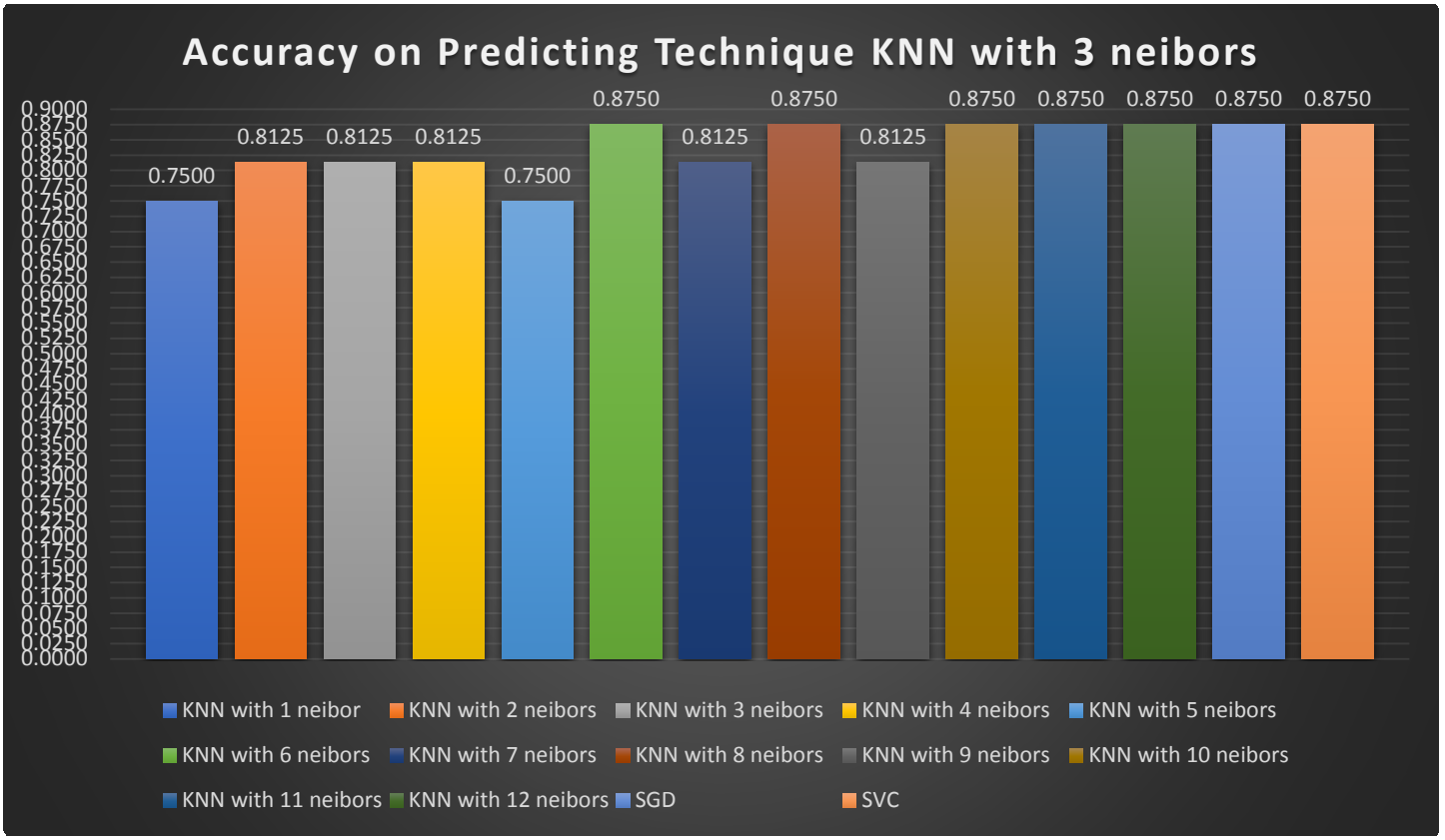
Αξιοπιστία Προβλέψεων

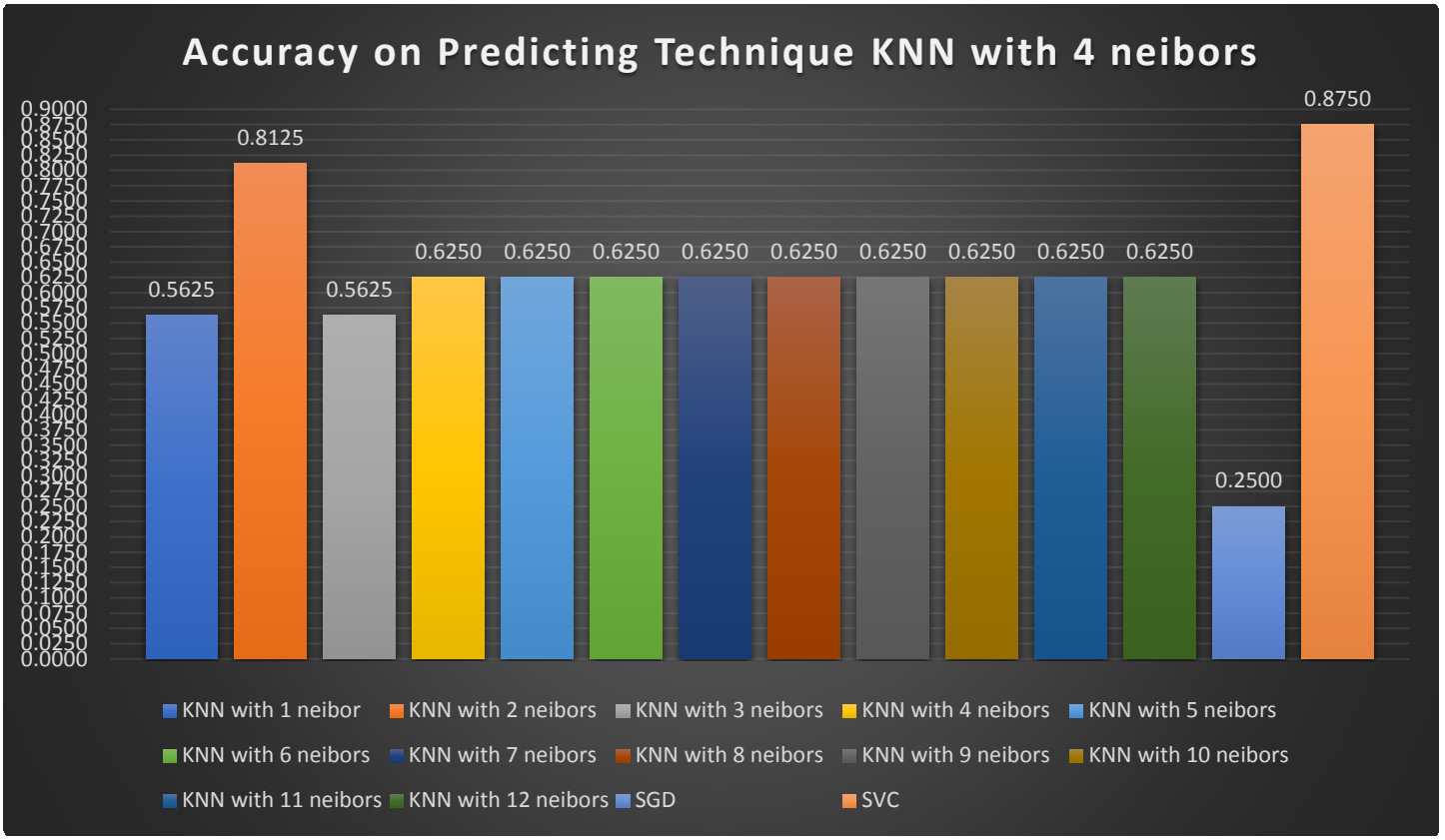
Για τον έλεγχο αξιοπιστίας των προβλέψεων κάθε μεθόδου συλλέχθηκε η ακρίβεια κάθε προβλεπόμενου συνόλου σε σχέση με όλους τους αλγορίθμους.

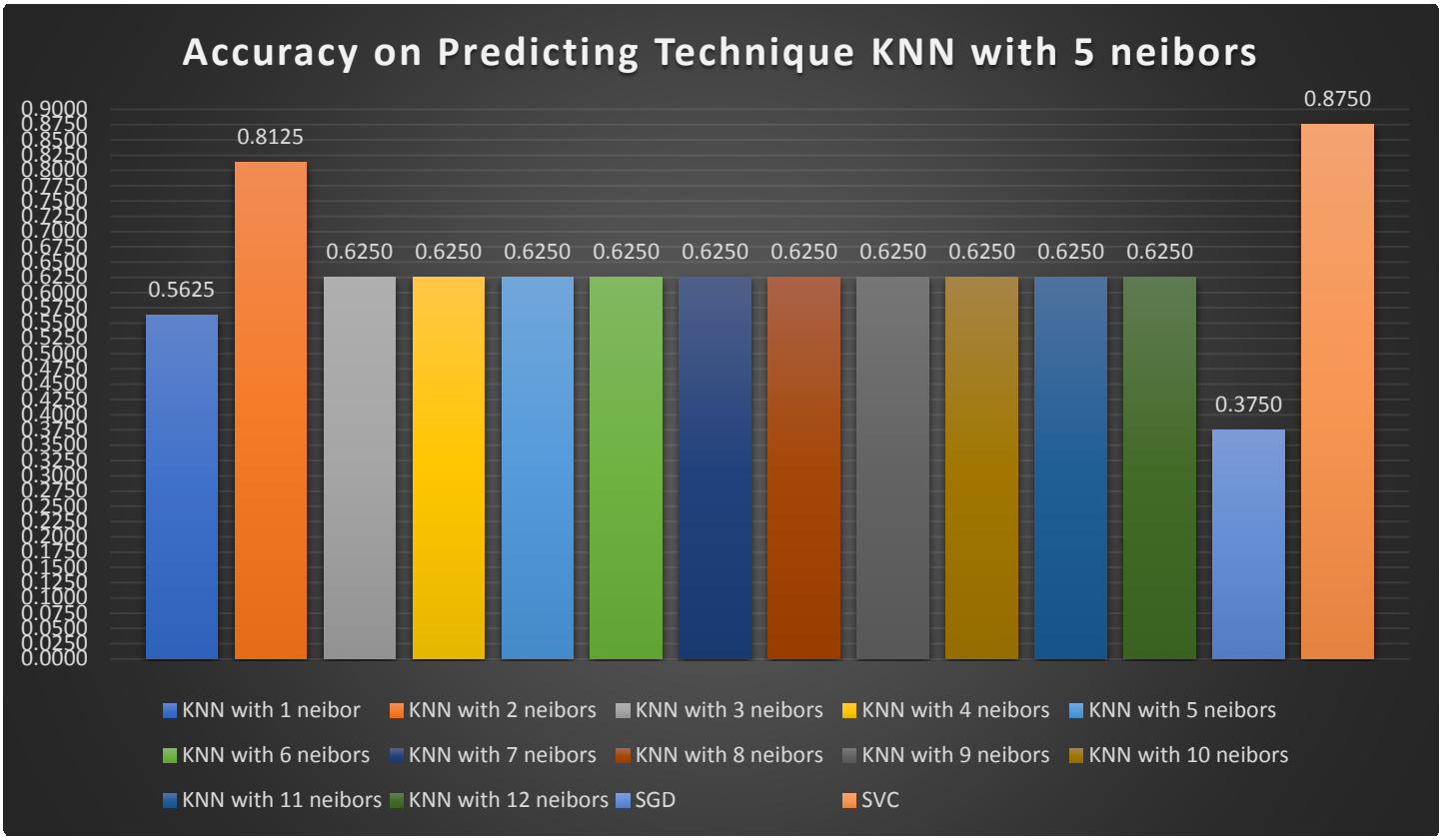
K-Nearest Neighbors

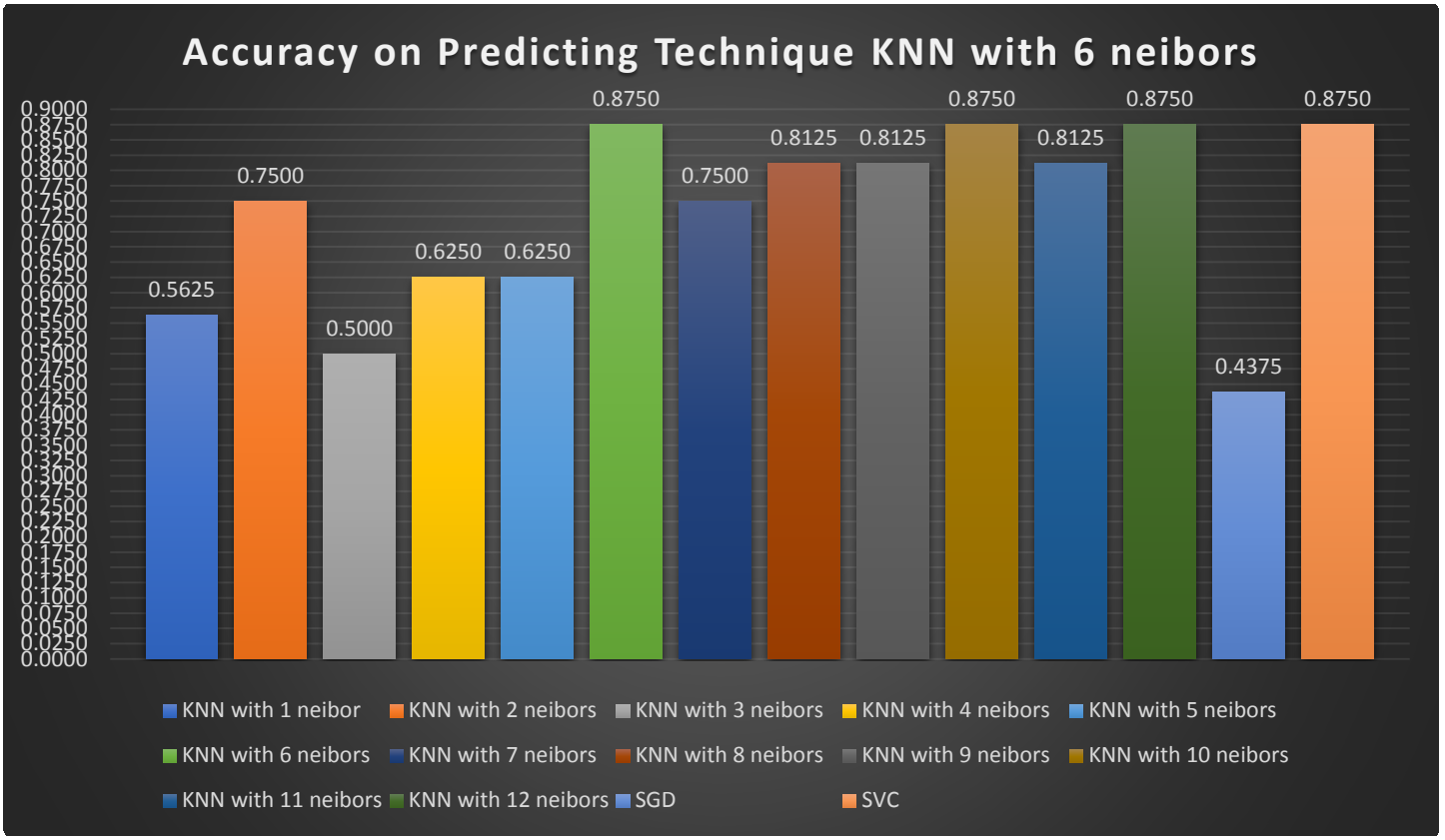


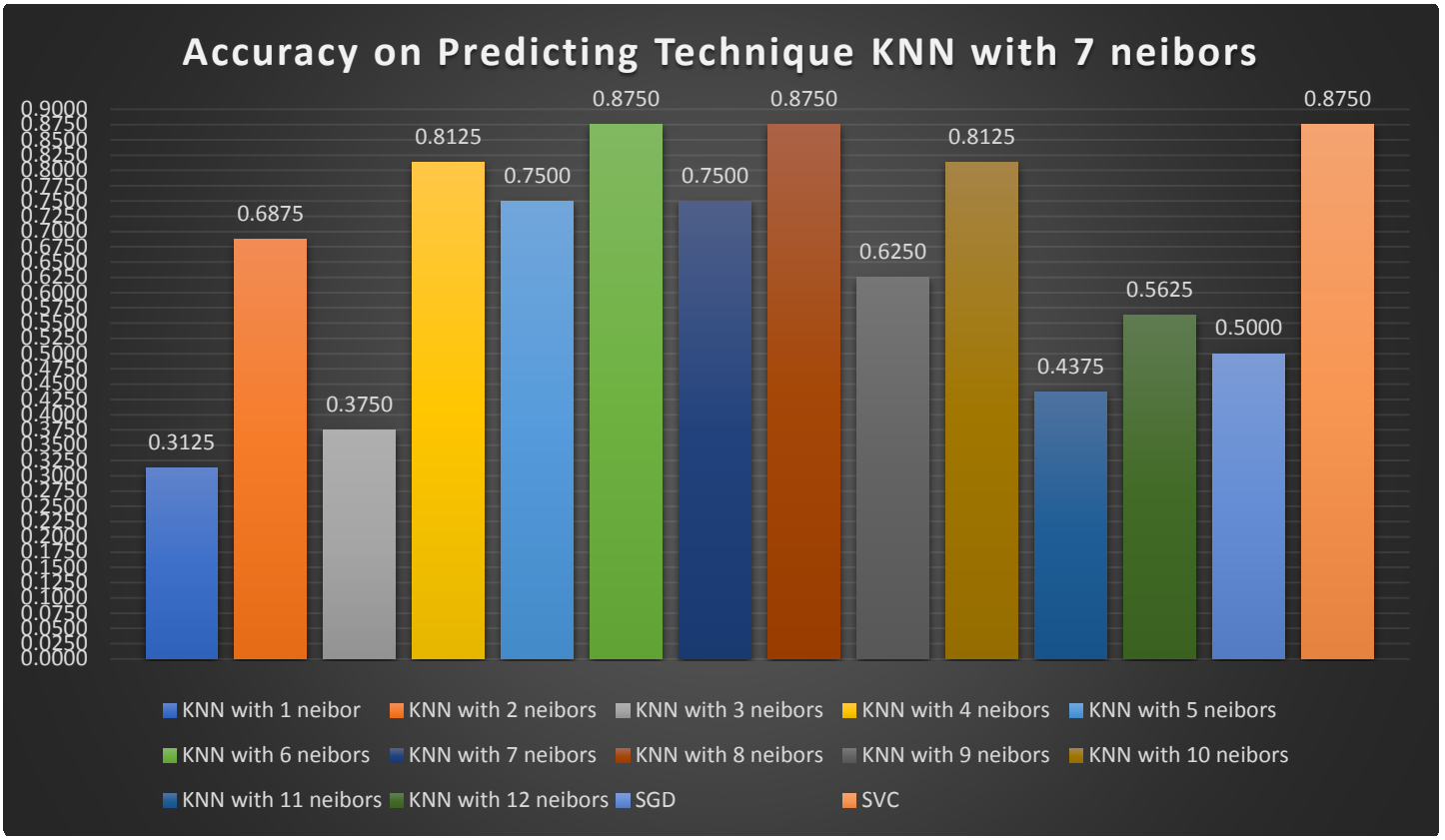


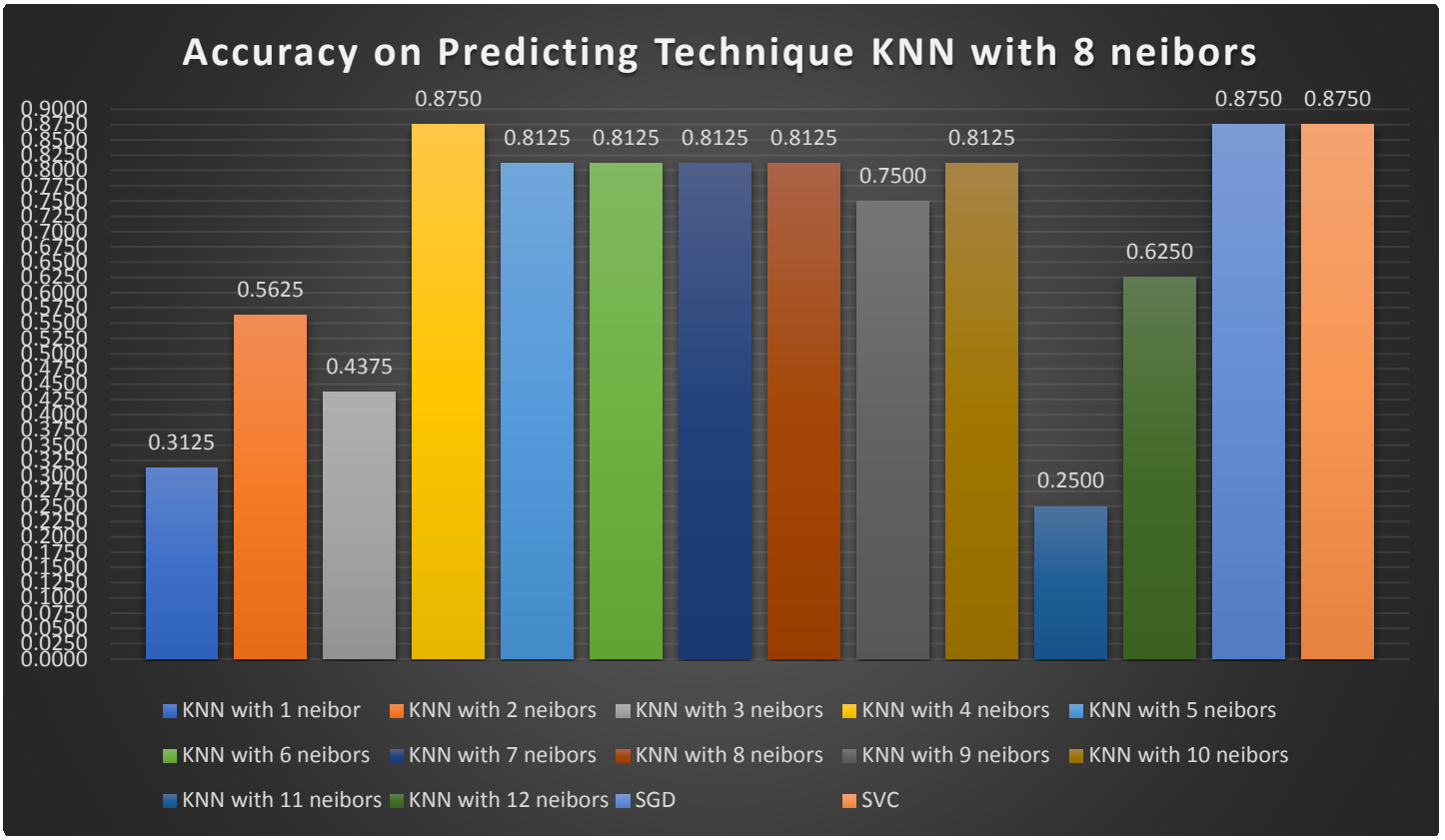

Accuracy on Predicting Technique KNN with 3 neibors
0.7500
0.8125
0.8125
0.8125
0.7500
0.8750
0.8125
0.8750
0.8125
0.8750
0.8750
0.8750
0.8750
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC

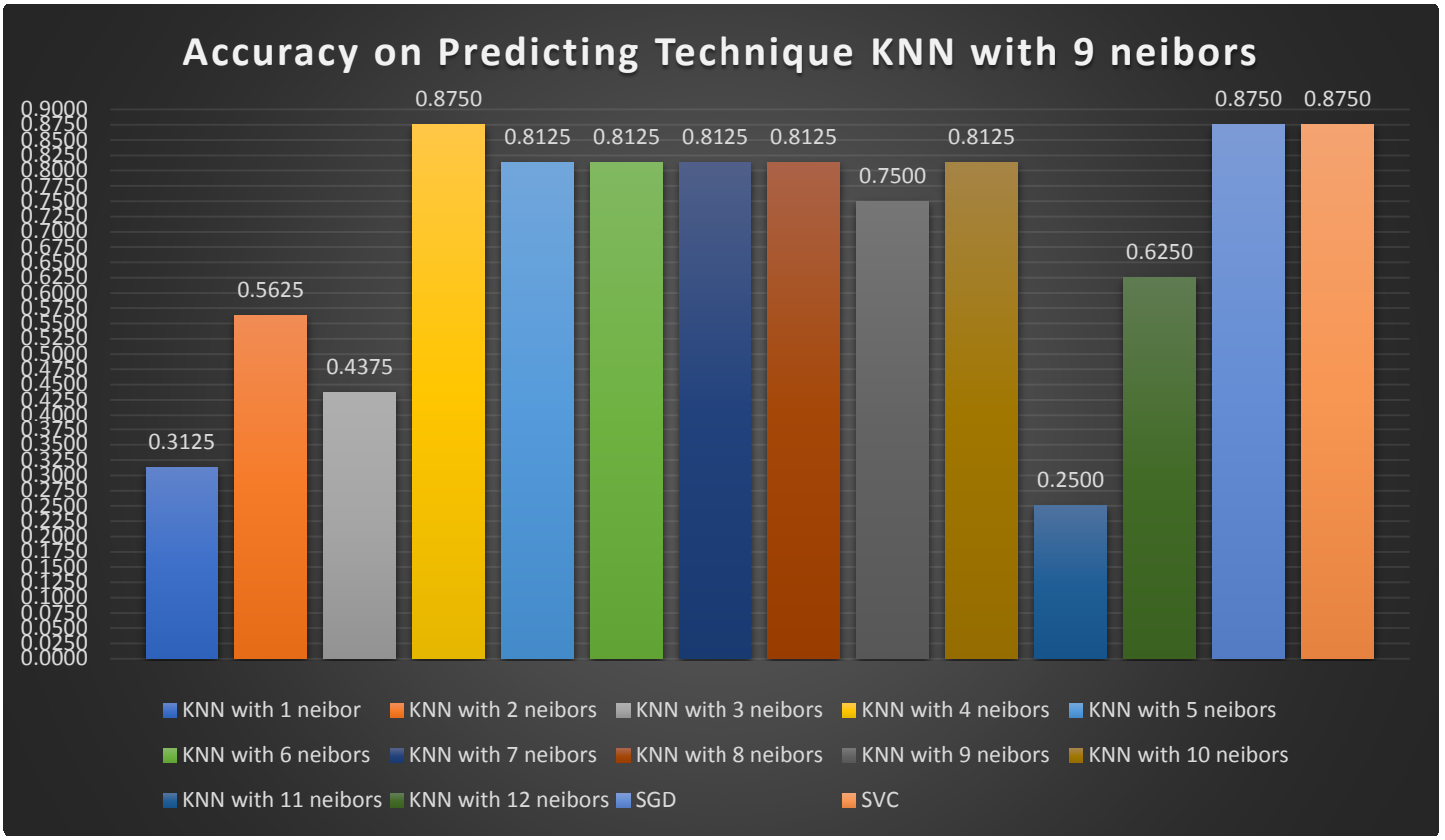

Accuracy on Predicting Technique KNN with 4 neibors
0.5625
0.8125
0.5625
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.2500
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC

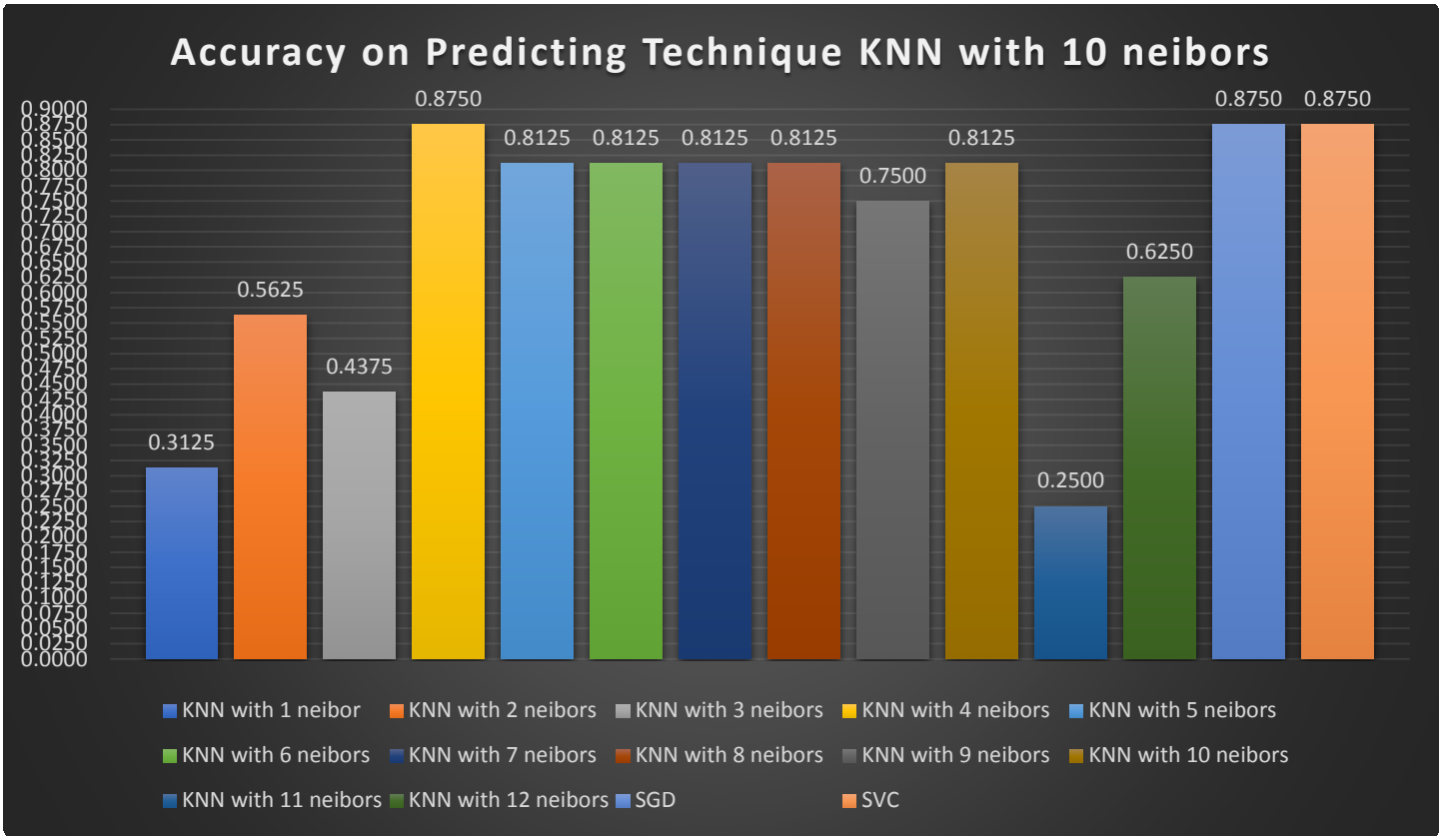

Accuracy on Predicting Technique KNN with 5 neibors
0.5625
0.8125
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.6250
0.3750
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC

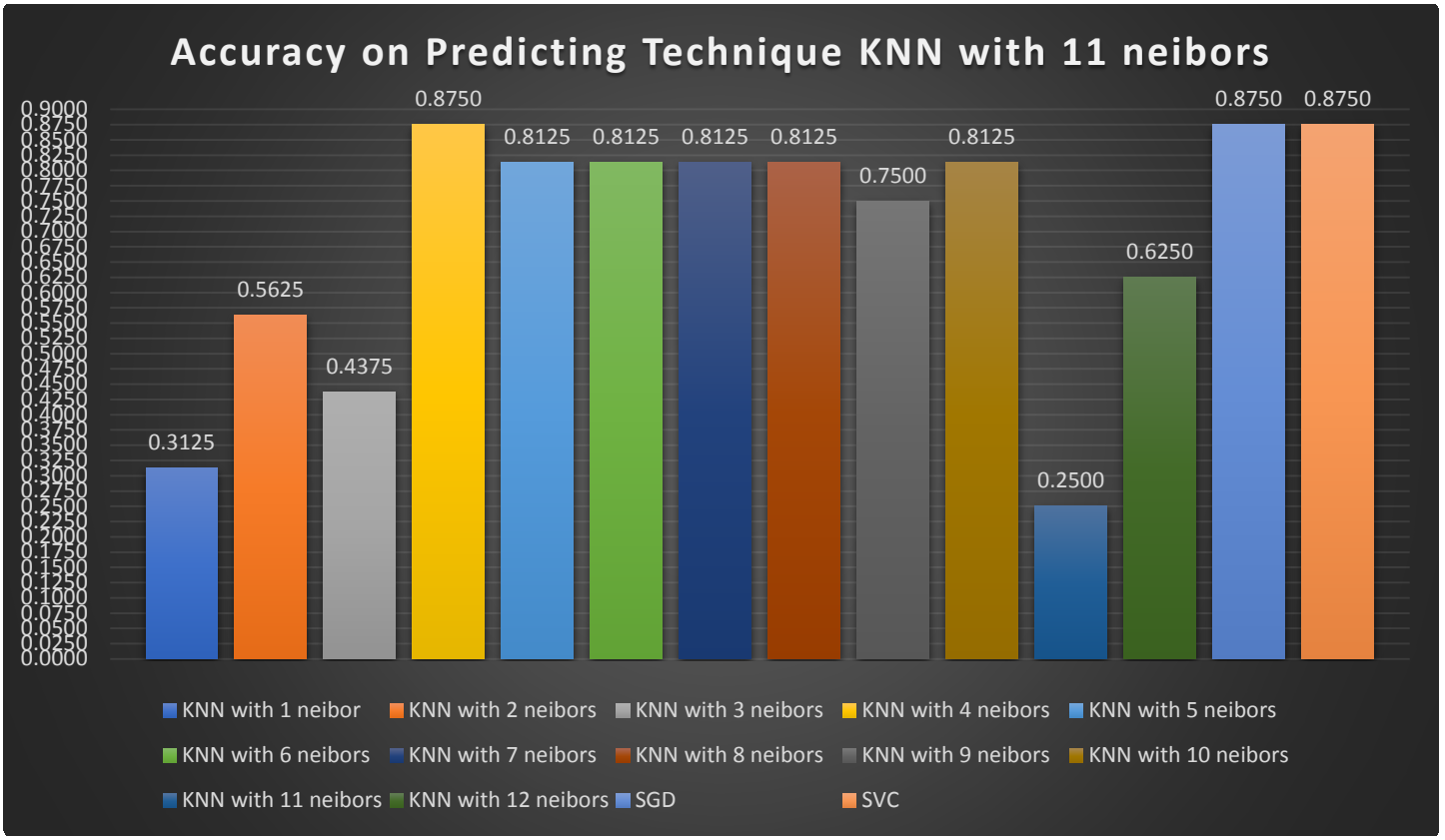

Accuracy on Predicting Technique KNN with 6 neibors
0.5625
0.7500
0.5000
0.6250
0.6250
0.8750
0.7500
0.8125
0.8125
0.8750
0.8125
0.8750
0.4375
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC

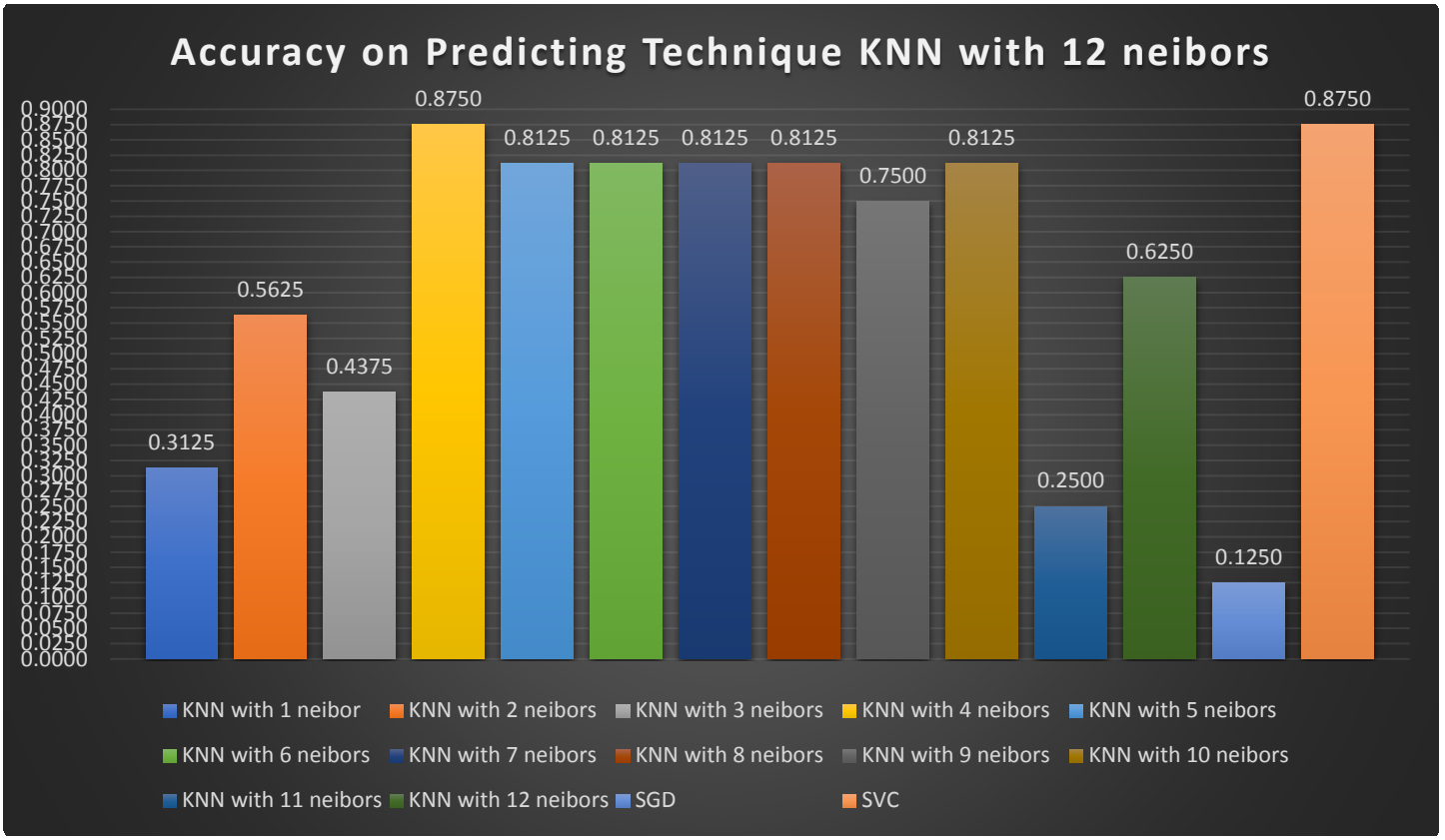

Accuracy on Predicting Technique KNN with 7 neibors
0.3125
0.6875
0.3750
0.8125
0.7500
0.8750
0.7500
0.8750
0.6250
0.8125
0.4375
0.5625
0.5000
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC


Accuracy on Predicting Technique KNN with 8 neibors
0.3125
0.5625
0.4375
0.8750
0.8125
0.8125
0.8125
0.8125
0.7500
0.8125
0.2500
0.6250
0.8750
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC


Accuracy on Predicting Technique KNN with 9 neibors
0.3125
0.5625
0.4375
0.8750
0.8125
0.8125
0.8125
0.8125
0.7500
0.8125
0.2500
0.6250
0.8750
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC

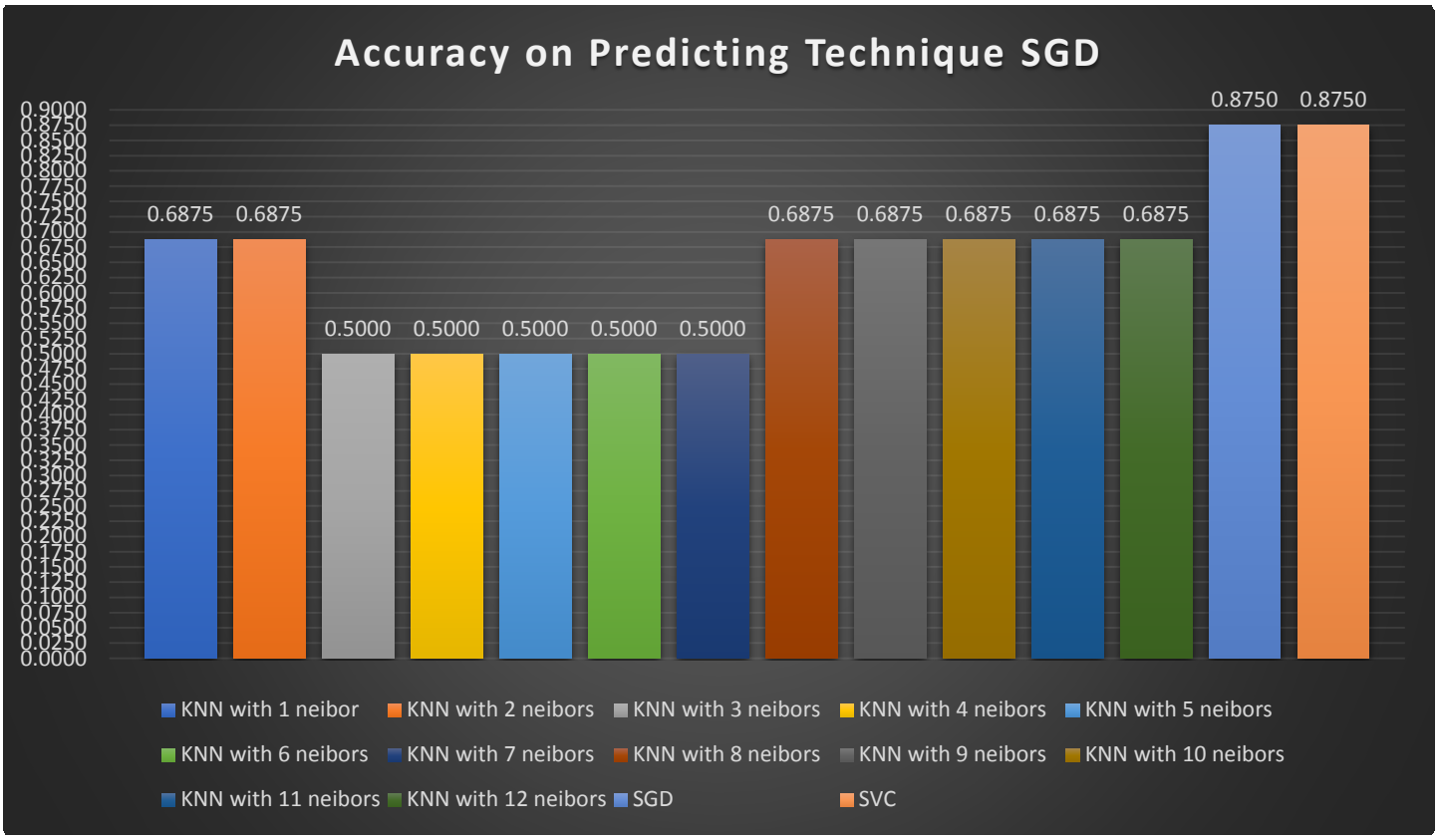

Accuracy on Predicting Technique KNN with 10 neibors
0.3125
0.5625
0.4375
0.8750
0.8125
0.8125
0.8125
0.8125
0.7500
0.8125
0.2500
0.6250
0.8750
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC


Accuracy on Predicting Technique KNN with 11 neibors
0.3125
0.5625
0.4375
0.8750
0.8125
0.8125
0.8125
0.8125
0.7500
0.8125
0.2500
0.6250
0.8750
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC


Accuracy on Predicting Technique KNN with 12 neibors
0.3125
0.5625
0.4375
0.8750
0.8125
0.8125
0.8125
0.8125
0.7500
0.8125
0.2500
0.6250
0.1250
0.8750
KNN with 1 neibor
KNN with 2 neibors
KNN with 3 neibors
KNN with 4 neibors
KNN with 5 neibors
KNN with 6 neibors
KNN with 7 neibors
KNN with 8 neibors
KNN with 9 neibors
KNN with 10 neibors
KNN with 11 neibors
KNN with 12 neibors
SGD
SVC

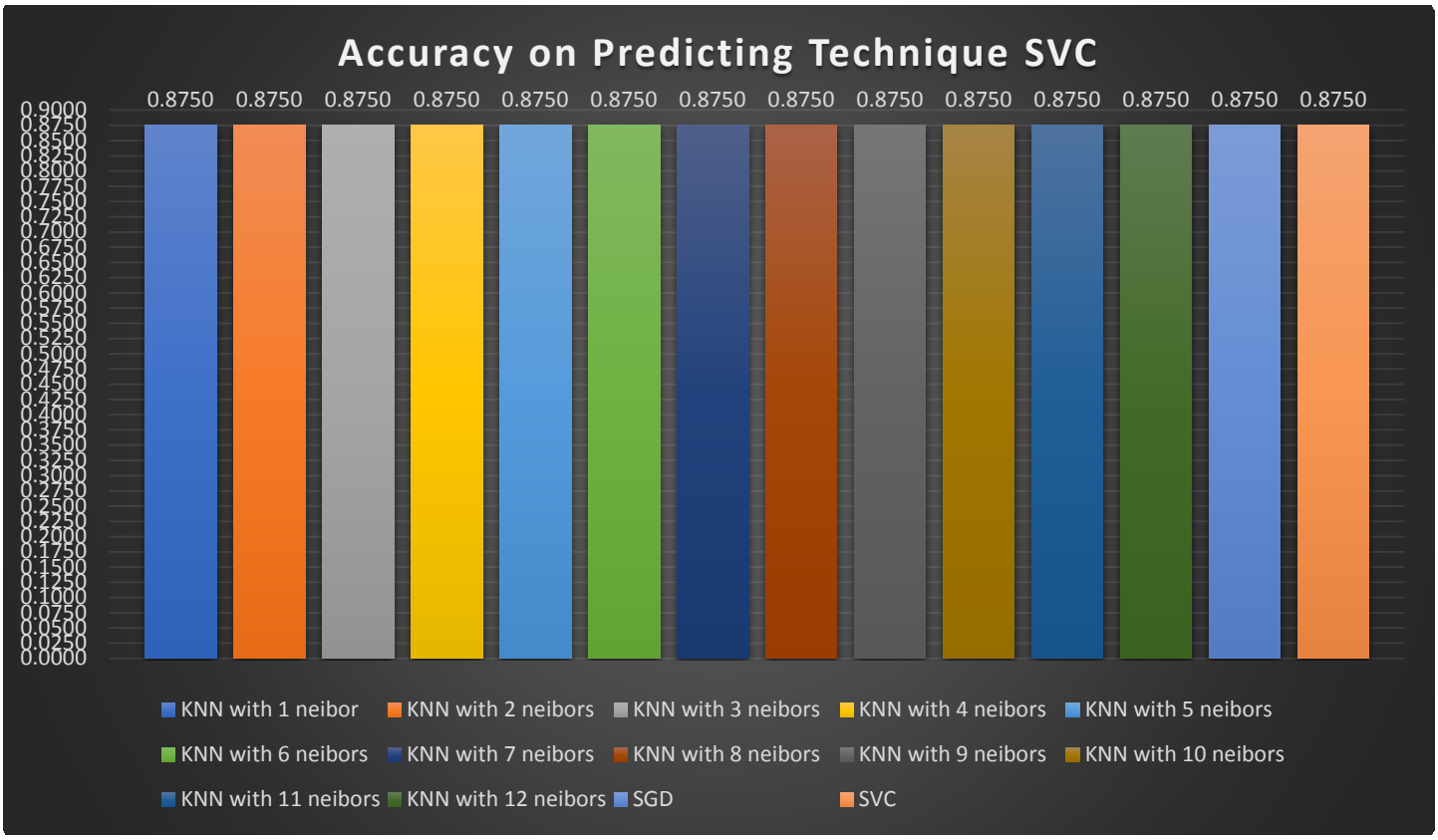
Όπως γίνεται αντιληπτό η χρήση της συγκεκριμένης μεθόδου δεν συνίσταται. Υπάρχει μια μεγάλη διασπορά στην ακρίβεια ανάμεσα στους αλγορίθμους ταυτοποίησης. Αυτό είχε ως αποτέλεσμα να μειώνεται η αξιοπιστία των αλγορίθμων γενικότερα. Αξίζει να σημειωθεί ότι σε πολλές περιπτώσεις η τεχνική εξαγωγής χαρακτηριστικών, (για παράδειγμα όταν χρησιμοποιήθηκε KNN12 για την εξαγωγή) δεν απέδωσε όπως αναμενόταν όταν χρησιμοποιήθηκε ως μέσο ταυτοποίησης. Σημαντική παρατήρηση αποτελεί ότι, ο αλγόριθμος SVC δεν παρουσίασε καμία διακύμανση και είχε το καλύτερο score ανεξαρτήτως συνόλου.

Stochastic Gradient Descent



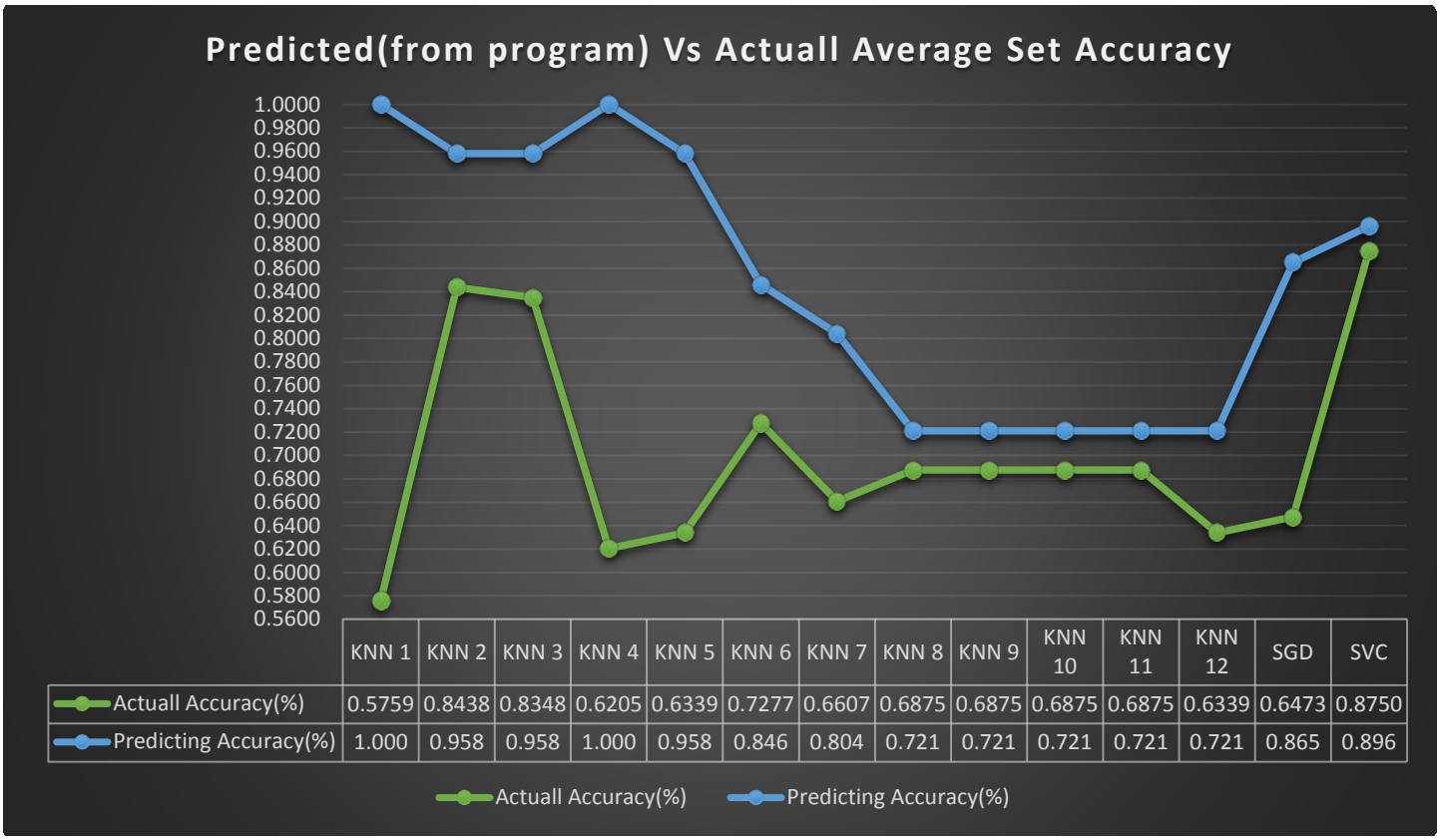
Στην μέθοδο SGD η διασπορά είναι μεν μικρότερη, αλλά και πάλι είναι απαγορευτική, αφού σχεδόν για όλες τις περιπτώσεις η ακρίβεια είναι μικρότερή από το 70%. Εν αντιθέσει με την προηγούμενη μέθοδο, η χρήση των χαρακτηριστικών που παρήγαγε η μέθοδος SGD ωφέλησε τον αλγόριθμο SGD. Παρατηρείται ότι ο SVC, μένει ανεπηρέαστος όπως έγινε και με την προηγούμενη μέθοδο.

Support Vector Classification



Στο πιο πάνω γράφημα παρατηρούμε ότι η μέθοδος SVC παράγει τον καλύτερο συνδυασμό χαρακτηριστικών, αφού ωφελεί εξίσου όλους τους αλγορίθμους και όλοι οι αλγόριθμοι έχουν το καλύτερο score.

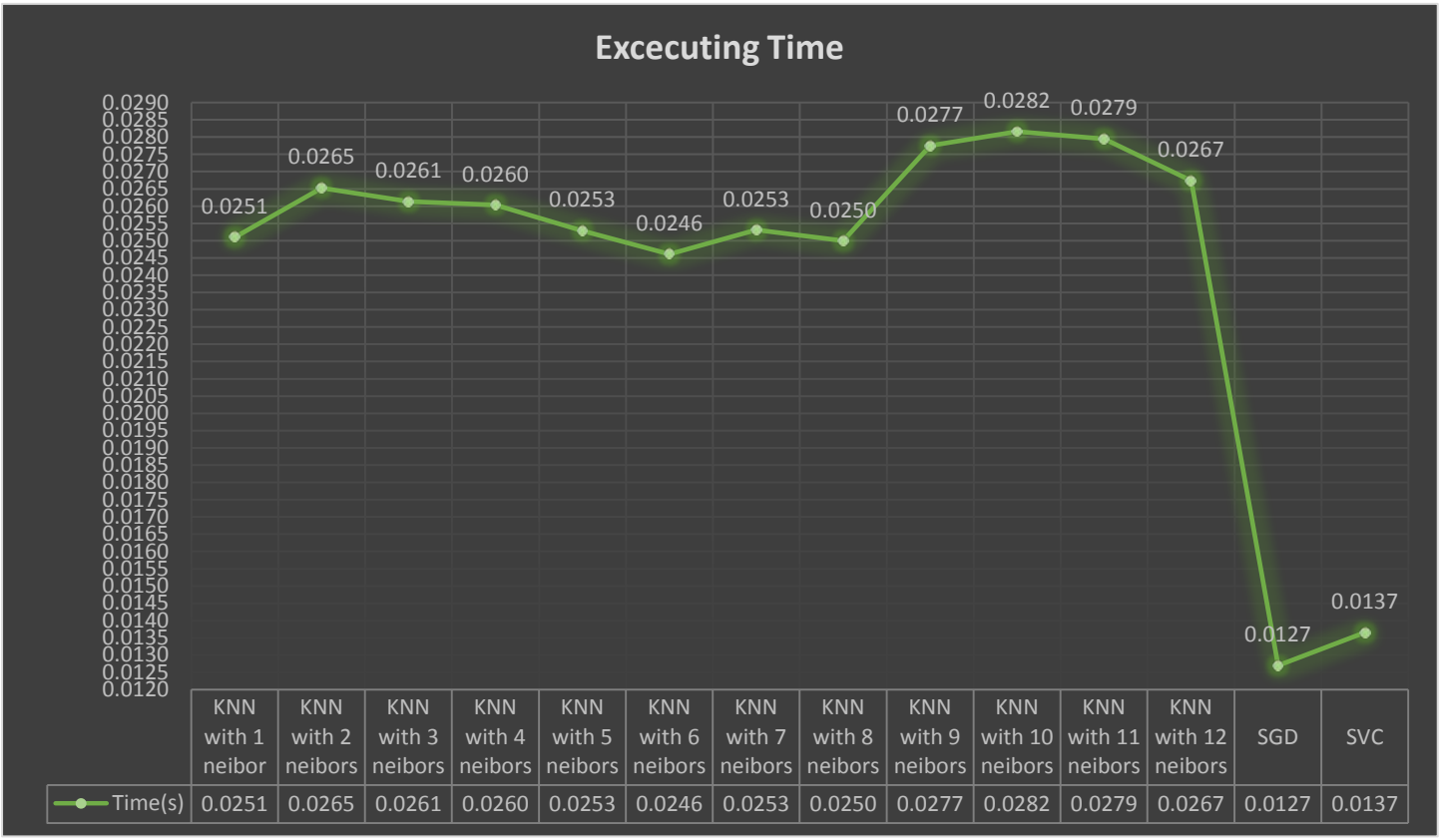
Prediction Vs Actuall Accuracy



	KNN 1	KNN 2	KNN 3	KNN 4	KNN 5	KNN 6	KNN 7	KNN 8	KNN 9	KNN 10	KNN 11	KNN 12	SGD	SVC
Actuall Accuracy(%)	0.5759	0.8438	0.8348	0.6205	0.6339	0.7277	0.6607	0.6875	0.6875	0.6875	0.6875	0.6339	0.6473	0.8750
Predicting Accuracy(%)	1.000	0.958	0.958	1.000	0.958	0.846	0.804	0.721	0.721	0.721	0.721	0.721	0.865	0.896

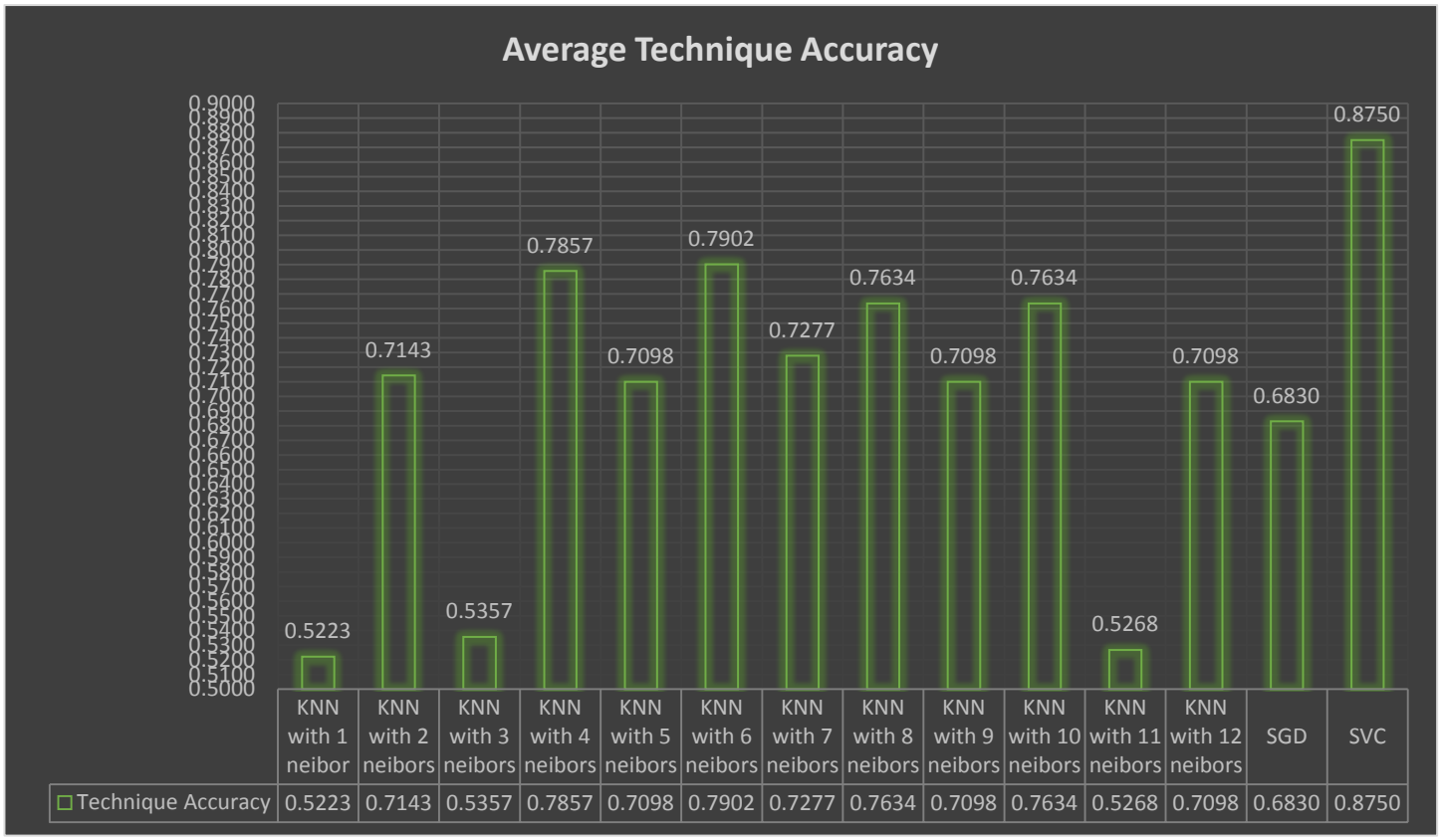
Το πιο πάνω γράφημα αναπαριστά την εκτιμώμενη ακρίβεια (την οποία προέβλεψε ο εκάστοτε αλγόριθμος κατά την επιλογή των χαρακτηριστικών), σε σχέση με την πραγματική ακρίβεια όπως πάρθηκε από τα δεδομένα ελέγχου. Παρατηρείται ότι η τεχνική KNN(K-Nearest Neighbors) για έναν και μέχρι επτά γείτονες έχουν αισθητή διαφορά. Για χρήση οκτώ μέχρι δώδεκα γειτόνων, δεν παρατηρείται αισθητή διαφορά, παρόλα αυτά η ακρίβεια τους καθιστά την χρήση τους απαγορευτική, αφού είναι ιδιαίτερα χαμηλή για ένα σύστημα ασφαλείας. Η καλύτερη τεχνική με διαφορά είναι η SVC αφού έχει την μικρότερη διακύμανση μεταξύ προβλεπόμενης και πραγματικής ακρίβειας, όντας ορθή περίπου στο 90%.

Χρόνος Εκτέλεσης



Στο πιο πάνω γράφημα αναπαρίσταται ο χρόνος εκτέλεσης των αλγορίθμων, για τα δεδομένα ελέγχου σε δευτερόλεπτα. Όπως γίνεται αντιληπτό ο αλγόριθμος KNN, χρειάζεται τον διπλάσιο χρόνο από τους άλλους δύο αλγόριθμους, για να ταυτοποιήσει τα δείγματα που του δόθηκαν. Παρόλα αυτά ο χρόνος ταυτοποίησης είναι εξαιρετικά μικρός, ως εκ τούτου δεν γίνεται αντιληπτή η διαφορά. Έτσι η επιλογή εναπόκειται μόνο στην ακρίβεια.

Ακρίβεια Ταυτοποίησης



Από το πιο πάνω γράφημα αντιλαμβανόμαστε ότι η τεχνική ταυτοποίησης SVC δίνει τα καλύτερα δεδομένα από όλα τα σύνολα των προβλεπόμενων χαρακτηριστικών καθιστώντας τον ιδανικό αλγόριθμο. Όπως έχει αναφερθεί κατά την επεξεργασία των αποτελεσμάτων αφαιρέθηκαν τα outliers, και έγινε εύρεση του μέσου όρου για να καταλήξουμε σε αυτό το αποτέλεσμα. Ο συγκεκριμένος αλγόριθμος είναι και ο μοναδικός, ο οποίος δεν είχε κανένα outlier. Ο αλγόριθμος με τις περισσότερες ακραίες τιμές είναι ο SGD το οποίο απαγορεύει την χρήση του. Ο αλγόριθμος KNN ανάλογα με τον αριθμό των γειτόνων που θα χρησιμοποιήσουμε παρουσιάζει μεγάλες διακυμάνσεις.

Συμπεράσματα

Από τα πιο πάνω συμπεραίνουμε ο αλγόριθμος SVC είναι η καλύτερη επιλογή τόσο για την εξαγωγή χαρακτηριστικών, όσο και για την μέθοδο ταυτοποίησης. Έχει σχεδόν τον μικρότερο χρόνο εκτέλεσης και την μεγαλύτερη ακρίβεια.

Κεφάλαιο 5: **Σύνοψη**

5.1: Συμπεράσματα

Η παρούσα διπλωματική είχε σκοπό να δημιουργηθεί ένα σύστημα ασφαλείας με σκοπό την αντικατάσταση των υφιστάμενων υποδομών ασφαλείας με βιομετρική ταυτοποίηση προσώπου. Για την επίτευξη του σκοπού της, αξιολογήθηκε σε διάφορους τομείς, η ικανότητα του συστήματος και αν είναι αρκετά αξιόπιστο για να αντικαταστήσει τα υφιστάμενα.

Από την ανάλυση των αποτελεσμάτων και γραφημάτων που παρουσιαστήκαν στην προηγούμενη ενότητα, προέκυψαν μια σειρά από συμπεράσματα όσο αφορά τους χώρους που μπορεί να χρησιμοποιηθεί, σύμφωνα με την αξιοπιστία του. Στις επόμενες παραγράφους παρουσιάζονται τα βασικότερα συμπεράσματα μέσα από τα επόμενα υποκεφάλαια, που ανταποκρίνονται στα ερευνητικά ερωτήματα που έχει θέσει η παρούσα ανασκόπηση.

5.1.1: Οργανισμοί – Επιχειρήσεις

Πολλές επιχειρήσεις έχουν υιοθετήσει μια πολιτική καταγραφής της ώρας προσέλευσης των εργαζομένων στο χώρο εργασίας. Τα συστήματα αυτά λειτουργούσαν με κάποιου είδους 4.1.2: Token-based Methods προσέγγιση(συνήθως κάποια κάρτα) ή και με καταγραφή τους από τον φρουρό ασφαλείας στην είσοδο. Όπως προ αναφέρθηκε στα προηγούμενα κεφάλαια, οι πρακτικές αυτές είναι πιο χρονοβόρες, σε αντίθεση με το σύστημα που αναπτύχθηκε το οποίο είναι και πιο φιλικό στο χρήστη και παρέχει μεγαλύτερη ταχύτητα ταυτοποίησης. Οργανισμοί όπως το Πανεπιστήμιο Κύπρου μπορούν να υιοθετήσουν την πρακτική αυτή, έτσι ώστε οι φοιτητές να έχουν πρόσβαση στις αίθουσες μόνο εάν είναι εξουσιοδοτημένοι. Για παράδειγμα είναι συχνό φαινόμενο την περίοδο προετοιμασίας εξετάσεων, φοιτητές άλλων τμημάτων να εισέρχονται στα

εργαστήρια πληροφορικής για να διαβάζουν. Η ενέργεια τους αυτή δεν επιτρέπει στους φοιτητές να εργαστούν στις υποδομές του εργαστηρίου αφού δεν υπάρχουν κενές θέσεις για τους υπολογιστές, ενώ παράλληλα υπάρχει οχλαγωγία. Επιπρόσθετα η αυθαίρετη είσοδος σε εργαστήρια, εγκυμονεί κινδύνους κλοπής ή καταστροφής των μηχανημάτων. Τέλος μπορεί να ρυθμιστεί να μην επιτρέπεται η είσοδος σε συγκεκριμένες ώρες όπου κλείνει το πανεπιστήμιο, ενώ παράλληλα δίνεται η δυνατότητα να απαγορεύει την πρόσβαση σε φοιτητές που είναι αργοπορημένοι.

5.1.2: Οικίες

Η χρήση του συστήματος για αντικατάσταση των υφιστάμενων κλειδαριών στο επίπεδο που βρίσκεται το σύστημα δεν είναι εφικτή. Ο λόγος είναι ότι για να είναι έμπιστο ένα τέτοιο σύστημα, η ακρίβεια πρόβλεψης πρέπει να είναι της τάξεως του 98% και μεγαλύτερη. Παρόλα αυτά, το σύστημα μπορεί να βελτιώνεται συνεχώς, εκθέτοντας το σε μεγαλύτερο σύνολο δειγμάτων και σταδιακή ρύθμιση των παραμέτρων του, αυξάνοντας την ακρίβεια του. Στο σημείο το οποίο βρίσκεται μπορεί να χρησιμοποιηθεί ως συμπληρωματικό μέτρο προστασίας, ειδοποιώντας το χρήστη ότι κάποιος μη εξουσιοδοτημένος από τον ίδιο, ξεκλείδωσε την είσοδο. Επιπρόσθετα όπως αναφέρθηκε και πιο πάνω, μπορεί να διατηρεί αρχείο για τις προσπάθειες εισόδου στην οικία του χρήστη.

5.2: Μελλοντικά Σχέδια

Με την ενασχόληση μας με την συγκεκριμένη διπλωματική, έχουμε αποκομίσει αρκετές γνώσεις. Συγκεκριμένα, θεωρούμε ότι η έρευνα που έχουμε κάνει πάνω στο αντικείμενο των βιομετρικών τεχνικών ασφάλειας μας δίδαξε ότι σε όλες τις πτυχές του σύγχρονου κόσμου, υπάρχει η δυνατότητα αναβάθμισης και ένταξης τους στο δίκτυο του Internet of Things. Επιπρόσθετα μας δόθηκε η δυνατότητα να εμπλουτίσουμε περισσότερο τις γνώσεις μας στους τομείς "Big Data Analysis[64]", "Machine Learning[65]", "Neural Network[66]".

Η εργασία αυτή έχει επιτελέσει το σκοπό για τον οποίο εκπονήθηκε, την επιτυχή ταυτοποίηση ατόμων για ένα σύστημα ασφαλείας. Παρόλα αυτά η εισαγωγή μεγαλύτερου

δείγματος φωτογραφιών θα οδηγήσει σε καλύτερα και πιο αξιόπιστα συμπεράσματα. Επιπρόσθετα πιθανή είναι και η εφαρμογή "fuzzy logic[67]" αλγορίθμων στο σύστημα, οι οποίοι επίσης πιθανόν να επιφέρουν βελτίωση των αποτελεσμάτων. Επιπρόσθετα, μπορεί να αξιοποιηθεί η τεχνική του "Hash Function"[68][69], η οποία προσφέρει μια αξιόπιστη και γρήγορη μέθοδο εύρεσης παρόμοιων χαρακτηριστικών. Τέλος τα δύο υποσυστήματα, (το πρώτο το οποίο είναι υπεύθυνο για την ταυτοποίηση και το δεύτερο το οποίο είναι υπεύθυνο για την λήψη της φωτογραφίας και την αλληλεπίδραση με το χρήστη) θα πρέπει να ενοποιηθούν έτσι ώστε να λειτουργούν ως ένα ενοποιημένο αυτοματοποιημένο σύστημα.

5.3: Εναλλακτικές Χρήσεις

Το Dock μπορεί να γίνει χρησιμοποιηθεί σε λογική Arduino, ή raspberry Pie και να προγραμματιστούν διάφορες εφαρμογές για διαφορετικά μέλη της οικογένειας. Για παράδειγμα προσωποποιημένη ρύθμιση της θερμοκρασίας στα δωμάτια. Ο κάθε χρήστης θα έχει προ εκχωρημένες ρυθμίσεις για της προτιμήσεις του στο σύστημα και στη συνέχεια κατά την ταυτοποίηση του να αλλάζουν οι συνθήκες στο σπίτι. Εναλλακτικά μπορεί να χρησιμοποιηθεί για παροχή κωδικών στην οικογένεια έτσι ώστε να μην υπάρχουν κοινοί κωδικοί αλλά αν διαφοροποιούνται ανά άτομο. Ουσιαστικά παρέχει όλα τα πλεονεκτήματα ενός παραδοσιακού dock με το πλεονέκτημα ότι μπορεί να υπάρχουν πιο προσωποποιημένες ρυθμίσεις

5.4: Περιορισμοί

Οι κυριότεροι περιορισμοί της παρούσας ανάπτυξης του συστήματος αφορούσαν το hardware και κυρίως την ενσωματωμένη κάμερα, η οποία προσφέρει εξαιρετικά χαμηλή ανάλυση για τα δεδομένα της εποχής. Αυτό έχει ως αποτέλεσμα να περιορίζει τον αριθμό χαρακτηριστικών ανά εικόνα. Επιπρόσθετα στο Sipeed MaixyPy M1W Dock δεν υποστηρίζεται η γλώσσα προγραμματισμού "Python", όπως αναφέρθηκε σε προηγούμενο κεφάλαιο, αλλά η γλώσσα "MicroPython" η οποία δεν έχει τις απαραίτητες δυνατότητες. Αυτό εισάγει την ανάγκη εξωτερικής συνεργασίας μέσω διαδικτύου με κάποια υπολογιστική υποδομή η οποία θα υποβοηθά το σύστημα, το οποίο είναι παράλληλα πιθανό σημείο παραβιάσεων.

Βιβλιογραφία

[1]: Mark Weister “The computer for the 21st Century”, September 1991

[2]: Friedemann Mattern, Christian Floerkemeier “From the Internet of Computers to the Internet of Things”, Distributed Systems Group, Institute for Pervasive Computing, ETH Zurich

[3]: “Definition - What does Facial Recognition mean?”, www.techopedia.com, May 2020

[4]: Andrew Heinzman “How Facial Recognition Works”, www.howtogeek.com, July 2011

[5]: Steve Symanovich “How Facial Recognition Works”, norton.com, 2020

[6]: “Biometrics and Facial Recognition”, www.animetrics.com, 2008

[7]: “Can facial recognition technology change the fortunes of British bookmakers?”, Paramount Digital, 2020

[8]: KEVIN BONSOR & RYAN JOHNSON “How Facial Recognition Systems Work”, howstuffworks.com

[9]: Sheng Zhang and Matthew Turk “Eigenfaces”, 2008

[10]: Jason Brownlee “Linear Discriminant Analysis”, February 2020

[11]: Elastic matching

[12]: “Hidden Markov model”, May 2020

[13]: “Multilinear subspace learning”, March 2020

[14]: “Tensor”, May 2020

[15]: Yoonsuck Choe “Dynamic link matching”, April 1996

[16]: Thomas David Heseltine “Face Recognition: Two-Dimensional and Three-Dimensional Techniques”, September 2005

[17]: IEEE “Three-View Surveillance Video Based Face Modeling for Recognition”, Septemper 2007

[18]: J. Heo, B. Abidi, S. Kong, and M. Abidi , “Performance Comparison of Visual and Thermal Signatures for Face Recognition”, Septemper 2003

[19]: AZoRobotics ,“Army Builds Face Recognition Technology that Works in Low-Light Conditions”, April 2018

[20]: Adam Shell“A glimpse at bank branches of the future: video walls, booth-sized locations and 24/7 access”, USA Today, December 2019

[21]: Juli Clover “Apple's Face ID Feature Works With Most Sunglasses, Can Be Quickly Disabled to Thwart Thieves”, MacRumors, September 2017

[22] : Yoni Heisler, “Infrared video shows off the iPhone X’s new Face ID feature in action”, November 2017

[23]: Australian Boarder Force, “SmartGates”, March 2020

[24] : Matthew Braga, “Facial recognition technology is coming to Canadian airports this spring”, CBC March 2002

[25]: JEFF JOHN ROBERTS, “How Many Adult Faces Are Scanned From Facial Recognition Databases by Cops”, October 2018

[26]: FBI.gov, “Next Generation Identification”

[27]: Christina Larson, “Xinjiang Face Recognition System”, ScienceMag.org, February 2018

[28]: DANNY THAKKAR, Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice

[29]: Rayan Gallagher, “These Goofy-Looking Glasses Could Make You Invisible to Facial Recognition Technology”, January 2013

[30]: Charlie Osorne “Privacy visor which blocks facial recognition software set for public release”, Zero Day, August 2015

[31]: Maddie Stone, “These Glasses Block Facial Recognition Technology”, August 2015

[32]: Jun Hango, “Eyeglasses with Face Un-Recognition Function to Debut in Japan”, Wall Street Journal, August 2015

[33]: “Camouflage from face detection.”, 2016

[34]: Hope Schreiber “Worried about facial recognition technology? Juggalo makeup prevents involuntary surveillance”, yahoolife, July 2018

[35]: “EFF Sues FBI For Access to Facial-Recognition Records”, EFF, June 2013

[36]: “The lawless growth of facial recognition in UK policing”, bigbrotherwatch.org.uk, May 2018

[37]: Harley Geiger, “Facial Recognition and Privacy” cdt.org, December 2011

[38]: “FACIAL RECOGNITION TECHNOLOGY Commercial Uses, Privacy Issues, and Applicable Federal Law”, United States Government Accountability Office, July 2015

[39]: Joy Buolamwini, Timnit Gebru , “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification” 2018

[40] Patrick J. Grother, George W. Quinn and P. Jonathon Phillips, “Report on the Evaluation of 2D Still-Image Face Recognition Algorithms”, August 2014

[41]: Tom Simonite, “Photo Algorithms ID White Men Fine—Black Women, Not So Much”, June 2018

[42]: Stephen Bunanyi, “Rise of the racist robots – how AI is learning all our worst impulses” guardian.com, August 2017

[43]: Ali Breland, “How white engineers built racist code – and why it's dangerous for black people”, guardian.com, December 2017

[44]: Stuart Feffer, “Its all about Features”, September 2017

[45]: Kevin Salton, “Face Recognition: Understanding LBPH Algorithm”, November 2017

[46]: “Local Binary Patterns”, Wikipedia, February 2020

[47]: Matti Pietikäinen, “Local Binary Patterns”, Scolarpedia 2010

[48]: “Classification”, Wikipedia April 2020

[49]: “Clustering”, Wikipedia April 2020

[50]: “Feature Selection” Wikipedia May 2020

[51]: “K-Nearest Neighbors Algorithm”, https://www.saedsayad.com/

[52]: “K-Nearest Neighbors Algorithm”, Wikipedia May 2020

[53]: “Stochastic Gradient Descent”, SckitLearn.org

[54]: “Stochastic Gradient Descent”, leon.bottou.org September 2019

[55]: Kristin P.Bennett, Collin Cambell “Support Vector Machines: Hype or Hallelujah”,

[56]: “Support Vector Classification”, SckitLearn.org

[57]: “Knowledge-Based Methods”, Wikipedia, April 2020

[58]: “Token-Based Methods”, Wikipedia May 2020

[59]: “Brute Force Attacks”, Wikipedia May 2020

[60]: “Man-in-the-middle Attacks”, Wikipedia May 2020

[61]: “Phishing” Wikipedia, May 2020

[62]: Shoulder-Surfing Wikipedia May 2020

[63]: Asymmetric Cryptography Wikipedia May 2020

[64]: Big Data Analysis Wikipedia May 2020

[66]: Machine Learning Wikipedia May 2020

[67]: Neural Network Wikipedia May 2020

[68]: Fuzzy Logic Wikipedia May 2020

[68]: Jure Leskovec, Anand Rajaraman,Jeffrey D. Ullman, “Mining Massive Datasets”, Book Chapter 3, Stanford University, 2019

[69]: Jure Leskovec, Anand Rajaraman,Jeffrey D. Ullman, “Finding Similar Items- Locality Sensitive Hashing”, Stanford University, 2019

Ατομική Διπλωματική Εργασία

Appendix

SMART HOMES APPLICATION AND INTERNET OF THINGS

USING MAIXPY DOCK TOOL KIT

Μενέλαος Αρτεμίου

Πανεπιστήμιο Κύπρου

Τμήμα Πληροφορικής

Μάιος 2020

Appendix

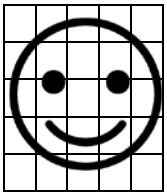
Κεφάλαιο 3: **Μεθοδολογία**

3.1: Local Binary Patterns: **LBP_youtube_explanation, LBP_wiki, LBP_Scholarpedia**

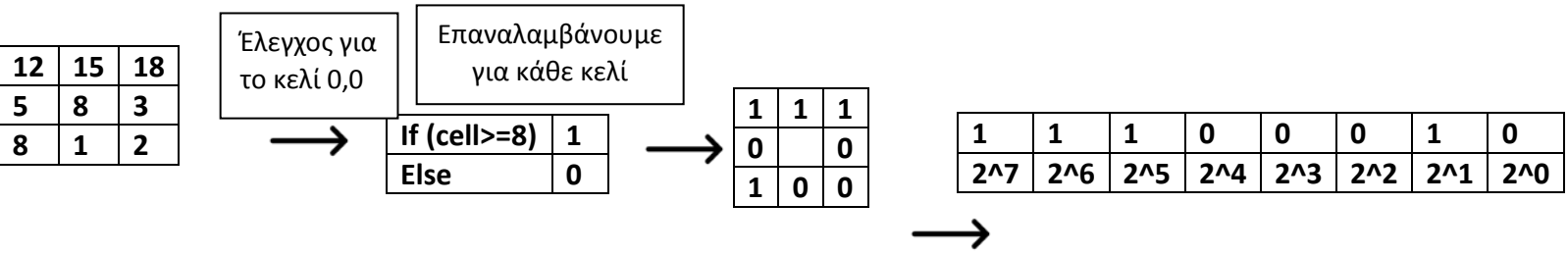
Ο αλγόριθμος αυτός παράγει τα αρχικά χαρακτηριστικά τα οποία θα χρησιμοποιηθούν για να γίνει η ταυτοποίηση του προσώπου

Διαδικασία 1*: Δημιουργία Grid*

Αναπαράσταση δημιουργίας του grid επάνω στην εικόνα για λόγους παραδείγματος χρησιμοποιήθηκε 4x4 grid (Σημείωση δεν είναι το 3x3 pixel που αναφέρεται στη διαδικασία 2. Το μέγεθος του grid όπως αναφέρεται εξαρτάται από τις διαστάσεις της εικόνας)



Διαδικασία 2-7: Υλοποίηση Αλγορίθμου



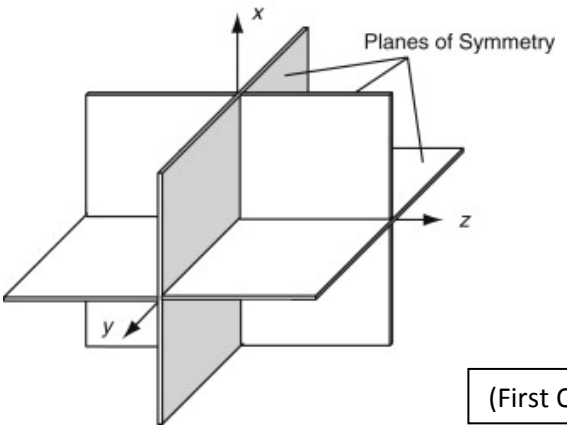
Διαδικασία 8: Εξαγωγή Αριθμού αναπαράστασης

Παράγουμε τον 8 bit αριθμό μας με τον ακόλουθο τρόπο, υψώνουμε το 2 στην δύναμη ανάλογα με την θέση του τελικού πίνακα (από το 0 μέχρι το 7) και το πολλαπλασιάζουμε με ΄0΄ ή ΄1΄ ανάλογα με την τιμή του κελίου. Πιο κάτω παρατίθεται παράδειγμα με τα δεδομένα από την διαδικασία 2 μέχρι 7.

0*(2^0)+1*(2^1)+0*(2^2)+0*(2^3)+0*(2^4)+1*(2^5)+1*(2^6)+1*(2^7)

Κάθε πίνακας 3x3 είναι ένα στιγμιότυπο στο χρόνο για τα συγκεκριμένα 9 pixel. Εάν παίρνουμε διαδοχικά στιγμιότυπα του ίδιου προσώπου μπορούμε να εισάγουμε τον χρόνο στα δεδομένα μας και μας επιτρέπετε έτσι να εντοπίσουμε διαφορές τόσο στο ίδιο στιγμιότυπο όσο και στο κάθε pixel

συγκρίνοντας τα με κεντρικό(αυτή τη φορά όμως το κεντρικό λόγο ότι έχουμε πολλά στιγμιότυπά και δεν έχουμε ένα grid σε σχήμα τετραγώνου αλλά σε σχήμα κύβου και το κέντρο είναι το μεσαίο κελί με συντεταγμένες (1,1,1) (η αρίθμηση ξεκινάει από το 0). Παρόλα αυτά δημιουργείται ένας αριθμός 26bit για κάθε κύβο 3x3x3 το οποίο αυξάνει κατά πολύ την πολυπλοκότητα. Παρόλα αυτά δεν έχουν όλα τα pixel την ίδια σημαντικότητα, έτσι από τον κύβο παίρνουμε τρείς ορθογώνιες μεταξύ τους επιφάνειες (στα αγγλικά first orthogonal plane). Παίρνουμε τετράγωνο XY, XZ, YZ, με αυτό τον τρόπο έχουμε 3*(2^8) pixels το οποίο είναι κατά πολύ μικρότερο του 2^26 pixels



(First Orthogonal Plane)

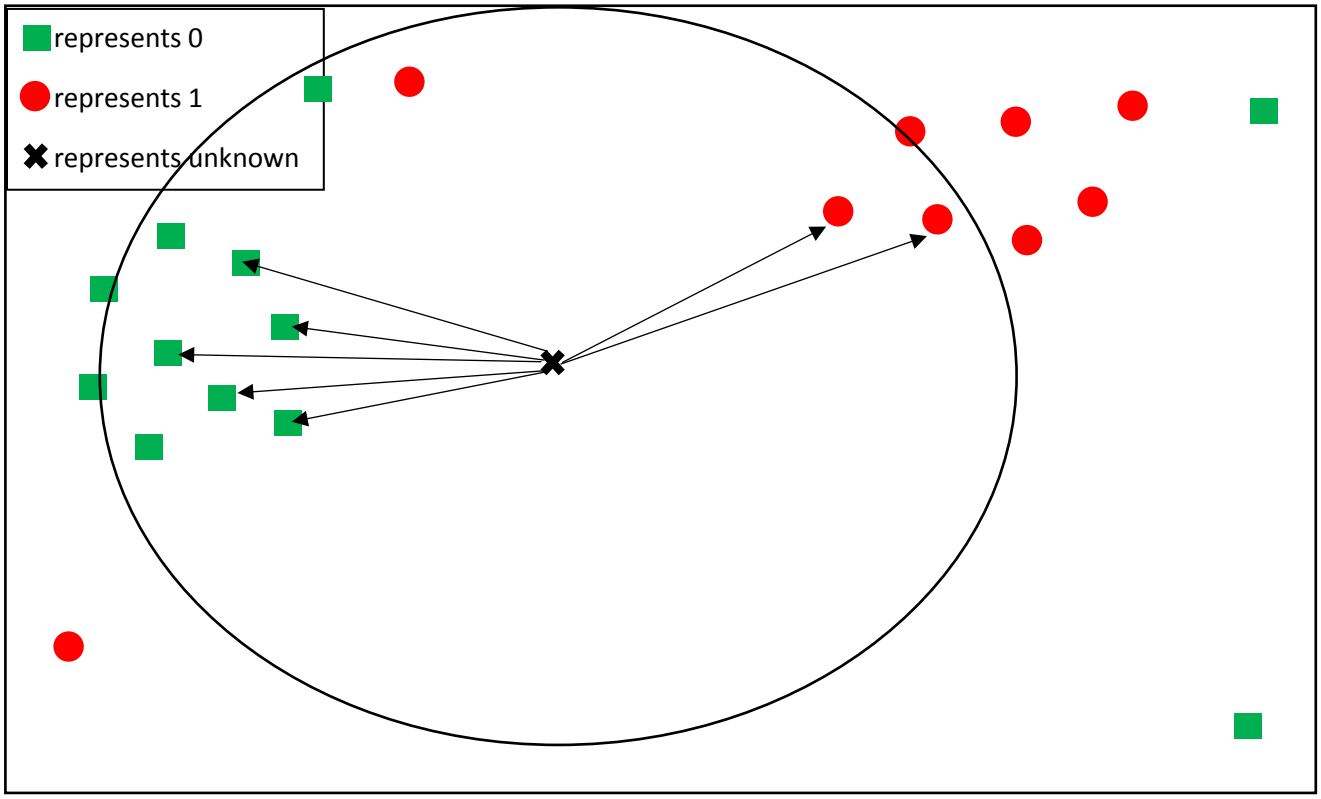
3.2: K Nearest Neighbors: KNN_youtube_explanation, KNN_wiki,

Ο αλγόριθμος αυτός θα χρησιμοποιηθεί τόσο στην ανάλυση των δεδομένων όσο και στην ταυτοποίηση

Σχηματική Αναπαράσταση Λειτουργίας Αλγορίθμου K Nearest Neighbors

Φάση 1: *Εύρεση k κοντινότερων γειτόνων*

Παράδειγμα για εύρεση k nears neighbors με k=6 όπως φαίνεται και από το πιο πάνω σχήμα οι 6 κοντινότεροι γείτονες υποδεικνύονται με βέλος, τέσσερις εκ των οποίων ανήκουν στην κλάση ‘0’ ενώ οι υπόλοιποι ανήκουν στην κλάση ‘1’. Ο αλγόριθμος συμπεραίνει ότι το νέο σημείο ανήκει στην κλάση ‘0’.

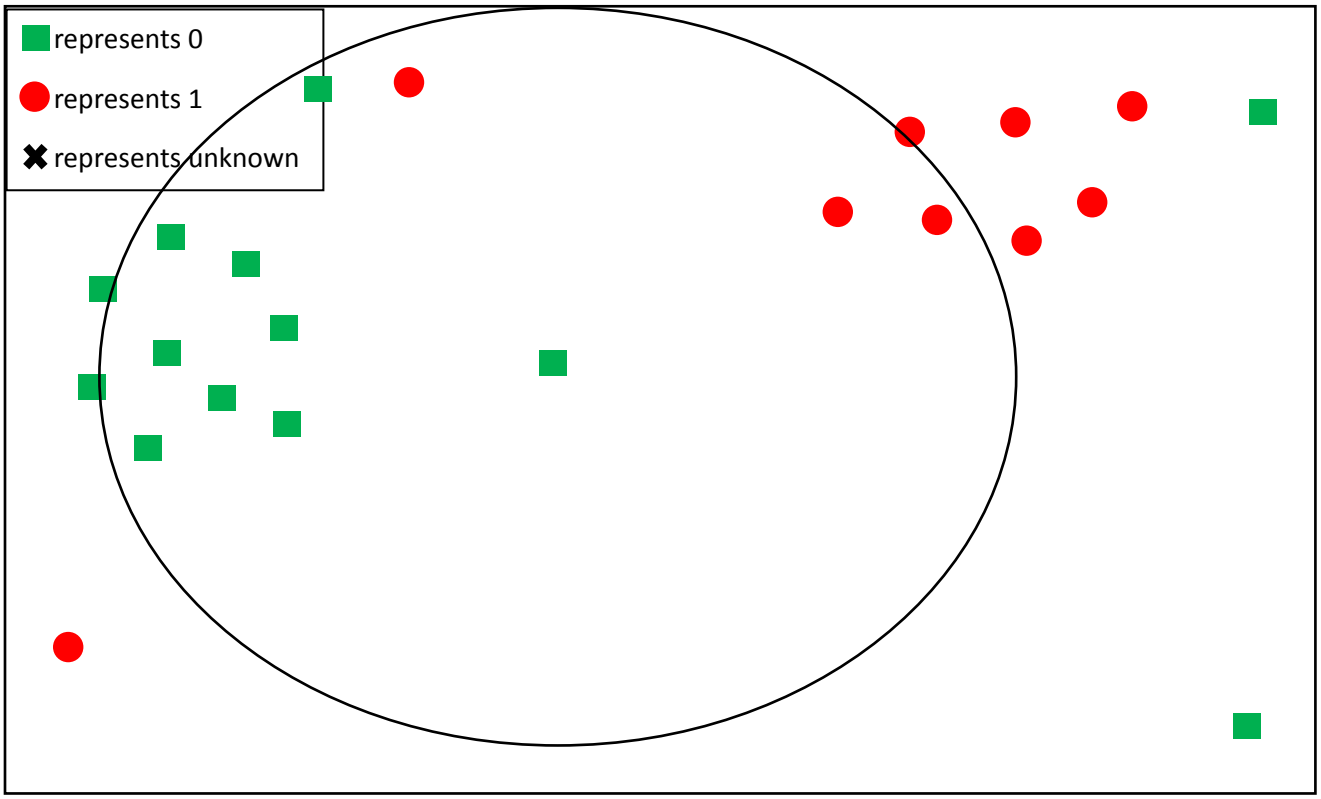


Φάση 2:

Εύρεση κλάσης στην οποία ανήκει η πλειοψηφία (στο παράδειγμα η κλάση είναι ‘0’)

Φάση 3:

Υιοθέτηση σημείου στην κλάση όπου ανήκει η πλειοψηφία (στο παράδειγμα η κλάση αυτή είναι το ‘0’)



Φάση 4: Επαναλαμβάνουμε τις Φάσεις 1-3 μέχρι να κατηγοριοποιηθούν όλα τα σημεία

Σημείωση: Το συγκεκριμένο παράδειγμα που δόθηκε αναπαριστά δεδομένα στον δισδιάστατο χώρο. Τα δεδομένα τα οποία χρησιμοποιούμε βρίσκονται σε χώρο πέντε διαστάσεων (λόγου του πλήθους δεδομένων που χρησιμοποιείται) ο οποίος είναι αδύνατος να αναπαρασταθεί σχηματικά, μια αναπαράσταση στον δισδιάστατο χώρο δίνει την γενική ιδέα λειτουργίας του αλγορίθμου αυτού.

3.3 Stochastic Gradient Descent: **SGD_youtube_explanation, SGD_wiki, GD_wiki**

Ο αλγόριθμος αυτός θα χρησιμοποιηθεί τόσο στην ανάλυση των δεδομένων όσο και στην ταυτοποίηση

Gradient Descent:

Παρατίθεται σύντομη εισαγωγή της μεθόδου Gradient Descent(κατάβασης κλίσης), έτσι ώστε να γίνει πιο κατανοητή η Stochastic Gradient Descent(Στοχαστική Κατάβαση Κλίσης)

Παρατίθεται το παρακάτω παράδειγμα μέσω του γραφήματος **(Figures GD)** που αναπαριστά την σχέση ύψους με βάρος ενός ατόμου, στον κατακόρυφο άξονα ύψος και στον οριζόντιο το βάρος. Στο παράδειγμα έχουμε τρία παραδείγματα και θέλουμε να τοποθετήσουμε την γραμμή απόφασης (γραμμή η οποία αναπαριστά την αναλογία ύψους-βάρους). Για την εύρεση της γραμμής χρησιμοποιούμε την εξίσωση: Predicted Height = intercept+lambda *Weight, ο στόχος μας είναι να ανακαλύψουμε τις ιδανικότερες τιμές για το intercept και lambda. Στην συνέχεια εφαρμόζουμε τον αλγόριθμο ως εξής:

Φάση 1: Ορίζουμε αρχικές τιμές για το intercept,lambda(π.χ. intercept=0 και lambda=1) και learning rate (καλή πρακτική είναι να τα ξεκινούμε με σχετικά μεγάλη τιμή ~0,1 και να το μειώνουμε σταδιακά)

Φάση 2: Υπολογίζουμε το predicted Height

Φάση 3: Χρησιμοποιούμε την εξίσωση: square_error=(Observed_Height-Predicted_Height)^2

Φάση 4: Αθροίζουμε όλα τα λάθη σε μια loss function για να υπολογίσουμε πόσο καλή αναπαράσταση κάνει η γραμμή στα δεδομένα μας.

Φάση 5: Υπολογίζουμε square_error=(Observed_Height- (intercept+lambda *Weight))^2

Φάση 6: Υπολογίζουμε την παράγωγο του σφάλματος ως προς το intercept τοποθετώντας τα δεδομένα που υπάρχουν(τύπος παραγώγου: $\Sigma\, d/d_{intercept}$=-2(Height-(intecept+lambda*Weight)))→($d/d_{intercept}$=-2*(1.4- (0+1 *0.5)+ 2*(1.9- (0+1 *2.3) +2*(3.2- (0+1 *2.9))

Φάση 7: Υπολογίσουμε την παράγωγο του σφάλματος ως προς το lambda τοποθετώντας τα δεδομένα που υπάρχουν(τύπος παραγώγου: $\Sigma\, d/d_{lambda}$=-2*Weight*(Height-

(intecept+lambda*Weight)))→(d/d_{lambda}=-2*0.5(1.4- (0+1 *0.5)+ 2*2.3(1.9- (0+1 *2.3) +2*2.9(3.2- (0+1 *2.9))

Φάση 8: Υπολογίζουμε $Step\_Size_{intercept}$=intercept*Learning_Rate ($Step\_Size_{intercept}$=-1.6*0.01)

Φάση 9: Υπολογίζουμε $Step\_Size_{lambda}$=lambda*Learning_Rate ($Step\_Size_{lambda}$ =-0.8*0.01)

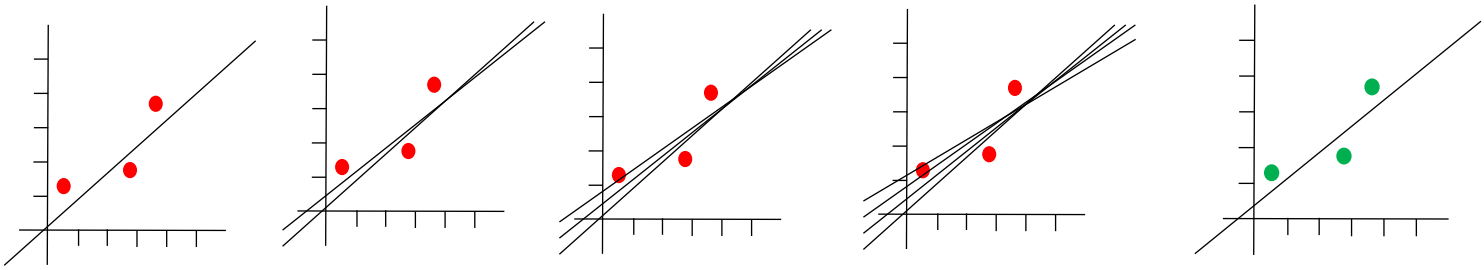
Φάση 10: Υπολογίζουμε $New_{intercept}$=$Old_{intercept}$-$Step\_Size_{intercept}$ ($New_{intercept}$=0-(-0.016))

Φάση 11: Υπολογίζουμε New_{lambda}=Old_{lambda}-$Step\_Size_{lambda}$ (New_{lambda}=1-(-0.008))

Φάση 12: Επαναλαμβάνουμε τις φάσεις 6-11 μέχρι να έχουμε απειροελάχιστες αλλαγές στα intercept και lambda ή να ξεπεράσουμε τον μέγιστο αριθμό προσπαθειών που ορίστηκε

Στόχος μας είναι να βρεθεί η βέλτιστη γραμμή απόφασης. Στο πιο πάνω παράδειγμα είχαμε μόνο τρία στοιχεία για κάθε παράγωγο. Αντιλαμβανόμαστε ότι η πολυπλοκότητα άρα κι ο χρόνος εκτέλεσης αλγορίθμου αυξάνεται εκθετικά όσο αυξάνεται ο αριθμός των στοιχείων και το πλήθος των στοιχείων των παραγώγων(στο συγκεκριμένο παράδειγμα είναι δύο).

Σημείωση: Τα κόκκινα σημεία αναπαριστούν σημεία που χρησιμοποιούνται για τον υπολογισμό της παραγώγου ενώ τα πράσινα όχι.

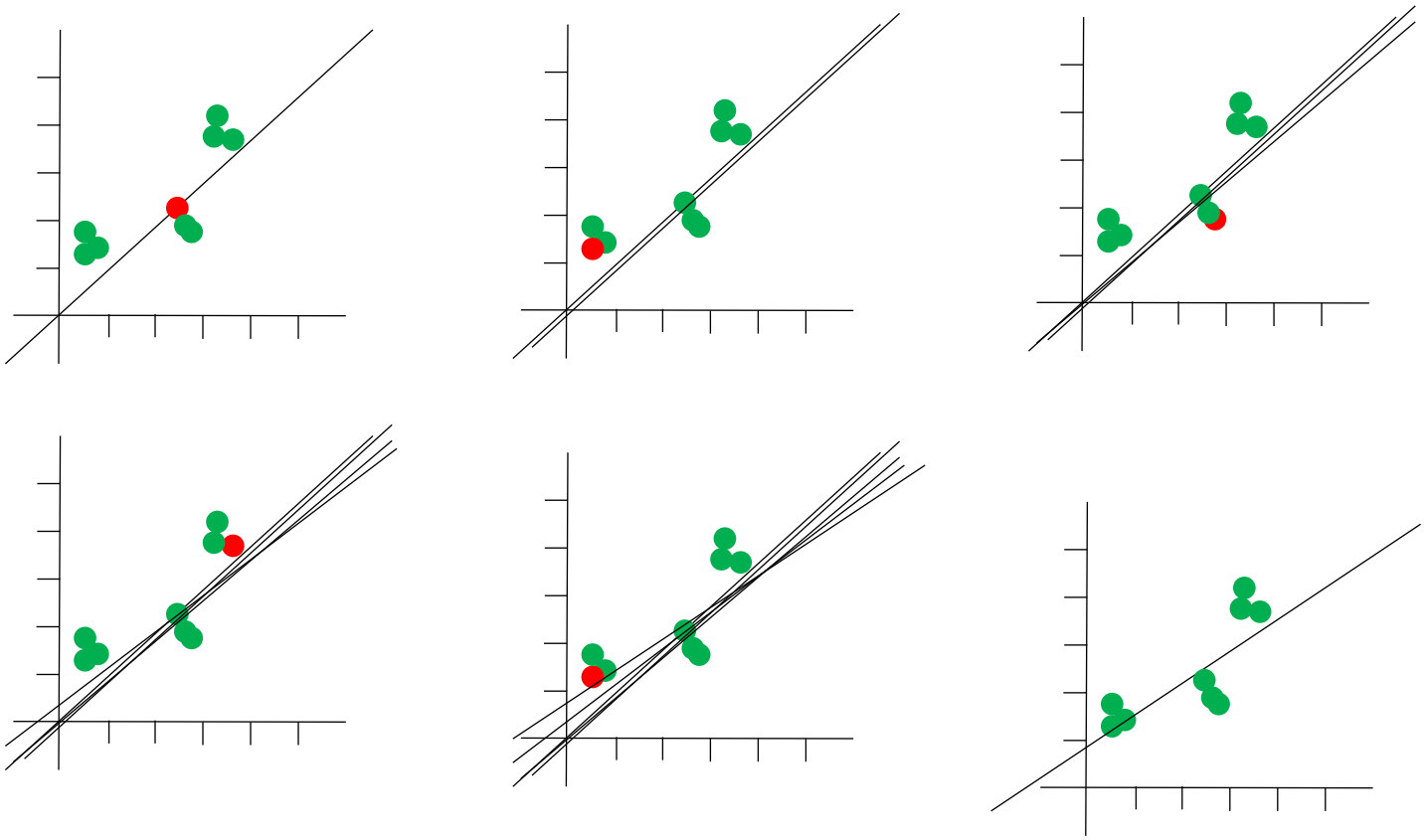


(figures GD)

Stochastic Gradient Descent:

Ακολουθούμε την ίδια διαδικασία με την gradient descent αλλά επιλέγουμε ένα μόνο τυχαίο σημείο κάθε φορά για να υπολογίσουμε τις παραγώγους.

Ακολουθούν στιγμιότυπα του αλγορίθμου με κάθε νέο στιγμιότυπο να έχει όλες τι προηγούμενες γραμμές εκτός του πρώτου και του τελευταίου.



(figures SGD)

Μια παραλλαγή του αλγορίθμου η οποία χρησιμοποιεί k σημεία (αριθμός επιλέγεται από εμάς) δείχνει ότι με σωστό αριθμό k πετυχαίνουμε καλύτερα αποτελέσματα (Σημείωση: Το συγκεκριμένο παράδειγμα που δόθηκε αναπαριστά δεδομένα στον δισδιάστατο χώρο, τα δεδομένα τα οποία χρησιμοποιούμε βρίσκονται σε χώρο πέντε διαστάσεων (λόγου του πλήθους δεδομένων που χρησιμοποιείται) ο οποίος είναι αδύνατος να αναπαρασταθεί σχηματικά, μια αναπαράσταση στον δισδιάστατο χώρο δίνει την γενική ιδέα λειτουργίας του αλγορίθμου αυτού.)

3.4 Support Vector Classification: **SVM_youtube_explanation,**

Ο αλγόριθμος αυτός θα χρησιμοποιηθεί τόσο στην ανάλυση των δεδομένων όσο και στην ταυτοποίηση.

Ανήκει στην ίδια κατηγορία αλγορίθμων με τον SGD και έχει παρόμοιο τρόπος λειτουργίας, ανήκει στην οικογένεια αλγορίθμων “Support Vector Machines”

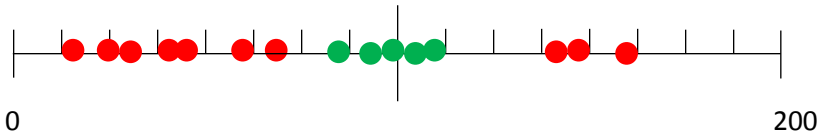
Support Vector Machines

Παρατίθεται σύντομη εισαγωγή της μεθόδου Support Vector Machine έτσι ώστε να γίνει πιο κατανοητή η Support Vector Classification

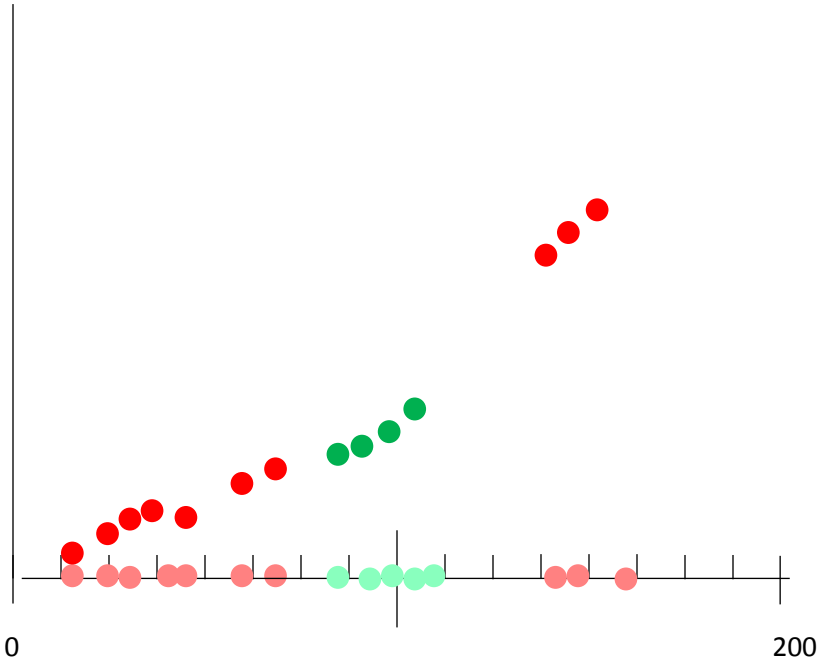
Παρατίθεται το παρακάτω παράδειγμα μέσω του γραφήματος**(Figure SVM_Basic)** που αναπαριστά τη μάζα ενός ατόμου, οι κόκκινες κουκκίδες αναπαριστούν άτομα τα οποία δεν είναι υπέρβαρα, ενώ οι πράσινες κουκκίδες άτομα που είναι. Στη συνέχεια θέτουμε ένα κατώφλι(ανάλογα με τις διαστάσεις του προβλήματος στην συγκεκριμένη περίπτωση είναι σημείο, αφού τα δεδομένα είναι σε μια ευθεία) το οποίο θα διαχωρίζει τις δύο κατηγορίες. Όποιο σημείο ανήκει δεξιά από το κατώφλι θα είναι υπέρβαρος ενώ όποιο βρίσκεται στα αριστερά δεν θα είναι(το κατώφλι θα αναπαρίσταται με μια ευθεία μπλε κάθετη γραμμή για ευκολότερη κατανόηση). Η απόσταση από το κοντινότερο σημείο στο κατώφλι από κάθε πλευρά λέγεται margin. Όταν η απόσταση αυτή είναι ίση και από τις δύο κατηγορίες τότε έχουμε Maximal Margin Classifiers, αλλά υστερεί εάν υπάρχουν outliers όπως φαίνεται και με το γράφημα**(Figure SVM_MMC),** δηλαδή εάν υπάρχει κάποιος που δεν είναι υπέρβαρος αλλά έχει περισσότερα κοινά χαρακτηριστικά με την κατηγορία των υπέρβαρων(π.χ. ένας αθλητής bodybuilding έχει παρόμοια μάζα με τους υπέρβαρους αλλά δεν ανήκει σε αυτή την κατηγορία). Για να επιλύσουμε το πρόβλημα αυτό επιτρέπουμε μερικούς λανθασμένους υπολογισμούς και εφαρμόζουμε Soft Margin Classification/Support Vector Classification. Για την εύρεση του ιδανικού Soft Margin χρησιμοποιούμε τεχνική Cross Validation για να καθορίσουμε πόσους “ λανθασμένους υπολογισμούς ” και πόσες “ παρατηρήσεις ” θα επιτρέψουμε και θα χρησιμοποιήσουμε την μέθοδο αυτή για να καθορίσουμε το θέση του κατωφλίου. Αξίζει να σημειωθεί ότι εάν προστεθεί και άλλη παράμετρος(παράδειγμα το ύψος) το κατώφλι δεν θα είναι σημείο αλλά γραμμή όπως φαίνεται από το γράφημα **(Figure SVM_2D)**. Στη περίπτωση του προβλήματος της διπλωματικής έχουμε πέντε στοιχεία άρα οι κλάσεις θα διαχωρίζονται από υπερεπιφάνεια τεσσάρων διαστάσεων το οποίο δεν μπορεί να αναπαρασταθεί γραφικά.

Παρατίθεται σχηματική αναπαράσταση επίλυσης του προβλήματος:

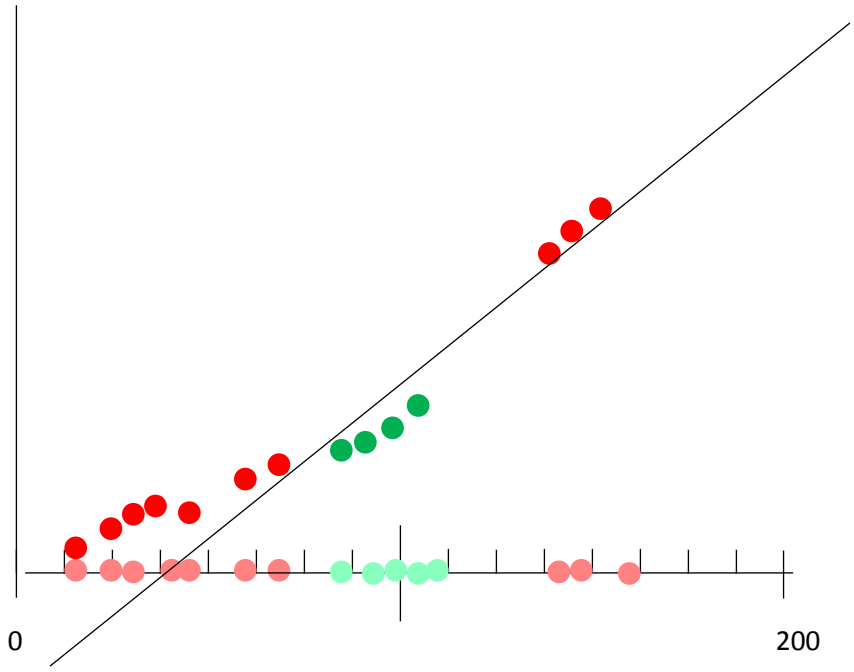
Φάση 1: Τοποθετούμε τα γνωστά δεδομένα στη διάσταση την οποία βρίσκονται(στο παράδειγμα είναι στην πρώτη διάσταση)



Φάση 2: Αναγάγουμε τα δεδομένα σε μεγαλύτερη διάσταση μέσω ενός kernel function(εδώ υψώνουμε την τιμή του σημείου στο τετράγωνο και δημιουργούμε προβολή του σημείου στον άξονα y) (τα σημεία που δεν έχουν έντονο χρώμα είναι τα σημεία πριν την αναγωγή, ενώ τα σημεία με έντονο χρώμα είναι μετά)



Φάση 3: Χρησιμοποιούμε τον αλγόριθμο SVC για να βρούμε το κατώφλι



Εάν επιθυμούμε να τα ανάγουμε σε τρίτη διάσταση θα πάρουμε και την τιμή στον κύβο. Το πρόβλημα δημιουργείται όταν θέλουμε να ανάγουμε ένα πρόβλημα σε διαστάσεις μεγαλύτερες των τριών. Για την επίλυση του προβλήματος αυτού χρησιμοποιούμε την συνάρτηση πυρήνα (kernel function) Radial Basis Function(RBF) που μπορεί να ανάγει το πρόβλημα σε άπειρες διαστάσεις.

Σημείωση: η αναγωγή σε μεγαλύτερη διάσταση δεν υλοποιείται αλλά υπολογίζονται οι σχέσεις των σημείων σαν να είχαν αναχθεί. Με τον τρόπο αυτό μειώνεται το κόστος υπολογισμού και επιτρέπει την αναγωγή σε πολύ μεγάλου αριθμού διαστάσεις

Radial Basis Function (RBF): RBF_youtube_explanation, RBF_wiki, Taylor_Series_wiki

Ο RBF συμπεριφέρεται σαν τον αλγόριθμο Weighted Nearest Neighbor, δηλαδή τα σημεία που βρίσκονται πιο κοντά στο σημείο που θέλουμε να υπολογίσουμε έχουν μεγαλύτερη επιρροή στην κατηγοριοποίηση του σημείου, ενώ τα σημεία που βρίσκονται μακριά από αυτό έχουν

σχετικά μικρότερη επιρροή στην κατηγοριοποίηση του. Για τον υπολογισμό των νέων σημείων ο RBF χρησιμοποιεί την εξίσωση: $e^{-\gamma(a-b)^2}$ όπου το γ χρησιμοποιείται για να ορίσει την επίδραση που θα έχει η εξίσωση(όσο πιο χαμηλή τιμή έχει τόσο μεγαλύτερη επίδραση έχει), το a και b είναι οι συντεταγμένες στο μονοδιάστατο χώρο.

Τρόπος λειτουργείας RBF για αναγωγή σε υψηλότερες διαστάσεις:

Φάση 1: Υπολογίζουμε το τετράγωνο $e^{-\gamma(a-b)^2} \rightarrow e^{-\gamma(a^2+b^2-2ab)} \rightarrow e^{-\gamma(a^2+b^2)} * e^{\gamma*2*a*b}$

Φάση 2: Ορίζουμε τιμή για το γ(π.χ. γ=1/2)$\rightarrow e^{-1/2*(a^2+b^2)} * e^{1/2*2ab} \rightarrow) \rightarrow e^{-1/2*(a^2+b^2)} * e^{ab}$

Φάση 3: Ορίζουμε την σειρά Taylor για το τελευταίο στοιχείο**(figure Taylor_Series, Taylor_Series_e_basic)**

Φάση 4: Θέτουμε το a=0, αφού εξορισμού μπορούμε να χρησιμοποιήσουμε οποιαδήποτε f(a) υπάρχει($e^0=1 \rightarrow$υπάρχει) **(figure Taylor_Series_e_simplified)**

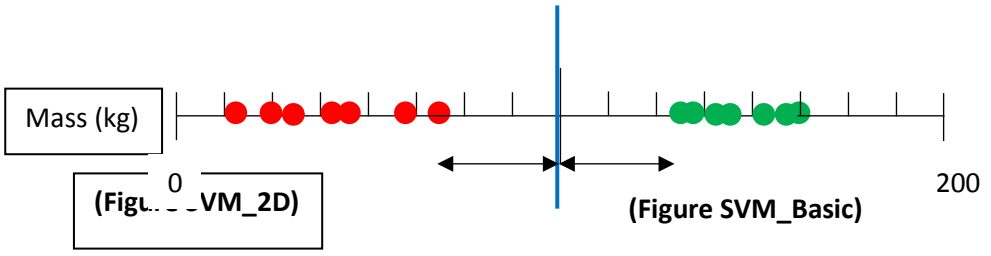
Φάση 5: Αντικαθιστούμε το e^x με e^{ab} για υπολογίσουμε το αποτέλεσμα για το τελευταίο στοιχείο**(figure Taylor_Series_e_ab)**

Φάση 6: Αντικαθιστούμε το e^{ab} στην αρχική εξίσωση **(Figure Dot_product_e^ab, Next_equation)**

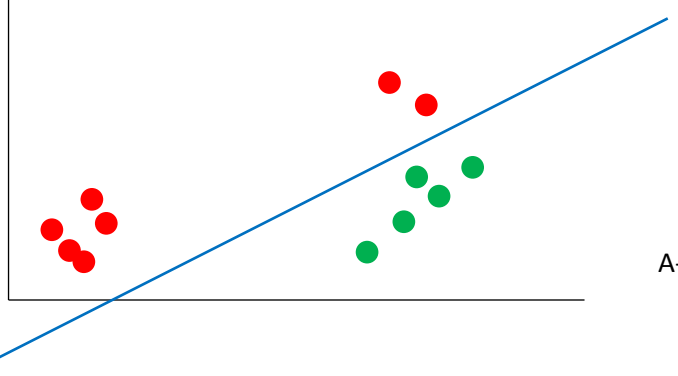
Φάση 7: Πολλαπλασιάζουμε με ρίζα τα δύο μέρη του γινομένου και πολλαπλασιάζουμε με s **(Figure set_s, Final_equation)**

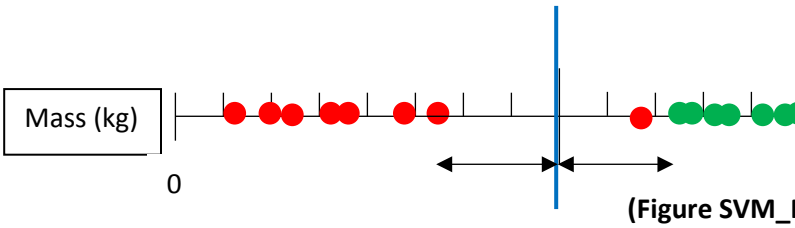
Φάση 8: Δημιουργήσαμε συντεταγμένες για άπειρες διαστάσεις

Φάση 9: Τοποθετώντας τις συντεταγμένες στην αρχική εξίσωση και αναπτύσσοντας τις πιο πάνω μαθηματικές εξισώσεις περνούμε τη σχέση μεταξύ δύο σημείων σε άπειρες διαστάσεις



(Figure SVM_Basic)





$$f(x) = f(a) + \frac{f'(a)}{1!}(x-a) + \frac{f''(a)}{2!}(x-a)^2 + \frac{f'''(a)}{3!}(x-a)^3 + \cdots + \frac{f^{\infty}(a)}{\infty!}(x-a)^{\infty}$$

(Figure Taylor_Series)

$$e^x = e^a + \frac{e^a}{1!}(x-a) + \frac{e^a}{2!}(x-a)^2 + \frac{e^a}{3!}(x-a)^3 + \cdots + \frac{e^a}{\infty!}(x-a)^{\infty}$$

(Figure Taylor_Series_e_Basic)

$$e^x = 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots + \frac{1}{\infty!}x^{\infty}$$

(Figure Taylor_Series_e_simplified)

$$e^{ab} = 1 + \frac{1}{1!}ab + \frac{1}{2!}(ab)^2 + \frac{1}{3!}(ab)^3 + \cdots + \frac{1}{\infty!}(ab)^{\infty}$$

(Figure Taylor_Series_e_ab)

$$e^{ab} = (1, \sqrt{\frac{1}{1!}}a, \sqrt{\frac{1}{2!}}a^2, \sqrt{\frac{1}{3!}}a^3, \ldots, \sqrt{\frac{1}{\infty!}}a^\infty) \cdot (1, \sqrt{\frac{1}{1!}}b, \sqrt{\frac{1}{2!}}b^2, \sqrt{\frac{1}{3!}}b^3, \ldots, \sqrt{\frac{1}{\infty!}}b^\infty)$$

(Figure Dot_product_e^ab)

$$e^{-\frac{1}{2}(a-b)^2} = e^{-\frac{1}{2}(a^2+b^2)} \left[(1, \sqrt{\frac{1}{1!}}a, \sqrt{\frac{1}{2!}}a^2, \ldots, \sqrt{\frac{1}{\infty!}}a^\infty) \cdot (1, \sqrt{\frac{1}{1!}}b, \sqrt{\frac{1}{2!}}b^2, \ldots, \sqrt{\frac{1}{\infty!}}b^\infty) \right]$$

(Figure Next_equation)

$$s = \sqrt{e^{-\frac{1}{2}(a^2+b^2)}}$$

(Figure set_s)

$$e^{-\frac{1}{2}(a-b)^2} = (s, s\sqrt{\frac{1}{1!}}a, s\sqrt{\frac{1}{2!}}a^2, \ldots, s\sqrt{\frac{1}{\infty!}}a^\infty) \cdot (s, s\sqrt{\frac{1}{1!}}b, s\sqrt{\frac{1}{2!}}b^2, \ldots, s\sqrt{\frac{1}{\infty!}}b^\infty)$$

(Figure Final_equation)