Ατομική Διπλωματική Εργασία

BUILDING AN AI SMART SECURITY SYSTEM FOR HOME USING M1W DOCK

Πρόδρομος Γεωργίου

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μάιος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Building an AI Smart Security System for Home Using M1W Dock

Πρόδρομος Γεωργίου

Επιβλέπων Καθηγητής
κ. Ανδρέας Πιτσιλλίδης

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

Μάιος 2020

ΕΥΧΑΡΙΣΤΙΕΣ

Για την υλοποίηση της διπλωματικής μου εργασίας, ήταν αρκετά χρήσιμη η βοήθεια από τον επιβλέπων καθηγητή μου Δρ. Ανδρέας Πιτσιλλίδης, ο οποίος κατά τη διάρκεια πραγματοποίησης της διπλωματικής μου ήταν σε εγρήγορση κάθε στιγμή που χρειαζόμουν τη βοήθεια και την καθοδήγηση του. Έτσι, θα ήθελα να τον ευχαριστήσω για την πολύτιμη βοήθεια που μου παρείχε κατά τη διάρκεια της διπλωματικής μου εργασίας και για την εμπιστοσύνη που μου έδειξε ούτως ώστε να παρουσιάσω ένα αξιόλογο αποτέλεσμα.

Ωστόσο, τόσο η οικογένεια μου όσο και οι φίλοι μου με υποστήριζαν και με εμψύχωναν όλους αυτούς τους μήνες, αφού ήταν μια πιεστική περίοδος για έμενα. Γι' αυτό νιώθω έντονη την ανάγκη για να τους ευχαριστήσω, για την κατανόηση που έδειξαν.

ΠΕΡΙΛΗΨΗ

Εδώ και αρκετά χρόνια, έχει ενταχθεί η τεχνολογία στις ζωές μας και αναπτύσσεται συνεχώς με ραγδαίους ρυθμούς. Γενικά η τεχνολογία μπορεί να χρησιμοποιηθεί για να ωφελήσει τον άνθρωπο και έχει αλλάξει ριζικά τον τρόπο ζωής μας. Μια σημαντική αναβάθμιση στη ζωή μας αποτελεί η δημιουργία συστημάτων προστασίας του ανθρώπου από κακόβουλες ενέργειες. Καθημερινά παρουσιάζονται διάφορα συμβάντα που αποσκοπούν στην παράνομη εισβολή σε ιδιωτικές περιουσίες. Έτσι, δημιουργήθηκαν διάφορα συστήματα προκειμένου να αποφευχθούν αυτά τα είδη ενεργειών για την ασφάλεια του κάθε ανθρώπου. Το Internet Of Things (IoT) αποτελεί μια συνεχώς αναπτυσσόμενη τεχνολογία η οποία θα μπορέσει να ελαχιστοποιήσει την πραγμάτωση τέτοιων συμβάντων.

Στη διπλωματική μου εργασία θα βασιστώ σε ένα όρο που έχει γίνει γνωστός τα τελευταία χρόνια ονομαζόμενος ως «Smart Home – Έξυπνο Σπίτι». Αναλυτικότερα, θα ασχοληθώ με τη δημιουργία ενός Artificial Intelligence (AI) Security System for Home using M1w Dock Tool Kit. Χρησιμοποιώντας την συγκεκριμένη τεχνολογία, ο κάτοικος του σπιτιού θα διαχειρίζεται ένα σύστημα ασφαλείας εκμεταλλευόμενος έτσι την αυτοματοποίηση και διασύνδεση που παρέχει ένα έξυπνο σπίτι. Μέσω του συστήματος αυτού θεωρητικά, όταν κάποιος βρεθεί στην εμβέλεια του συστήματος αυτομάτως αυτό αναγνωρίζει εάν το συγκεκριμένο άτομο εμπίπτει στον κοινωνικό κύκλο του ιδιοκτήτη. Οι αλγόριθμοι στους οποίους βασίστηκε η αναγνώριση του προσώπου στο σύστημα ήταν ο Local Binary Patterns Histograms (LBPH) , ο Eigenfaces και ο Fisherfaces.

Προκειμένου να διαχειρίζεται το σύστημα ασφαλείας πιο εύκολα ο διαχειριστής, δημιουργήθηκε μια ιστοσελίδα υλοποιημένη στο framework Laravel. Πιο συγκεκριμένα, ο διαχειριστής έχει την δυνατότητα εγγραφής και διαγραφής χρηστών οι οποίοι θα εγκρίνονται ή θα απορρίπτονται από το σύστημα αντίστοιχα και θα παρακολουθεί οποιαδήποτε κίνηση η οποία καταγράφτηκε από αυτό. Επιπρόσθετα, για περεταίρω αυτοματοποίηση του συστήματος όταν κάποιος χρήστης βρεθεί στην εμβέλεια του, ο διαχειριστής αυτόματα λαμβάνει ειδοποίηση στο προσωπικό του email πως κάποιος προσπαθεί να εισέλθει στο χώρο. Εν κατακλείδι, θα υπάρχει μια πλήρης

εικόνα με τις μετακινήσεις προς το σπίτι, εκμεταλλεύοντας στο μέγιστο την τεχνολογία και διατηρώντας έτσι το αίσθημα της ασφάλειας.

ΠΕΡΙΕΧΟΜΕΝΑ

Table of Contents

Κεφάλαιο 1

Εισαγωγή

1.1 Γενική Εισαγωγή

Βρισκόμαστε στην ψηφιακή εποχή η οποία άλλαξε ριζικά τον τρόπο ζωής μας και αυτό αναμφισβήτητα οφείλεται στη δημιουργία του διαδικτύου. Το διαδίκτυο χρησιμοποιήθηκε πρώτη φορά για ιδιωτική χρήση κατά την περίοδο 1984 – 1989 [1]. Στα μετέπειτα χρόνια, οι δυνατότητες που παρέχει το διαδίκτυο έχουν αυξηθεί δραματικά. Για παράδειγμα, το διαδίκτυο προσφέρει δυνατότητες άμεσης επικοινωνίας ανεξαιρέτου αποστάσεως, δυνατότητα άμεσης αναζήτησης πληροφοριών σε ελάχιστο χρόνο κ.α.. Η περεταίρω αναβάθμιση του διαδικτύου απαιτεί την δημιουργία μιας καινούργιας εποχής όπου θα καλύπτει όλες τις υπάρχουσες και νέες ανάγκες αλλά και την πραγμάτωση της αυτοματοποίησης της ζωής μας . Ο όρος Internet of Things αποτελεί τη λύση για την επίτευξη μιας καινούργιας αυτοματοποιημένης εποχής.

Είναι γεγονός ότι εκμεταλλεύοντας τις δυνατότητες που προσφέρει το IoT δημιουργείτε η έννοια του έξυπνου σπιτιού - «Smart Home». Το έξυπνο σπίτι δημιουργήθηκε με σκοπό να σκέπτεται και να ενεργεί με βάση τις ανάγκες και τις συνήθειες των κατοίκων. Κατ' επέκταση το έξυπνο σπίτι αναβάθμισε σε μεγάλο βαθμό τον τομέα της οικονομίας, της άνεσης και της ασφάλειας.

1.2 Περιγραφή και Κίνητρο

Κατά την περίοδο 1990 με 2000 τα συμβάντα κλοπής αυξήθηκαν από 58,8 περιστατικά ανά 100.000 κάτοικους σε 114,3 περιστατικά ανά 100.000 κατοίκους στις κεντρικές και ανατολικές χώρες [3]. Επιπλέον μετά από μελέτη άλλων ερευνών, παρατηρήθηκε ότι το 2016 στις Ευρωπαϊκές χώρες (34 χώρες) διαπράχθηκαν 1070 ληστείες κάθε 100.000 κατοίκους. Με βάση τα προαναφερθέντα στατιστικά δημιουργείται η ανάγκη ανάπτυξης καινούργιων τεχνολογικών συστημάτων τα οποία θα προστατεύουν τις περιουσίες των ανθρώπων. Με την ανάπτυξη της τεχνολογίας και του IoT δίνεται η δυνατότητα εφεύρεσης και ανάπτυξης τέτοιου είδους συστημάτων.

Ο τομέας της ασφάλειας εδώ και χρόνια δεν είχε υποστεί κάποια αξιοσημείωτη αναβάθμιση. Οι τεχνολογίες προηγούμενων γενιών δεν παρείχαν τη δυνατότητα εγγύησης ασφάλειας του ατόμου καθώς επίσης και της περιουσίας του. Ένα έξυπνο σπίτι προσφέρει πλήθος λειτουργιών οι οποίες κατοχυρώνουν μεγαλύτερη ασφάλεια και προστασία της προσωπικής ιδιοκτησίας.

Προηγουμένως δεν υπήρχε άμεσος τρόπος ενημέρωσης του ιδιοκτήτη σε τυχόν συμβάν παραβίασης προσωπικής ιδιοκτησίας και κλοπής προσωπικών αντικειμένων. Με τη δημιουργία του έξυπνου σπιτιού τα κρούσματα ληστείας προβλέπεται να ανιχνεύονται και να αντικρούονται με μεγάλη πιθανότητα σε ελάχιστο χρονικό διάστημα. Ένα χαρακτηριστικό παράδειγμα όταν επιχειρείται κάποια διάρρηξη θα ενεργοποιείται αυτόματα ο συναγερμός, ο φωτισμός του σπιτιού και θα ειδοποιείται στο προσωπικό του τηλέφωνο ο ιδιοκτήτης για το συμβάν και ενδεχομένως με τις σωστές ρυθμίσεις να ενημερώνεται και η αστυνομία. Επιπρόσθετα, ο ιδιοκτήτης μπορεί να έχει την δυνατότητα οπτικής παρακολούθησης της οικίας οπουδήποτε και αν βρίσκεται, μέσω των καμερών οι οποίες θα βρίσκονται εγκατεστημένες και θα μεταφέρουν την εικόνα του σπιτιού στο κινητό τηλέφωνο ή στον υπολογιστή του σε πραγματικό χρόνο.

1.3 Στόχος εργασίας και συνεισφορά

Ο κύριος στόχος της διπλωματικής εργασίας αποτελεί την υλοποίηση και δημιουργία ενός έξυπνου συστήματος ασφάλειας προκειμένου να επιτευχθεί η προστασία της ιδιοκτησίας των ανθρώπων. Για την επίτευξη ενός ολοκληρωμένου συστήματος, θα γίνει χρήση του εργαλείου M1W Dock Tool Kit το οποίο έχει εγκατεστημένο δικό του λογισμικό. Το σύστημα θα είναι εγκατεστημένο στην είσοδο του σπιτιού και οποιοσδήποτε βρεθεί στην εμβέλεια αυτού, θα τον καθοδηγεί για να τον φωτογραφίσει με απλές εντολές (Εικόνα 1.1). Όταν το σύστημα φωτογραφήσει το άτομο που επιθυμεί να εισέλθει στο σπίτι, θα είναι σε θέση να κρίνει αν είναι γνωστό γνωστό άτομο ή όχι. Τέλος, η είσοδος στο σπίτι θα επιτρέπεται μόνο σε «γνωστά» άτομα του συστήματος.

Το σύστημα θα είναι σε θέση να αναγνωρίζει τα «γνωστά» άτομα μέσω εκπαίδευσης αλγορίθμου αναγνώρισης προσώπου. Λόγω της κρισιμότητας της απόφασης που θα λαμβάνει το σύστημα, θα γίνει σύγκριση τριών διαφορετικών αλγορίθμων που προσφέρονται από την βιβλιοθήκη της Python, την “OpenCV”. Συγκεκριμένα, στόχος είναι η επιλογή του πιο αποτελεσματικού αλγορίθμου, που σε διαφορετικές καταστάσεις θα δίνει ορθή απάντηση στο άτομο που προσπαθεί να εισέλθει στο σπίτι.

Όταν κάποιο άτομο, «γνωστό» ή «άγνωστο» προσπαθεί να εισέλθει στο σπίτι ο ιδιοκτήτης θα λαμβάνει αυτόματα ειδοποίηση στο προσωπικό του email ακόμη και αν δεν βρίσκεται εντός της οικίας. Επιπρόσθετα, θα δημιουργηθεί μια ιστοσελίδα στην οποία θα διαχειρίζεται ο ιδιοκτήτης τα «γνωστά» ή «άγνωστα» άτομα. Η ιστοσελίδα θα παρουσιάζει στον ιδιοκτήτη χρήσιμες πληροφορίες για το εργαλείο που χρησιμοποιεί και θα του δίνεται η δυνατότητα για την επεξεργασία των «γνωστών» ατόμων. Με αυτό τον τρόπο θα δημιουργηθεί ένα πλήρως αυτοματοποιημένο σύστημα ασφαλείας χαμηλού κόστους και ταυτόχρονα η αναβάθμιση της ασφάλειας πραγματοποιείται.

Εικόνα 1.1: Οθόνη M1W Dock Toolkit με απεικόνιση τις εντολές της

1.4 Δομή Εργασίας

Κεφάλαιο 1: Το συγκεκριμένο κεφάλαιο περιλαμβάνει γενική περιγραφή για την ανάπτυξη της τεχνολογίας και του διαδικτύου. Ακολούθως, αναφέρονται κάποια στατιστικά στοιχεία που με ώθησαν στην δημιουργία και ανάπτυξη του συστήματος ασφαλείας. Τέλος γίνεται αναφορά στον στόχο της διπλωματικής εργασίας.

Κεφάλαιο 2: Στο κεφάλαιο 2 αναφέρονται οι τεχνολογίες οι οποίες είναι απαραίτητες για το σύστημα και η ιστορική τους ανάπτυξη με το πέρασμα του χρόνου (IoT, Smart Home). Στη συνέχεια, περιγράφεται η αναγνώριση προσώπου αλλά και το πως επιτυγχάνεται μέσω της βιβλιοθήκης OpenCV. Εν κατακλείδι, αναλύεται το υπόβαθρο των τεχνολογιών που θα χρησιμοποιηθούν.

Κεφάλαιο 3: Στο κεφάλαιο 3 περιγράφεται η μεθοδολογία η οποία ακολουθήθηκε για την ανάπτυξη και ολοκλήρωση του συστήματος. Αρχικά, γίνεται περιγραφή και αναλύονται οι δυνατότητες του hardware και του software που χρησιμοποιήθηκε. Τέλος, περιγράφεται εις βάθος η λειτουργία των αλγορίθμων και η μεθοδολογία που επιλέχθηκε για την υλοποίηση του προγράμματος αναγνώρισης προσώπου.

Κεφάλαιο 4: Στο κεφάλαιο 4 περιγράφεται λεπτομερώς η ανάπτυξη του συστήματος της Laravel. Πιο συγκεκριμένα, περιγράφονται κάποιες σημαντικές λειτουργίες που προσφέρει η Laravel και παρουσιάζονται σημαντικά στοιχεία της ιστοσελίδας (πίνακες που είναι απαραίτητοι για την βάση δεδομένων και οι κύριες διεπιφάνειες τις ιστοσελίδας).

Κεφάλαιο 5: Στο κεφάλαιο 5 γίνεται αξιολόγηση των τριών αλγορίθμων που χρησιμοποιήθηκαν. Περιγράφονται οι παράμετροι που καθορίζουν σε μεγάλο βαθμό την απόδοση των αλγορίθμων. Ακολούθως, γίνεται αξιολόγηση των παραμέτρων αλλά και της απόδοσης των αλγορίθμων (χρόνος εκτέλεσης, εκπαίδευσης και confidence).

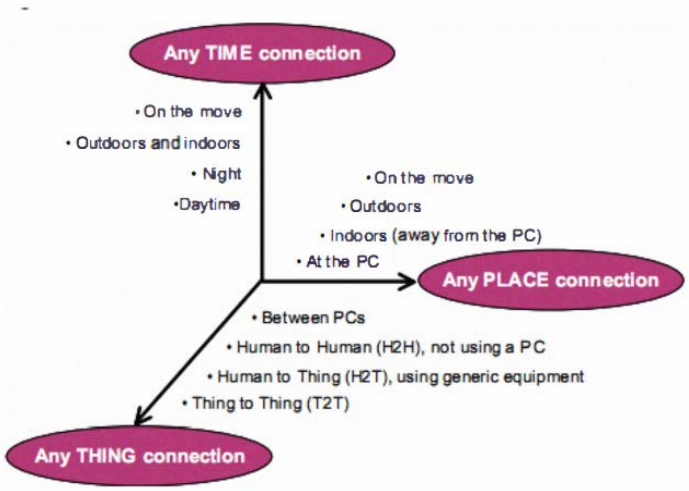
Κεφάλαιο 6: Στο τελευταίο κεφάλαιο περιγράφονται τα συμπεράσματα που εξήγαγα από την ανάλυση των αλγορίθμων και γίνεται αναφορά στα μελλοντικά πλάνα τα οποία μπορούν να αναβαθμίσουν το συγκεκριμένο σύστημα.

Κεφάλαιο 2

Background

2.1 Internet of Things

Το Internet of Things ορίζεται ως ένα σύστημα αλληλένδετων υπολογιστικών συσκευών, ψηφιακών μηχανών, αντικειμένων, ζώων ή προσώπων που θα διαθέτουν μοναδικά αναγνωριστικά στοιχεία (unique ID). Έτσι, δημιουργείται η δυνατότητα μεταφοράς δεδομένων μέσω του διαδικτύου χωρίς να απαιτείται η παρέμβαση ανθρώπου με ανθρώπου (human – human) ή ανθρώπου με υπολογιστή (human – computer). Οι συσκευές θα έχουν την δυνατότητα να ενώνονται απευθείας στο διαδίκτυο και να ανταλλάσσουν πληροφορίες μεταξύ τους. Από οποιοδήποτε σημείο και αν βρίσκεται ο άνθρωπος, ανά πάσα χρονική στιγμή θα μπορεί να επικοινωνήσει ή να συνδεθεί με οποιαδήποτε συσκευή π.χ. κινητό τηλέφωνο ή υπολογιστή (Εικόνα 2.1)[4]. Συνοψίζοντας εκμεταλλεύοντας τη συγκεκριμένη τεχνολογία η καθημερινότητα του ανθρώπου θα διευκολυνθεί σε μεγάλο βαθμό.



Εικόνα 2.1: Σχηματική απεικόνιση της λειτουργίας του IoT [4]

2.1.1 History of IoT

Η βασική ιδέα των συνδεδεμένων συσκευών προήλθε από τις αρχές του 1970, η οποία ονομαζόταν "embedded internet" ή "pervasive computing". Ο όρος Internet of Things προήλθε από τον Kevin Ashton κατά την διεκπεραίωση κάποιας μελέτης το 1999 στην οποία παρουσίασε τις δυνατότητες της τεχνολογίας παρακολούθησης RFID (Radio Frequency Identification). Την επόμενη χρονιά η LG ανακοίνωσε την δημιουργία του πρώτου «έξυπνου» ψυγείου. Το 2009 η Google προχώρησε στις πρώτες δοκιμές στην αυτόνομων αυτοκινήτων. Την ίδια χρονιά δημιουργήθηκε το πλέον γνωστό bitcoin το οποίο αποτέλεσε τον πρόδρομο των τεχνολογιών "blockchain", οι οποίες στο μέλλον θα εξελίσσονταν ως ένα πολύ σημαντικό κομμάτι του IoT. Οκτώ χρόνια αργότερα, το 2017, το IoT έχει πλέον ενσωματωθεί σε διάφορους τομείς της ζωής μας, αφού η ανάπτυξη του έχει γίνει πιο αποδεκτή, φτηνή αλλά και πιο εύκολη.[2]

2.2 «Έξυπνο Σπίτι» - Smart Home

Οι έντονοι ρυθμοί του σύγχρονου τρόπου ζωής δημιουργούν διαρκώς νέες ανάγκες, οι οποίες απαιτούν ειδική διαχείριση από ένα σύστημα αυτοματισμών και ελέγχου. Η φράση "έξυπνο σπίτι" χρησιμοποιείται για οποιαδήποτε οικία, ενσωματώνει σε κάποιο βαθμό τη δυνατότητα

ρύθμισης και ελέγχου ορισμένων ηλεκτρομηχανολογικών εγκαταστάσεων. Με αυτό το τρόπο το «έξυπνο σπίτι» αποτελεί μια αυτοματοποιημένη εκδοχή των ποικίλων λειτουργιών που απαιτούνται στο σπίτι.

Ένα έξυπνο σπίτι αποτελείται από διάφορες συσκευές όπως ο θερμοστάτης, ψυγεία, φούρνοι, συστήματα κάμερας και ασφάλειας ακόμη και ο φωτισμός οι οποίες ελέγχονται απομακρυσμένα από τον ιδιοκτήτη. Ο έλεγχος αυτός επιτυγχάνεται μέσω εφαρμογής η οποία είναι εγκατεστημένη πάνω στο κινητό τηλέφωνο του ιδιοκτήτη ή μέσω του διαδικτύου ή με προκαθορισμένο χρόνο ο οποίος είναι προγραμματισμένος εκ των προτέρων. Πιο αναλυτικά, το Smart Home συμπεριλαμβάνει αντικείμενα στα οποία υπάρχουν ενσωματωμένοι αισθητήρες συνδεδεμένους σε ένα κεντρικό κόμβο. Οι αισθητήρες αυτοί, παρέχουν την δυνατότητα να επικοινωνούν απευθείας μεταξύ τους και ανταλλάζουν δεδομένα χωρίς να απαιτείται η άμεση παρέμβαση από τον χρήστη. Με λίγα λόγια η δημιουργία των «Smart Homes» συνεπάγεται με την αναβάθμιση της ρουτίνας του ατόμου με όσο το δυνατόν περισσότερη αυτοματοποίηση, διευκολύνοντας την όσο το καλύτερο δυνατόν. [5]

2.2.1 History of Smart Homes

Στις αρχές του 20ου αιώνα, η βιομηχανική επανάσταση αποτέλεσε τη θεμελιώδη λίθο για μια «έκρηξη» τεχνολογικών ανακαλύψεων. Αρχικά εισάχθηκαν στην ζωή των ανθρώπων οι πρώτες οικιακές συσκευές οι οποίες δεν θεωρούνταν ως «έξυπνες» ακόμα, αλλά αποτελούσαν σημείο καμπής για τη καθημερινότητα των ανθρώπων. Η πρώτη αυτοματοποιημένη ιδέα το «Echo IV» για το σπίτι υλοποιήθηκε το 1966, αλλά δεν κατάφερε να γινεί εμπορικό προϊόν λόγω του υψηλού κόστους αγοράς. Το 1971 μετά την δημιουργία του πρώτου μικροελεγκτή, οι τιμές των ηλεκτρονικών συσκευών έγιναν πιο προσιτές για το μέσο καταναλωτή. Προς το τέλος του 20^{ου} αιώνα εισήχθησαν καινούργιες τεχνολογίες στη ζωή των ανθρώπων. Οι αρχές του 21^{ου} αιώνα στιγματίστηκαν από την δραματική αύξηση των έξυπνων τεχνολογιών. Διάφορες τεχνολογίες άρχισαν να ενσωματώνονται στα σπίτια, όπως ο έξυπνος οικιακός αυτοματισμός (αυτοματοποιημένος έλεγχος θέρμανσης της οικίας κ.α.), καθιστώντας έτσι την ζωή των ανθρώπων πιο εύκολη. [5]

2.3 Face Recognition – Αναγνώριση Προσώπου

Αναγνώριση προσώπου ονομάζεται η διαδικασία ταυτοποίησης ενός προσώπου από μια ψηφιακή εικόνα ή από βίντεο. Υπάρχουν πολλαπλοί τρόποι αναγνώρισης προσώπου, έχουν ως κοινό κανόνα λειτουργίας την λήψη των χαρακτηριστικών του προσώπου από μια εικόνα και ακολούθως συγκρίνονται με τις εικόνες που βρίσκονται αποθηκευμένες σε μια βάση δεδομένων. Στην ουσία αποτελεί μια κατηγορία βιομετρικού λογισμικού τα οποία χαρτογραφούν μαθηματικά συγκεκριμένα χαρακτηριστικά προσώπου και τα αποθηκεύουν ως ένα αποτύπωμα προσώπου. Η αναγνώριση προσώπου χρησιμοποιείται κυρίως σε συστήματα ασφαλείας και μπορεί να συγκριθεί με άλλους βιομετρικούς τρόπους αναγνώρισης κάποιου ατόμου (δακτυλικά αποτυπώματα, iris recognition)[6].

2.3.1 History of Face Recognition

Η έννοια της αναγνώρισης προσώπου προήλθε από τον Woodrow Wilson Bledsoe την δεκαετία του 60΄, ο οποίος δημιούργησε ένα σύστημα το οποίο οργάνωνε τις εικόνες χρησιμοποιώντας Rand tablet. Μέσω του συστήματος αυτού, οι ανθρώπου είχαν την δυνατότητα να καταγράφουν τις συντεταγμένες που βρίσκονταν τα χαρακτηριστικά του προσώπου και να τα αποθηκεύουν. Το 1983 προτάθηκε το principal component analysis (PCA) για την εξαγωγή χαρακτηριστικών από την εικόνα. Το 1988 εισάχθηκε η γραμμική άλγεβρα για την βελτίωση της αναγνώρισης προσώπου χρησιμοποιώντας το PCA, η οποία ονομάστηκε προσέγγιση Eigenfaces. Τρία χρόνια αργότερα, το 1991 αποτελεί βασικό ορόσημο για την ανάπτυξη της τεχνολογίας αφού ανακαλύφθηκαν τρόποι εξαγωγής προσώπων από φωτογραφίες χρησιμοποιώντας την προσέγγιση του Eigenfaces από τους Pentland και Turk. Πιο συγκεκριμένα, ήταν η πρωταρχική προσπάθεια αναγνώρισης προσώπου χρησιμοποιώντας τεχνολογικούς και περιβαλλοντικούς παράγοντες για εύρεση προσώπου στην εικόνα. Στον $21^{ο}$ αιώνα συνέχισαν να εμφανίζονται και να εξελίσσονται νέες τεχνολογίες στο ευρύτερο τομέα της ασφάλειας. Κάποια συγκεκριμένα παραδείγματα που γίνεται χρήση αυτοματοποιημένης αναγνώρισης προσώπου είναι σε

αεροδρόμια για αναγνώριση επιβατών και στην αναγνώριση θυμάτων από τον στρατό της Αμερικής [7].

2.3.2 Face Recognition OpenCV

OpenCV

Open Source computer vision (OpenCV) είναι βιβλιοθήκη της Python η οποία στοχεύει στην επίλυση open - vision προβλημάτων. Η συγκεκριμένη βιβλιοθήκη έχει δυνατότητες αναγνώρισης και ταυτοποίησης προσώπων, είτε από φωτογραφίες, είτε σε αληθινό χρόνο (real–time video).

Face Recognition OpenCV

Για την υλοποίηση της πτυχιακής εργασίας θα γίνει χρήση της βιβλιοθήκης OpenCV η οποία θα χρησιμοποιηθεί για την δημιουργία αλγορίθμων αναγνώρισης προσώπου οι οποίοι θα χρησιμοποιηθούν από το σύστημα. Η αναγνώριση προσώπου είναι ένας τρόπος αναγνώρισης ατόμων χωρίς να επέμβει ο άνθρωπος και είναι πιο γρήγορο από άλλες μεθόδους αναγνώρισης αφού έχει την δυνατότητα πολλαπλής αναγνώρισης προσώπων την ίδια χρονική στιγμή. Για την αναγνώριση κάποιου προσώπου απαιτεί την ανίχνευση προσώπου (face recognition) και την ταυτοποίησή του (face detection). Πιο συγκεκριμένα η ανίχνευση προσώπου, αποτελεί την διαδικασία εύρεσης των προσώπων στην εικόνα ή βίντεο. Ομοίως, η ταυτοποίηση προσώπου αποτελεί την διαδικασία ταυτοποίησης του προσώπου που βρέθηκε προηγουμένως στην εικόνα ή το βίντεο, μέσω σύγκρισης με την βάση δεδομένων που είναι καταχωρημένα όλα τα πρόσωπα [8]. Με το συνδυασμό αυτό, μπορεί να κατηγοριοποιηθεί με το σωστό όνομα το άτομο που βρίσκεται στην εικόνα ή βίντεο.

2.3.3 Haar-like Features

Μια μέθοδος για αναγνώριση προσώπων θα ήταν η χρησιμοποίηση χαρακτηριστικών ή συγκεκριμένων δομών από το πρόσωπο. Η ανίχνευση προσώπου σε κάποια φωτογραφία πραγματοποιείται συνδυάζοντας ένα συνδυασμό διαφορετικών χαρακτηριστικών (Haar–like

features). Ένα Haar–like feature θεωρεί γειτονικά ορθογώνιες περιοχές σε ένα παράθυρο ανίχνευσης, αθροίζει τα pixels στη κάθε περιοχή και υπολογίζει την διαφορά τους. Ένα χαρακτηριστικό παράδειγμα για την αναγνώριση προσώπου, είναι συνήθως οι περιοχές γύρω από τα μάτια σε σχέση με τις περιοχές στα μάγουλα [9]. Έτσι ανιχνεύοντας γειτονικά χαρακτηριστικά επιτυγχάνεται ο προσδιορισμός των μοναδικών χαρακτηριστικών του ατόμου.

2.3.4 Haar Cascade

Η αναγνώριση προσώπου θα επιτευχθεί με την χρήση Haar cascade classifiers. Ο Haar Cascade είναι αλγόριθμος μάθησης που αναγνωρίζει αντικείμενα ή πρόσωπα ο οποίος εκπαιδεύεται με θετικές αλλά και αρνητικές εικόνες. Ο αλγόριθμος αποτελείται από τέσσερα στάδια:

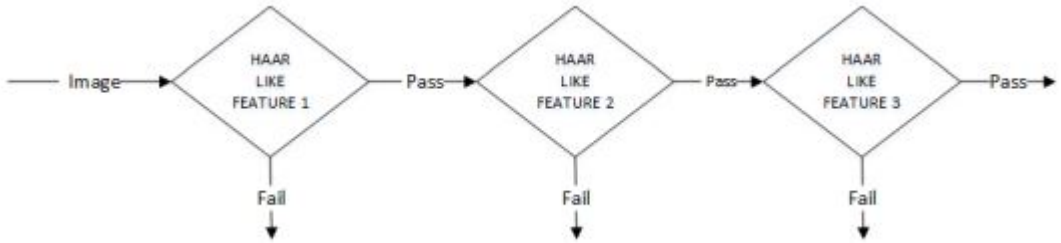
1) Επιλογή χαρακτηριστικών (Haar Feature Selection)
2) Δημιουργία σημαντικών εικόνων (Create Integral Images)
3) Εκπαίδευση Adaboost (Adaboost training)
4) Cascading Classifiers.

Στο πρώτο στάδιο γίνεται η επιλογή των χαρακτηριστικών όπως προ ειπώθηκε. Αναμενόμενο είναι πως μεταξύ των διαφόρων χαρακτηριστικών που εντοπίζεται, συγκεκριμένος αριθμός από αυτά θα καθίσταται αχρείαστος για την αναγνώριση προσώπου. Έτσι, επιβάλλεται να γίνει επιλογή των πιο σημαντικών χαρακτηριστικών από το γενικό σύνολο. Αυτό επιτυγχάνεται με την χρήση των integral images, οι οποίες αποτελούν μια δομή που υπολογίζει το άθροισμα των τιμών κάποιου υποσυνόλου της εικόνας, έτσι ώστε η διαδικασία να επιταχύνει. Ο στόχος είναι η μείωση του αριθμού των υπολογισμών που απαιτούνται για τη λήψη των εντάσεων των pixels μέσα σε ένα παράθυρο. Το Adaboost επιλέγει τα καλύτερα χαρακτηριστικά και εκπαιδεύει τους classifiers που θα χρησιμοποιηθούν. Ένας classifier δεν είναι επαρκής για ακριβή αποτελέσματα, έτσι σε συνδυασμό με άλλους classifiers επιτυγχάνεται η αναγνώριση προσώπου (Εικόνα 2.2). Κατά την διάρκεια της αναγνώρισης η εικόνα σαρώνεται από ένα μετακινούμενο παράθυρο για να υπολογιστούν τα Haar features (weak classifiers). Πιο συγκεκριμένα, ο αλγόριθμος σε κάθε στάδιο συμβολίζει την περιοχή που ορίζεται από το σημείο που βρίσκεται το μετακινούμενο παράθυρο ανάλογα αν ο συμβολισμός είναι θετικός ή αρνητικός. Θετικό είναι το στάδιο στο οποίο έχει ανιχνευθεί κάποιο πρόσωπο και αρνητικό το στάδιο στο οποίο δεν έχει

ανιχνευθεί. Αν το σύμβολο είναι αρνητικό τότε η κατηγοριοποίηση της περιοχής που βρίσκεται εντός του παραθύρου ολοκληρώνεται και στη συνέχεια το μετακινούμενο παράθυρο μετακινείται στην επόμενη περιοχή της εικόνας. Αντιθέτως, αν ο συμβολισμός της περιοχής είναι θετικός, ο classifier μεταβιβάζει την περιοχή στο επόμενο στάδιο. Συνεπώς, ο αλγόριθμός αυτός λειτουργεί με τέτοιο τρόπο έτσι ώστε να ανιχνεύονται αρνητικά δείγματα στην εικόνα πολύ γρήγορα με την υπόθεση ότι το ενδιαφερόμενο πρόσωπο δεν εμπεριέχεται στο μεγαλύτερο μέρος του μετακινούμενου παραθύρου. Με βάσει τα πιο πάνω, ο αλγόριθμος δεν εξάγει πάντοτε επιθυμητά αποτελέσματα. Έτσι το αποτέλεσμα του αλγορίθμου μπορεί να διαχωριστεί σε τρείς κατηγορίες:

- True positive: Συμβαίνει όταν ένα θετικό δείγμα κατηγοριοποιείται ορθά.
- False positive: Συμβαίνει όταν ένα αρνητικό δείγμα κατηγοριοποιείται ορθά.
- False negative: Συμβαίνει όταν ένα θετικό δείγμα κατηγοριοποιείται ως αρνητικό.

Ένας Haar classifier θεωρείται αποδοτικός όταν σε κάθε στάδιο έχει χαμηλό ρυθμό false negatives. Όταν εντοπιστεί ένα false negative τότε ο αλγόριθμος σταματά και κατ' επέκταση η κατηγοριοποίηση «παγώνει» και η διόρθωση του λάθους καθίσταται αδύνατη. Παρομοίως, αν εντοπιστεί ένα false positive τότε αυτή η περιοχή μεταφέρεται στο μετέπειτα στάδιο του αλγορίθμου. Προσθέτοντας περισσότερα στάδια στον αλγόριθμο μειώνεται ο ρυθμός εύρεσης των false positive, αλλά ταυτοχρόνως μειώνεται και ο ολικός ρυθμός εύρεσης true positive περιοχών. [8,9]



Εικόνα 2.2: Haar Cascade Classifier stages

Κεφάλαιο 3

Μεθοδολογία

3.1 Hardware

Για την υλοποίηση του συγκεκριμένου συστήματος υπήρχε ποικιλία εξαρτημάτων, όπως raspberry pi, Arduino ή κάποιο υλικό MaixPy. Μετά από μελέτη και σε συνεργασία με τον υπεύθυνο καθηγητή μου, αποφάσισα να υλοποιήσω το σύστημα χρησιμοποιώντας το υλικό που προσφέρει το MaixPy, το M1W Dock Tool Kit (Εικόνα 3.1). Εκμεταλλεύοντας τις δυνατότητες που προσφέρει το MaixPy μπορούμε να δημιουργήσουμε ένα έξυπνο σύστημα με ελάχιστο κόπο. Κάποια από τα πλεονεκτήματα που με ώθησαν στην χρήση του συγκεκριμένου υλικού είναι:

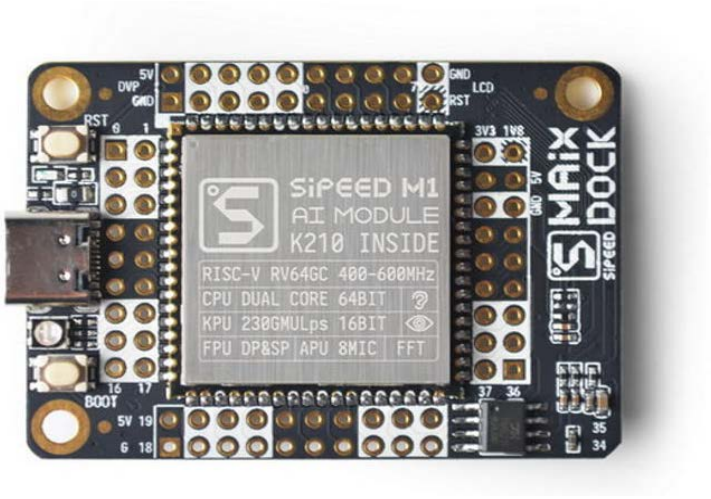
- Δεν αποτελεί ένα απλό υλικό (hardware) αλλά παρέχει υποδομή υλικού και λογισμικού για την διευκόλυνση της ανάπτυξης των λύσεων τεχνητής νοημοσύνης των πελατών.
- Η χαμηλή ισχύς και το χαμηλό κόστος επιτρέπει την ευρεία ανάπτυξη υψηλής ποιότητας τεχνητής νοημοσύνης.
- Συνδυάζει προσαρμοσμένο υλικό, ανοικτό λογισμικό και υπερσύγχρονους αλγορίθμους τεχνητής νοημοσύνης για να παρέχει υψηλής ποιότητας λύσεων τεχνητής νοημοσύνης καθώς και ευκολίες στη δημιουργία τους.
- Το συγκεκριμένο υλικό μπορεί να χρησιμοποιηθεί σε πολλούς τομείς. Συγκεκριμένα παραδείγματα εφαρμογών αποτελούν η προληπτική συντήρηση, ανίχνευση ανωμαλιών, μηχανική όραση (machine vision), ρομποτική, έξυπνα σπίτια, συγκοινωνίες, υγεία και άλλα.

3.1.1 M1W Dock Tool Kit

Βασικό εξάρτημα για την διεκπεραίωση της διπλωματικής εργασίας είναι το εξάρτημα M1W Dock Tool Kit. Αρχικά, το M1W Dock υποστηρίζει γλώσσα προγραμματισμού MaixPy, η οποία είναι η Micropython που είναι ενσωματωμένη στο chip Kendryte K210. Η Micropython είναι μια πιο απλή έκδοση και εφαρμογή της Python 3, η οποία αποτελείται από ένα υποσύνολο των βιβλιοθηκών της Python. Αποτελεί βελτιωμένη έκδοση για να εκτελείται σε μικροελεγκτές και περιορισμένα περιβάλλοντα. Τα κύρια χαρακτηριστικά που παρέχει το M1W Dock board είναι:

- Display – 4” (inches) Display with resolution 320 x 240 pixels
- Camera – 2MP (megapixels) camera OV2460
- Storage – microSD card slot
- Audio – Power amplifier IC for use with speakers, ενσωματωμένο μικρόφωνο
- USB – USB Type-C connector
- Kendryte K210 processing unit
- Διασυνδεσιμότητα:
  - ✓ Wi-Fi
  - ✓ I/Os

- ✓ On-board high speed DAC
- ✓ Access to all 72-pin full pin lead-out, freely mapable



Εικόνα 3.1: M1W MaixPy Dock

3.1.1.1 Kendryte K210

Μελετώντας άλλα machine vision boards κατέληξα στο συμπέρασμα ότι η συγκεκριμένη επιλογή θεωρείται η καλύτερη, αφού υπερτερεί σε όλους τους τομείς (*Πίνακας 3.1*). Πιο αναλυτικά, το συγκεκριμένο chip που είναι εγκατεστημένο στο M1W Dock είναι το πιο γρήγορο από το είδος του και έχει τεράστιο χώρο μνήμης RAM. Προσφέρει λύσεις τεχνητής νοημοσύνης, οι οποίες είναι:

- machine vision: face detection, face recognition, image classification base on CNN, general target detection based on CNN, λαμβάνει το μέγεθος και τις συντεταγμένες του στόχου σε αληθινό χρόνο, λαμβάνει τον τύπο του στόχου σε αληθινό χρόνο
- machine hearing: sound source orientation, sound field imaging, beamforming, voice wake up, speech recognition
- Καλύτερη ταχύτητα και ακρίβεια επεξεργασίας machine vision χαμηλής ισχύος
- Convolutional Artificial Neural Network Accelerator KPU, υψηλής απόδοσης Convolutional Artificial Neural network operation.
- Υποστηρίζει κρυπτογράφηση του firmware.

- Χαμηλότερη τάση και κατανάλωση ισχύος σε σχέση με άλλα συστήματα με την ίδια ισχύ επεξεργασίας.

Πίνακας 3.1: K210 vs Other Boards Specs

SPECS/BOARD	K210	ESP32	OPENMV M7	Pixy 2
No. of Cores	2	2	1	2
Architecture	64bit	32bit	32bit	32bit
CPU Frequency	400MHz	160MHz	216MHz	204Mhz
NN Hardware	Yes	No	No	No
Wi-Fi	Yes	Yes	No	No
RAM	8192 KB	512KB	512KB	264KB
FLASH	16MB	16MB	2MB	2MB

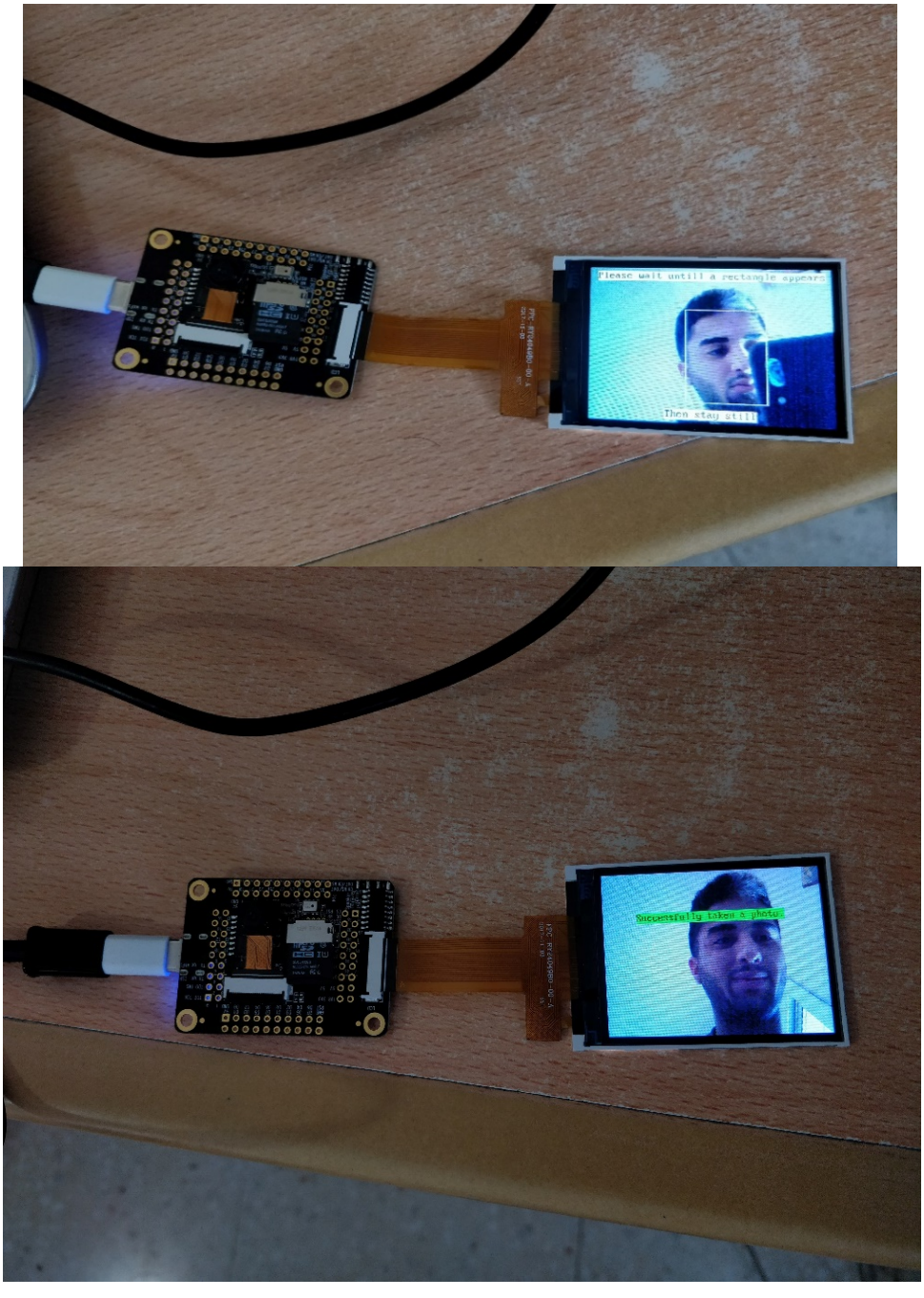
Συνοψίζοντας μπορεί να ειπωθεί ότι, το Kendryte K210 δημιουργήθηκε με σκοπό την ανάπτυξη του AIoT (συνδυασμός τεχνητής νοημοσύνης και δυνατοτήτων IoT), εκμεταλλεύοντας την ισχυρή απόδοση και το χαμηλό κόστος που προσφέρει. Η επανάσταση της τεχνητής νοημοσύνης έχει ήδη ξεκινήσει και αλλάζει ριζικά την καθημερινότητα μας, συστήματα και υλικά σαν αυτά θεωρούνταν επιστημονικής φαντασίας λίγα χρόνια πριν [10,11]

3.2 Τεχνολογίες Software

3.2.1 MaixPy IDE

Διαβάζοντας και αναλύοντας το documentation του MaixPy, θεωρήθηκε πιο εύκολο και κατανοητό να εγκατασταθεί το IDE που προσφέρει. Αρχικά, προτού ξεκινήσω την δημιουργία του προγράμματος εξαγωγής φωτογραφίας στο MaixPy IDE, έπρεπε να εγκαταστήσω το kflash_gui το οποίο είναι πλατφόρμα για εγκατάσταση των firmware (μοντέλα για λειτουργία του προγράμματος). Μετά από μελέτη εγκατέστησα το firmware face_model_at_0x300000.kfpkg. Για την χρήση του συγκεκριμένου μοντέλου και οποιουδήποτε άλλου μοντέλου επιθυμούσα έπρεπε να επαναλαμβάνω την διαδικασία εγκατάστασης του

firmware. Δηλαδή, το μοντέλο να γίνεται burn στη σωστή τοποθεσία της flash memory του επεξεργαστή. Στη συνέχεια αφού εγκατέστησα το επιθυμητό firmware, δημιούργησα ένα πρόγραμμα αναγνώρισης προσώπου και εξαγωγή φωτογραφίας. Όταν στην εμβέλεια του συστήματος ανιχνεύεται κάποιο άτομο, τον καθοδηγεί με απλές εντολές (*Εικόνα 1*). Το σύστημα έχει την δυνατότητα εξαγωγής φωτογραφίας αυτόματα μόλις αναγνωρίζει κάποιο πρόσωπο ή αναμένοντας κάποιο χρονικό διάστημα (Εικόνα 3.2). Ακολούθως, όταν ληφθεί φωτογραφία αποθηκεύεται στην κάρτα μνήμης που βρίσκεται ενσωματωμένη στο εξάρτημα και εμφανίζεται μήνυμα επιτυχίας (Εικόνα 3.3).



Εικόνα 3.3: Στάδιο μετά την λήψη φωτογραφίας

3.2.2 Laravel PHP Framework

Το software που χρησιμοποιήθηκε για την ανάπτυξη και δημιουργία της ιστοσελίδας διαχείρισης του συστήματος είναι το Laravel PHP Framework (η ανάλυση της Laravel θα γινεί εις βάθος στο κεφάλαιο 4 και το appendix).

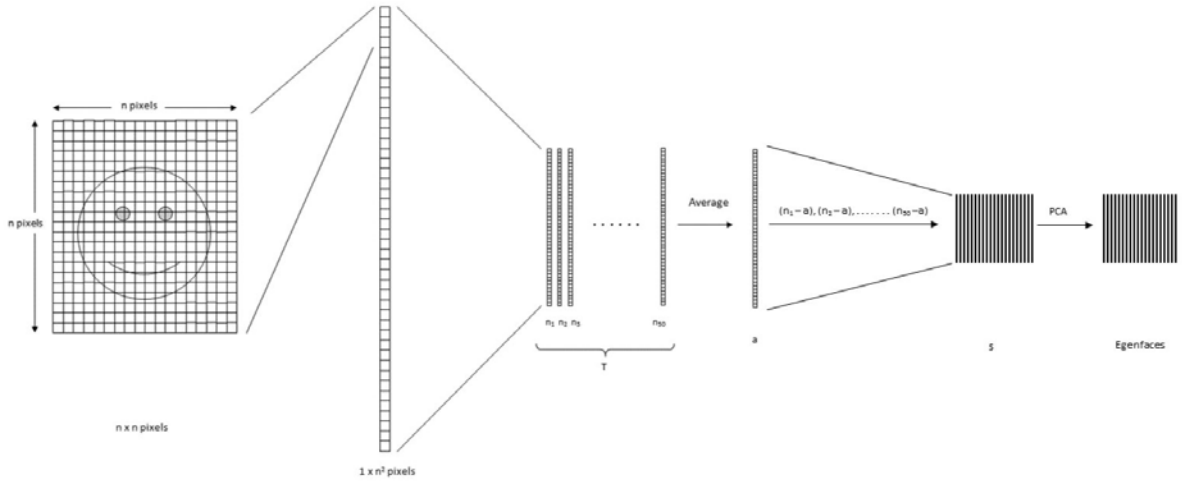
3.3 Αλγόριθμοι Αναγνώρισης Προσώπου

Στο κεφάλαιο 2 μελετήθηκε το υπόβαθρο της αναγνώρισης προσώπου, αλλά και η λειτουργία του μέσω της βιβλιοθήκης OpenCV της Python. Μέσω της χρήσης της συγκεκριμένης βιβλιοθήκης, χρησιμοποιήθηκαν τρεις διαφορετικοί αλγόριθμοι αναγνώρισης προσώπου ο Eigenfaces, Fisherfaces και ο LBPH Algorithm. Στο συγκεκριμένο κεφάλαιο θα γίνει περιγραφή και ανάλυση με λεπτομέρεια την λειτουργία των τριών αλγορίθμων. Ακολούθως, θα αναλυθεί η μεθοδολογία που ακολουθήθηκε λεπτομερώς, για το πώς θα αξιοποιηθούν οι τρείς αλγόριθμοι προκειμένου να πραγματοποιηθεί η αναγνώριση προσώπου του Έξυπνου Σπιτιού. Η μεθοδολογία αποτελείται από τρία βασικά στάδια, την ανίχνευση των προσώπων, την εξαγωγή των χαρακτηριστικών και τέλος την αναγνώριση προσώπου. Στο πρώτο στάδιο γίνεται προ επεξεργασία των εικόνων και δημιουργούνται οι εικόνες που απαρτίζουν τα datasets με τους haar classifiers. Το δεύτερο στάδιο αποτελεί την εξαγωγή των χαρακτηριστικών χρησιμοποιώντας τα haar features, integral images, cascade classifiers και του μοντέλου εκπαίδευσης. Τελευταίο βήμα αποτελεί η αναγνώριση προσώπου από τον αλγόριθμο αναγνώρισης, είτε τον LBPH, είτε τον Eigenfaces, είτε τον Fisherfaces.

3.3.2 Eigenfaces Algorithm

Ο αλγόριθμος Eigenfaces είναι βασισμένος στο PCA ο οποίος κατηγοριοποιεί τις φωτογραφίες για να εξάγει τα χαρακτηριστικά χρησιμοποιώντας ένα σύνολο φωτογραφιών. Απαραίτητη προϋπόθεση του συγκεκριμένου αλγόριθμου είναι οι εικόνες που προορίζονται για εκπαίδευση, να βρίσκονται σε παρόμοιες συνθήκες φωτισμού, τα μάτια να βρίσκονται σε εμφανή σημείο στην φωτογραφία και να υπάρχει σταθερό περιβάλλον.

Αρχικά υποθέτοντας ότι μια εικόνα αποτελείται από n x n pixels, κάθε γραμμή ενώνεται για την δημιουργία ενός διανύσματος 1 x n^2. Όλες οι εικόνες του dataset αποθηκεύονται σε ένα πίνακα, του οποίου η κάθε στήλη αντιπροσωπεύει μια εικόνα (άρα ο αριθμός των στηλών είναι ίσος με τον αριθμό των εικόνων που βρίσκονται στο dataset). Στη συνέχεια, ο πίνακας γίνεται normalized έτσι ώστε να δημιουργηθεί ο μέσος πίνακας που να αντικατοπτρίζει τις τιμές ενός μέσου ανθρώπινου προσώπου. Στο τέλος αφαιρείται η κάθε στήλη του πίνακα με τον μέσο πίνακα για να ανιχνευθούν τα μοναδικά χαρακτηριστικά του κάθε προσώπου. Οι στήλες του τελικού πίνακα αντιπροσωπεύουν μια αναπαράσταση της διαφοράς κάθε προσώπου από το μέσο πρόσωπο (*Εικόνα 3.4*) .



Εικόνα 3.4: Σχηματική απεικόνιση τρόπου λειτουργίας του Eigenfaces

Έπειτα, υπολογίζεται ο πίνακας συν διακύμανσης (covariance matrix) και χρησιμοποιώντας principal components analysis (PCA) υπολογίζονται τα διανύσματα eigen. Ακολούθως, δίνοντας ως είσοδο μια εικόνα για να γίνει αναγνώριση προσώπου, αναδιαμορφώνεται στο ίδιο μέγεθος όπως τις εικόνες της βάσης δεδομένων. Προβάλλοντας τα εξαγόμενα χαρακτηριστικά σε κάθε eigenface, υπολογίζονται τα βάρη. Αυτά τα βάρη αναπαριστούν την ομοιότητα των εξαγόμενων χαρακτηριστικών από τις διαφορετικές ομάδες εικόνων που βρίσκονται στο dataset με τα εξαγόμενα χαρακτηριστικά της εικόνας εισόδου. Ακολούθως, συγκρίνοντας την εικόνα εισόδου με ολόκληρο το dataset, μπορεί να αναγνωριστεί ένα πρόσωπο, πιο συγκεκριμένα συγκρίνοντας κάθε φορά με μια υποομάδα φωτογραφιών, το άτομο μπορεί να αναγνωριστεί. Θέτοντας μια οριακή τιμή (threshold) ανίχνευσης και αναγνώρισης εξαλείφεται η πιθανότητα εμφάνισης false detection και κατ' επέκταση αναγνώρισης.

Το PCA είναι ευαίσθητο σε μεγάλους αριθμούς και υποθέτει ότι ο χώρος είναι γραμμικός. Ωστόσο, αν το ίδιο πρόσωπο αναλύεται σε διαφορετικές συνθήκες φωτισμού, οι τιμές θα μπερδευτούν όταν υπολογίζεται η κατανομή και δεν μπορεί να κατηγοριοποιηθεί σωστά, με αποτέλεσμα να θέτει ένα σημαντικό πρόβλημα στην ταυτοποίηση των χαρακτηριστικών.[8]

Ο Eigenfaces με πιο απλά λόγια θεωρεί ότι τα μέρη του προσώπου δεν έχουν την ίδια βαρύτητα και δεν είναι εξίσου σημαντικά ή χρήσιμα για την αναγνώριση προσώπου. Ο συγκεκριμένος αλγόριθμος αναγνωρίζει κάποιο άτομο με βάση τα ξεχωριστά του χαρακτηριστικά, για παράδειγμα τα μάτια, τη μύτη, το μέτωπο, τα μάγουλα και πώς μεταβάλλονται σε σχέση μεταξύ τους.

Ο αλγόριθμος με βάση την πιο πάνω περιγραφή εστιάζει στους τομείς της μέγιστης αλλαγής. Όπως από τα μάτια μέχρι την μύτη υπάρχει μια σημαντική αλλαγή και το ίδιο ισχύει από τη μύτη μέχρι το στόμα. Όταν αναλύει πολλαπλά πρόσωπα, τα συγκρίνει μεταξύ τους εξετάζοντας τις συγκεκριμένες περιοχές, διότι με την αλίευση της μέγιστης διακύμανσης μεταξύ των προσώπων, βοηθά στο να διαφοροποιήσει το ένα πρόσωπο από το άλλο. Καταλήγουμε στο συμπέρασμα ότι, εξάγει τα συστατικά που είναι σχετικά και χρήσιμα και απορρίπτει τα υπόλοιπα.

3.3.3 Fisherfaces Algorithm

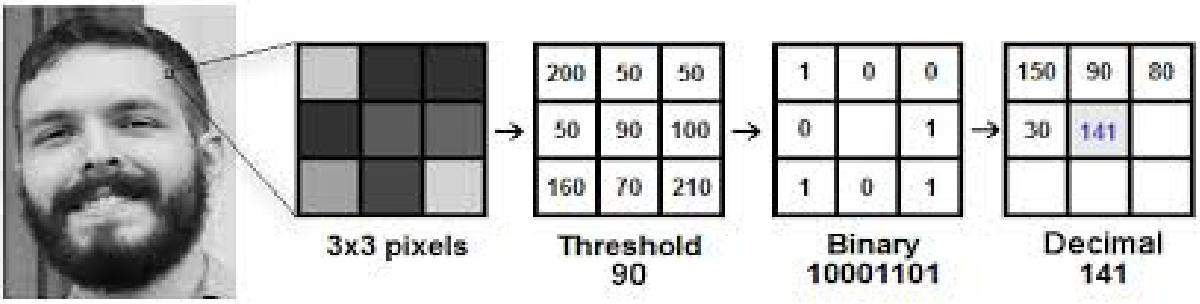
Ο αλγόριθμος Fisherfaces είναι μια βελτιστοποιημένη έκδοση του αλγορίθμου Eigenfaces ο οποίος είναι βασισμένος στο Linear Discriminant Analysis (LDA). Χρησιμοποιεί labels για τις κλάσεις καθώς επίσης και πληροφορίες μεταξύ αυτών. Κατά την διαδικασία μείωσης των διαστάσεων το LDA, δημιουργεί labels και ομαδοποιεί τις τάξεις που εν τέλει δημιουργούνται, ενώ ο PCA βασίζεται στην εύρεση της μέγιστης μεταβολής του πίνακα. Κύρια ιδέα είναι η μεγιστοποίηση της αναλογίας μεταξύ της κλάσης και των πινάκων της για να βρεθεί ο συνδυασμός των χαρακτηριστικών που διαχωρίζουν τις κλάσεις. Ο Fisherfaces μεγιστοποιεί την μέση απόσταση μεταξύ των διαφορετικών κλάσεων και ελαχιστοποιεί τις διακυμάνσεις εντός των κλάσεων. Οι διαφορετικές συνθήκες φωτισμού στις φωτογραφίες έχουν περιορισμένη επίδραση στη διαδικασία κατηγοριοποίησης του LDA. Αυτό καθιστά το LDA πιο ικανό να διαχωρίζει με βάση τα ξεχωριστά χαρακτηριστικά καλύτερα από την τεχνική PCA. Είναι αναγκαίο να σημειωθεί ότι ο Fisherfaces εξαρτάται σε μεγάλο βαθμό στα δεδομένα εισόδου, δηλαδή αν εκπαιδευτεί με φωτογραφίες με αρκετό φωτισμό μόνο και γίνει προσπάθεια εκπαίδευσης σε φωτογραφία χαμηλού φωτισμού, πιθανότατα θα εξαχθεί λανθασμένη πρόβλεψη αφού θα εντοπίσει λανθασμένα χαρακτηριστικά.

Με πιο απλά λόγια, αναφέρθηκε πιο πάνω ο αλγόριθμος Eigenfaces εξετάζει όλες τις εικόνες εκπαίδευσης και βρίσκει τα βασικά συστατικά από όλες τις εικόνες. Κάνοντας αυτό, δεν επικεντρώνεται στα χαρακτηριστικά που διακρίνουν ένα πρόσωπο από κάποιο άλλο, αντιθέτως ο Fisherfaces στοχεύει στην εξαγωγή ποικίλων σημαντικών και χρήσιμων χαρακτηριστικών τα οποία θα διαχωρίσουν το ένα άτομο από το άλλο.

Από όλα τα παραπάνω γίνεται φανερό ότι ο αλγόριθμος Fisherfaces είναι όμοιος με τον αλγόριθμο Eigenfaces αλλά με βελτιστοποιημένη κατηγοριοποίηση των διαφορετικών κλάσεων μιας εικόνας. Με τον τρόπο λειτουργίας του αλγόριθμου αυτού, όταν μια εικόνα έχει έντονο φωτισμό δε θα επηρεάσει σε μεγάλο βαθμό την διαδικασία εξαγωγής χαρακτηριστικών των άλλων εικόνων, προσφέροντας λύση στο πρόβλημα του φωτισμού ως ένα βαθμό αλλά δεν εξαλείφεται πλήρως. Γενικότερα όμως, θεωρείται ένας ικανός αλγόριθμος στην κατηγοριοποίηση και την διαφοροποίηση των ανθρώπινων εκφράσεων.

3.3.4 Local Binary Patterns Histograms (LBPH) Algorithm

Ο Eigenfaces και ο Fisherfaces χρησιμοποιούν μαθηματικές περιγραφές για την εξαγωγή των στοιχείων, ενώ ο LBPH αναλύει την κάθε εικόνα που βρίσκεται στο dataset ανεξάρτητα και ξεχωριστά. Ο αλγόριθμος LBPH δεν αναλύει την εικόνα σαν μια εικόνα ολόκληρη (1 κομμάτι) όπως τους προηγούμενους δύο αλγορίθμους, αλλά επιλέγει κάθε φορά μικρά κομμάτια συγκρίνοντας κάθε pixel με τα γειτονικά του pixels. Αναλύοντας περαιτέρω την λειτουργία του για την κωδικοποίηση των χαρακτηριστικών, η εικόνα χωρίζεται σε κελιά μεγέθους 3 x 3. Σε κάθε επανάληψη συγκρίνει όλα τα εξωτερικά pixels με το κεντρικό pixel. Η τιμή που έχει κάθε γειτονικό pixel συγκρίνεται με το κεντρικό pixel. Εάν οι γειτονικές τιμές είναι μεγαλύτερες από την τιμή του κεντρικού pixel τότε τους ανατίθεται η τιμή 1. Αντιθέτως αν οι τιμές τους είναι μικρότερες τότε παίρνουν την τιμή 0. Το αποτέλεσμα της κάθε επανάληψης του αλγορίθμου είναι μια 8-bit τιμή, διαβάζοντας την τιμή αρχίζοντας από πάνω αριστερά και έπειτα δεξιόστροφα όπως την φορά του ρολογιού. Το πλεονέκτημα του συγκεκριμένου αλγορίθμου είναι ότι εάν η φωτεινότητα της εικόνας αλλάξει το αποτέλεσμα (η 8-bit τιμή) θα είναι ακριβώς η ίδια. Ακολούθως, μετατρέπεται η 8-bit binary τιμή σε decimal και αποτελεί το καινούργιο κεντρικό pixel, έτσι δημιουργείται μια καινούργια εικόνα που απεικονίζει καλύτερα τα χαρακτηριστικά της εικόνας. Με αποτέλεσμα, γίνεται εξαγωγή του histogram για το συγκεκριμένο παράθυρο. Άρα με το πέρας της διαδικασίας γίνεται δημιουργία ενός μεγαλύτερου histogram, συγχωνεύοντας όλα τα μικρότερα σε ένα το οποίο αντιπροσωπεύει μια εικόνα με τα χαρακτηριστικά της από το dataset. Έτσι, ως αποτέλεσμα οι εικόνες του dataset κατηγοριοποιούνται. Κατά την διάρκεια της αναγνώρισης, δίνοντας ως είσοδο μια εικόνα κατηγοριοποιείται ακολουθώντας την ίδια διαδικασία, δημιουργείται το δικό της histogram και συγκρίνεται με τα υπόλοιπα που βρίσκονται αποθηκευμένα (σύγκριση στοιχείων histogram). Το histogram που έχει την μικρότερη απόσταση με το histogram εισόδου, του καθορίζεται το ανάλογο label. Με τον καθορισμό ενός κατωφλίου (threshold), μπορεί να προσδιοριστεί εάν το άτομο στην εικόνα είναι γνωστό ή άγνωστο (*Εικόνα 3.5*). [8]



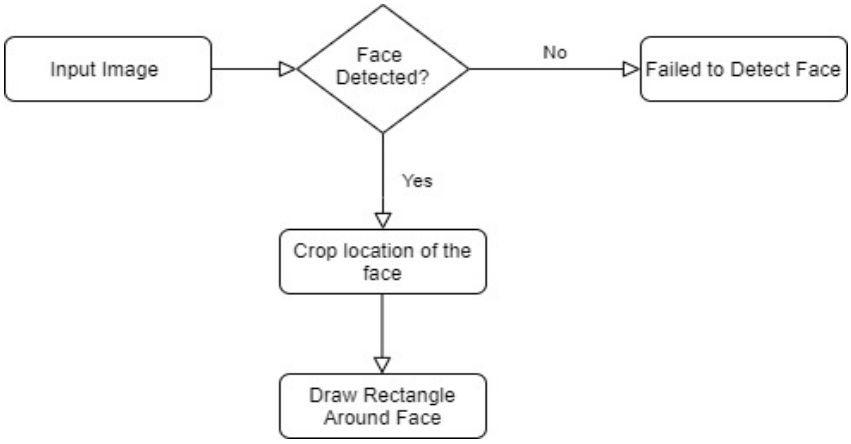
Εικόνα 3.5: LBPH παραγωγή 8-bit τιμής και μετατροπή σε decimal

3.4 Μεθοδολογία Υλοποίησης Αναγνώρισης Προσώπου

Στο συγκεκριμένο υποκεφάλαιο θα γίνει περιγραφή της διαδικασίας που ακολουθήθηκε για την υλοποίηση του προγράμματος αναγνώρισης προσώπου. Προτού, ξεκινήσει η περιγραφή, αξίζει να σημειωθεί ότι η ανάπτυξη του κώδικα έγινε στο περιβάλλον PyCharm IDE. Η χρήση του συγκεκριμένου IDE δεν έγινε τυχαία αφού παρέχει έξυπνη υποστήριξη, ωθεί στην καλύτερη ποιότητα κώδικα, αυξάνει την παραγωγικότητα και είναι απλό στην χρήση του.

Πρώτο βήμα για την ανάπτυξη του προγράμματος της αναγνώρισης προσώπου ήταν η δημιουργία του συστήματος χρησιμοποιώντας Haar-cascades, το οποίο εξηγήθηκε στο κεφάλαιο 2. Στο πρόγραμμα έγινε χρήση του haar_cascade_frontalface_default.xml ο οποίος αποτελεί προ-εκπαιδευμένο μοντέλο για την ανίχνευση προσώπων από εικόνες, για την δημιουργία αντικειμένων με πρόσωπα (objects). Όλες οι εικόνες που βρίσκονται στο dataset δόθηκαν ως είσοδοι στον classifier έτσι ώστε να ανιχνευθούν τα πρόσωπα. Απαραίτητη προϋπόθεση είναι η μετατροπή των φωτογραφιών από RBG μορφή σε gray_scale. Ο λόγος που συμβαίνει αυτό είναι γιατί όταν οι εικόνες βρίσκονται σε gray_scale μορφή είναι πιο εύκολο να επεξεργαστούν και απαιτείται λιγότερη υπολογιστική δύναμη αφού περιέχει μόνο 1 κανάλι, μαύρο – άσπρο. Ακολούθως, χρησιμοποιώντας την μέθοδο detectMultiScale ανιχνεύεται η περιοχή του προσώπου στην καινούργια εικόνα. Αυτό επιτεύχθηκε χρησιμοποιώντας όλα τα χαρακτηριστικά που είναι αποθηκευμένα στον face_classifier. Τέλος, χρησιμοποιώντας τα δεδομένα της

περιοχής του προσώπου περικόπτονται και προχωρούν για περεταίρω επεξεργασία. Εάν βρεθεί πρόσωπο τότε ένα τετράγωνο σχηματίζεται γύρω από την συγκεκριμένη περιοχή (*Εικόνα 3.6*).



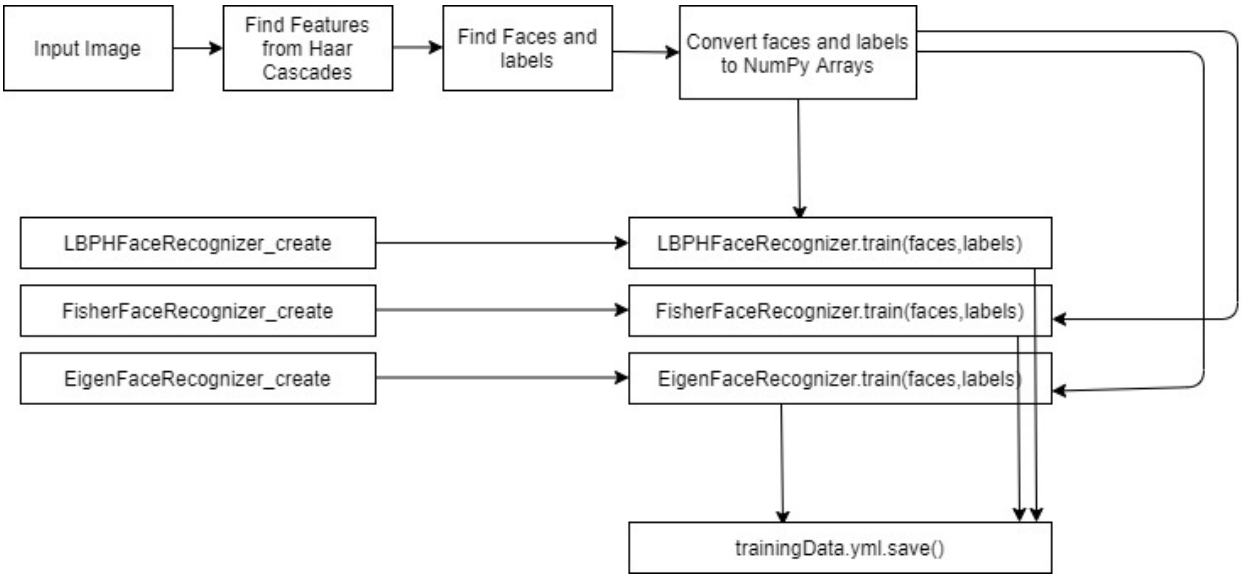
Εικόνα 3.6: Εικονική Απεικόνιση διαδικασίας Haar Classifier

Πιο αναλυτικά, κατά την διάρκεια αναγνώρισης προσώπου με την βιβλιοθήκη OpenCV απαιτούνται τρία κύρια στάδια. Το πρώτο στάδιο είναι η διαδικασία του labeling των εικόνων έτσι ώστε να τους καθοριστεί ένα συγκεκριμένο id. Το δεύτερο στάδιο αποτελεί την εξαγωγή των χαρακτηριστικών, κατηγοριοποιώντας τις εικόνες και αποθηκεύοντας τα σε ένα *YML* file, το οποίο στο τρίτο στάδιο χρησιμοποιείται για να γίνει σύγκριση των χαρακτηριστικών που είναι αποθηκευμένα με τα χαρακτηριστικά της εικόνας που δίνεται ως είσοδος. Έτσι, ο αλγόριθμος είναι σε θέση να αναγνωρίζει την ταυτότητα του συγκεκριμένου ατόμου που ευρίσκεται στην φωτογραφία εισόδου.

Το πρόγραμμα διαβάζει όλα τα αρχεία που βρίσκονται στον υποφάκελο trainingImages, το dataset εκπαίδευσης. Ειδικότερα, στο φάκελο trainingImages υπάρχουν υποφάκελοι ονομαζόμενοι «1», «2», «3» και ούτω καθεξής. Σε κάθε υποφάκελο υπάρχουν φωτογραφίες από ένα συγκεκριμένο άτομο του οποίου το πρόσωπο φαίνεται ξεκάθαρα έτσι ώστε να εκπαιδευτεί το *YML* file. Επιπρόσθετα, δημιουργείται ένα dictionary στο οποίο αντιστοιχεί κάθε υποφάκελο με το όνομα του ατόμου που τον απαρτίζει. Διαβάζοντας όλους τους υποφακέλους το αρχείο *YML* εκπαιδεύεται με τα χαρακτηριστικά προσώπου των ατόμων και τα κατηγοριοποιεί ανάλογα.

Εκπαίδευση των Classifiers

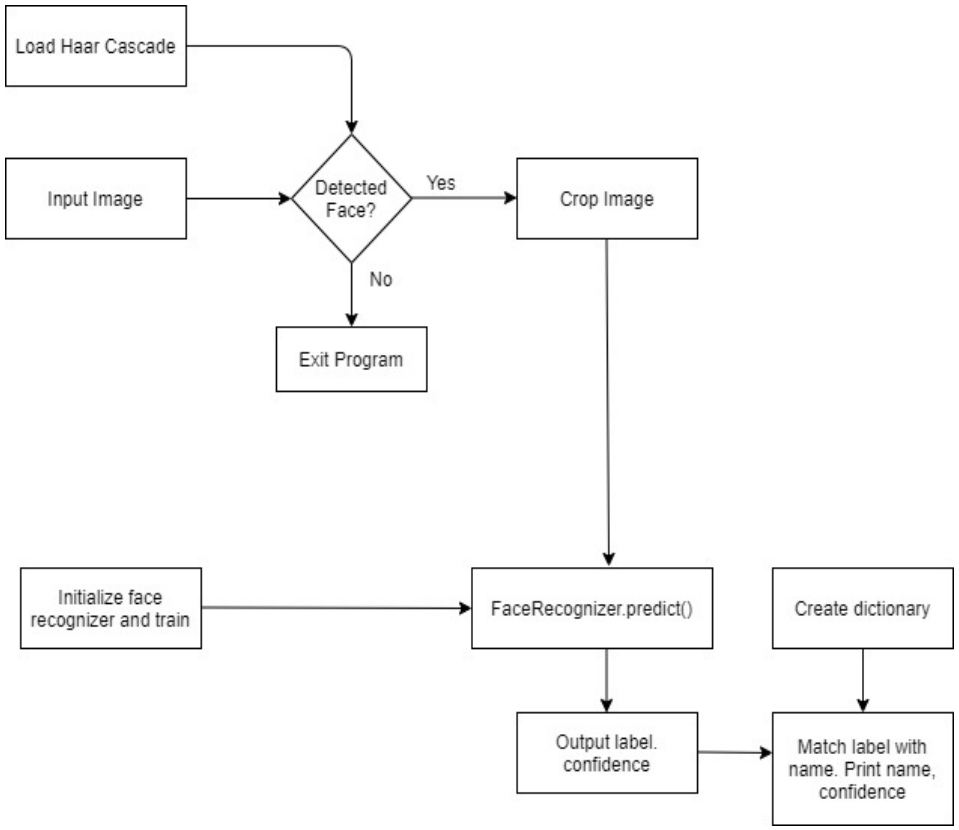
Στη συνέχεια, αρχικοποιείται ο αλγόριθμος που εκτελείται και τα δεδομένα που έχουν παρθεί από τις φωτογραφίες (χαρακτηριστικά των προσώπων) εκπαιδεύονται με τον συγκεκριμένο αλγόριθμο. Οι προαναφερθέντες αλγόριθμοι που εξηγήθηκαν πιο πάνω εκπαιδεύουν τα δεδομένα (πρόσωπα, ετικέτες - labels), eigenface, fisherface και LBPH και αποθηκεύονται στο YML file. Τα αντικείμενα των recognizer που δημιουργούνται, δηλαδή οι εικόνες, εισάγονται, αποκόπτονται και μετατρέπονται σε numpy πίνακες. Η μετατροπή σε numpy οφείλεται στην λειτουργία της OpenCV. Αξίζει να σημειωθεί, ότι μόνο στους αλγόριθμους Fisherfaces και eigenfaces απαιτείται η αναδιαμόρφωση των εικόνων εκπαίδευσης και της εικόνας εισόδου, δηλαδή να έχουν το ίδιο μέγεθος στην μορφή gray_scale. Στο τέλος το αρχείο YML αποθηκεύεται, για να επιτευχθεί σε αργότερο στάδιο η αναγνώριση προσώπου.(*Εικόνα 3.7*)



Εικόνα 3.7: Εικονική απεικόνιση εκπαίδευσης από τους αλγορίθμους και αποθήκευση του YML file.

Τελευταίο στάδιο του προγράμματος, μετά την εξαγωγή των χαρακτηριστικών, καθορισμό των labels στις φωτογραφίες και εκπαίδευσή τους από τους αλγορίθμους είναι το στάδιο της πρόβλεψης. Αρχικά, το πρόγραμμα διαβάζει την εικόνα που βρίσκεται στον υποφάκελο TestImages (εικόνα εισόδου). Εάν ο αλγόριθμος που εκτελείται είναι ο eigenfaces ή ο fisherfaces τότε η εικόνα αλλάζει μέγεθος σε 200 * 200, αντιθέτως αν εκτελείται ο LBPH τότε

παραμένει το μέγεθος της ως έχει. Έπειτα, ακολουθείται παρόμοια διαδικασία όπως τις εικόνες εκπαίδευσης που υπήρχαν στο dataset, δηλαδή μέσω του haar_classifier_frontal_face ανιχνεύονται όλα τα πρόσωπα που βρίσκονται στην φωτογραφία. Για κάθε πρόσωπο γίνεται πρόβλεψη με βάση των εκπαιδευμένο facerecognizer και το αποτέλεσμα είναι το label στο οποίο ανήκει και το confidence. Η τιμή του confidence καθώς πλησιάζει το 0 τόσο πιο ορθή είναι η πρόβλεψη του αλγόριθμου για την κατηγοριοποίηση του προσώπου. Όταν η τιμή κυμαίνεται σε χαμηλές τιμές εννοείται ότι η απόσταση της εικόνας εισόδου είναι μικρή σε σχέση με το πρόσωπο που εξήγαγε ο αλγόριθμος (0 = exact match) (*Εικόνα 3.8*).

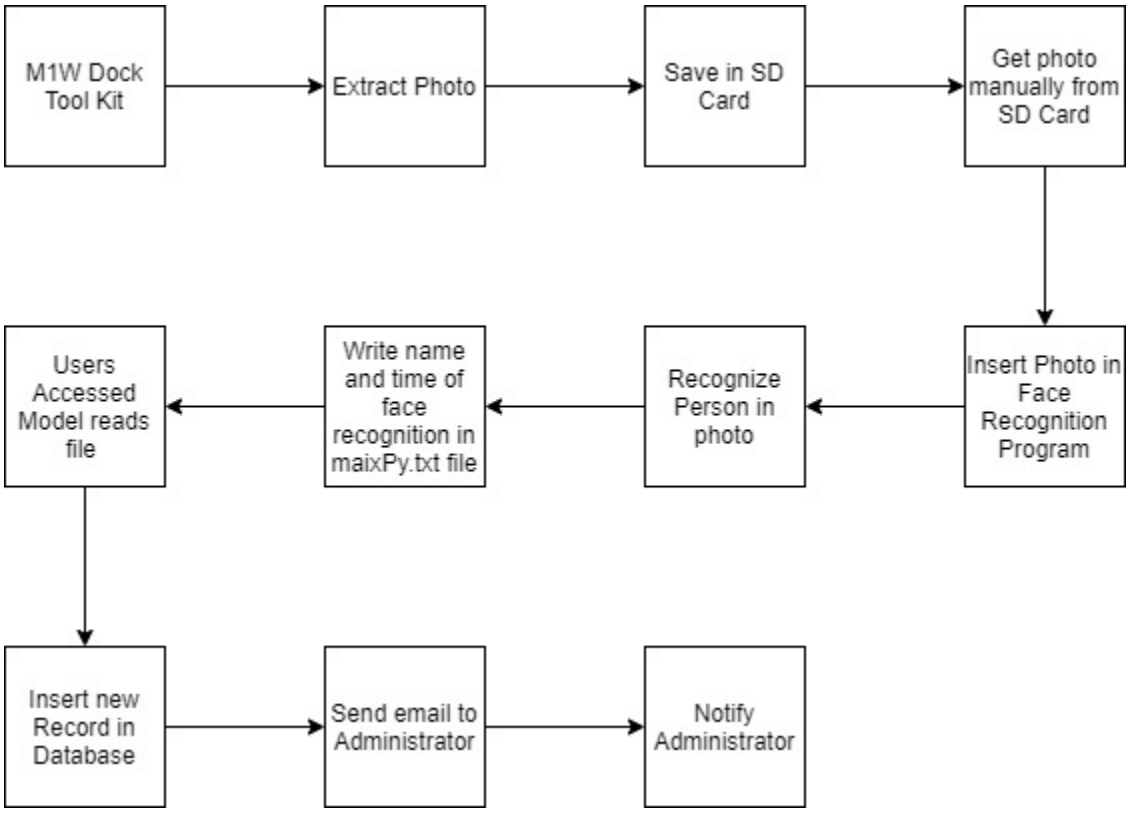


Εικόνα 3.8: Σχηματική απεικόνιση εισόδου εικόνας και εύρεση κατηγοριοποίησης που ανήκει

3.5 Διασύνδεση με Laravel Application

Τελευταίο βήμα που απομένει μετά την ολοκλήρωση του συστήματος αναγνώρισης προσώπου, είναι η διασύνδεση του αποτελέσματος που εξήγαγε το πρόγραμμα με το Laravel application. Πιο αναλυτικά, όταν εξάγει αποτέλεσμα το σύστημα αναγνώρισης προσώπου, καταγράφεται το όνομα του και ο χρόνος (ώρα : λεπτά : δευτερόλεπτα) στον οποίο ανιχνεύθηκε από το σύστημα σε ένα αρχείο ονομαζόμενο MaixPy.txt. Στη συνέχεια, το παραγόμενο αρχείο διαβάζεται από το Model των users_accessed και καταχωρείται στον πίνακα της βάσης δεδομένων. Αυτόματα, ο διαχειριστής του συστήματος λαμβάνει ειδοποίηση στο ηλεκτρονικό email στο προσωπικό του λογαριασμό ότι αναγνωρίστηκε κάποιο άτομο, γνωστό ή όχι, στην εμβέλεια του συστήματος.

Πιο κάτω φαίνεται αφαιρετικά η διασύνδεση του M1W Dock με το πρόγραμμα Αναγνώρισης Προσώπου και του Laravel Application



Εικόνα 3.9: Αφαιρετικός σχεδιασμός διασύνδεσης ολόκληρου του συστήματος

Κεφάλαιο 4

Laravel Application – Laravel PHP Framework

4.1 Εισαγωγή

Η Laravel είναι ένα δωρεάν ανοιχτού κώδικα PHP web framework. Δημιουργός της Laravel είναι ο Taylor Otwell, ο οποίος είχε ως πρόθεση την ανάπτυξη διαδικτυακών εφαρμογών (web applications) ακολουθώντας το μοντέλο MVC (Model – View – Controller) βασισμένο στο Symfony. Η φιλοσοφία που ακολουθεί η Laravel είναι η ευχάριστη ανάπτυξη και δημιουργική εμπειρία για οποιοδήποτε σκοπό ανάπτυξης συστήματος και λογισμικού. Αυτό το επιτυγχάνει ενσωματώνοντας τις πλείστες εργασίες που χρησιμοποιούνται στον ιστό μέσα σε ένα «κουτί». Πιο αναλυτικά, παρέχει ισχυρά εργαλεία που απαιτούνται για την δημιουργία μεγάλων εφαρμογών, όπως ο έλεγχος του control container, του migrations system και το ενσωματωμένο unit testing τα οποία είναι απαραίτητα για την υλοποίηση οποιουδήποτε στόχου. Επιπρόσθετα, προσφέρει δύο επίπεδα ασφαλείας, την ασφάλεια εφαρμογής και την ασφάλεια του διακομιστή.

4.2 MVC Model

MVC μοντέλο είναι ένα software design pattern, το οποίο χρησιμοποιείται για την δημιουργία διεπιφάνειας χρήστη και συσχετίζει την λογική του προγράμματος σε τρία διασυνδεδεμένα

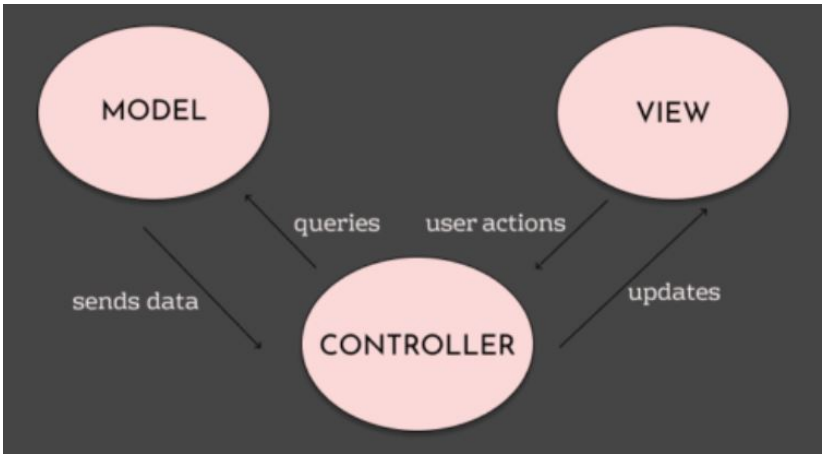
στοιχεία. Ο λόγος που επιτυγχάνεται αυτό, είναι για να γίνεται διαχωρισμός των εσωτερικών αναπαραστάσεων των πληροφοριών που παρουσιάζονται αλλά και από τον τρόπο που παρουσιάζονται και γίνονται αποδεκτές. Το κάθε συστατικό του μοντέλου αποσκοπεί διαφορετική λειτουργία (Εικόνα 4.1). Η λειτουργία – ευθύνες του κάθε συστατικού είναι:

- Model: Το model αποτελεί το κεντρικό συστατικό του μοντέλου. Ουσιαστικά, ορίζει τη δυναμική δομή της εφαρμογής ανεξάρτητα από την διεπιφάνεια χρήστη και διαχειρίζεται τα δεδομένα, τη λογική και τους κανόνες της εφαρμογής.

  Λειτουργία: Είναι υπεύθυνο για την διαχείριση των δεδομένων της εφαρμογής. Λαμβάνει από τον controller τα δεδομένα που δίνει ως είσοδο ο χρήστης.
- View: Το view είναι οποιοδήποτε είδος αναπαράστασης πληροφορίας, για παράδειγμα πίνακας ή διάγραμμα.

  Λειτουργία: Είναι υπεύθυνο για την αναπαράσταση του μοντέλου σε συγκεκριμένη μορφή.
- Controller: Ο controller λαμβάνει όλες τις εισόδους και τις μετατρέπει σε εντολές για το model και το view.

  Λειτουργία: Με βάση την είσοδο του χρήστη ο controller αλληλοεπιδρά με τα αντικείμενα του μοντέλου. Πιο συγκεκριμένα, λαμβάνει την είσοδο, τα επιβεβαιώνει προαιρετικά και τα μεταβιβάζει στο model [12].



Εικόνα 4.1: Απεικόνιση MVC Model

4.3 Laravel Homestead

Θεώρησα πιο εύκολο να εγκαταστήσω το Laravel Homestead, το οποίο είναι ένα προ συσκευασμένο vagrant box (virtual box) το οποίο περιέχει ένα εκπληκτικό περιβάλλον ανάπτυξης χωρίς να απαιτείται η εγκατάσταση της PHP, του διακομιστή ιστού (web server) και οποιουδήποτε άλλου διακομιστή λογισμικού (server software) στον υπολογιστή μου τοπικά. Πιο συγκεκριμένα το homestead περιέχει nginx, PHP, MySQL, PostgreSQL, Memcached, Node και πολλά άλλα τα οποία είναι απαραίτητα για την δημιουργία του Laravel web application.

Μετά την εγκατάσταση του virtual box, το μόνο που απόμεινε για τη δημιουργία του Laravel web application ήταν η διασύνδεση του με την βάση δεδομένων στην οποία θα αποθηκεύονταν τα δεδομένα. Η βάση δεδομένων είναι απαραίτητη για την αποθήκευση όλων των στοιχείων που χρειάζεται ο διαχειριστής της ιστοσελίδας.

4.4 Middleware

Ένας από τους σημαντικότερους μηχανισμούς που προσφέρει η Laravel είναι ο μηχανισμός middleware ο οποίος προσφέρει ασφάλεια στην εφαρμογή. Ένα middleware παρέχει μηχανισμούς για το φιλτράρισμα των HTTP αιτημάτων, προτού να εισέλθουν στην εφαρμογή. Ο λόγος που παρέχεται κάποιο middleware είναι για να επιτευχθεί περεταίρω ασφάλεια της εφαρμογής. Ένα παράδειγμα χρήσης κάποιου middleware για το web application είναι το middleware που επαληθεύει αν ο χρήστης της εφαρμογής είναι επικυρωμένος (authenticated), δηλαδή είναι συνδεδεμένος με τον προσωπικό του λογαριασμό. Στην προκειμένη περίπτωση μόνο ο διαχειριστής της ιστοσελίδας έχει λογαριασμό. Ο διαχειριστής για να συνδεθεί και να επικυρωθεί πρέπει να εισάγει τα στοιχεία του λογαριασμού του, προσωπικό email και κωδικό. Αν ο χρήστης δεν είναι επικυρωμένος, τότε το middleware θα τον ανακατευθύνει στη διεπιφάνεια εισαγωγής στοιχείων, αντιθέτως θα του επιτρέψει την πλοήγηση στο κύριο μενού και οπουδήποτε αλλού επιθυμεί ο ίδιος.

4.5 CSRF Protection

Η Laravel προσφέρει προστασία από επιθέσεις Cross-Site Request Forgery. Το CSRF αποτελεί κακόβουλη επίθεση με την οποία εκτελούνται μη εξουσιοδοτημένες εντολές για λογαριασμό ενός επικυρωμένου χρήστη. Έτσι, η Laravel για αντιμετώπιση τέτοιων παραβιάσεων, παρέχει CSRF protection. Πιο συγκεκριμένα, παράγει για κάθε user session αυτόματα ένα CSRF token. Το συγκεκριμένο token χρησιμοποιείται για να ταυτοποιεί ότι ο επικυρωμένος χρήστης, εκτελεί αίτημα στην εφαρμογή και όχι κάποιος ξένος, κακόβουλος χρήστης. Κάθε φορά που γίνεται χρήση HTML form στην εφαρμογή, συμπεριλαμβάνεται ένα κρυφό CSRF token έτσι ώστε το CSRF middleware να επικυρώνει το αίτημα. Το middleware ακολούθως επιβεβαιώνει αν το CSRF token που αιτήθηκε είναι ίδιο με το token που αποθηκεύτηκε στο user session. Εάν, τα δύο tokens δεν είναι όμοια τότε θα επιστρέψει «HTTP 500 error».

4.6 Eloquent ORM (Object Relational mapper)

Η Laravel προσφέρει προστασία από SQL injections εάν και εφόσον γίνεται χρήση του eloquent ORM, το οποίο είναι ενσωματωμένο. Κάνοντας χρήση του Eloquent γίνεται χρήση προ επεξεργασμένων **statements** τα οποία αποφεύγουν τις εισόδους οι οποίες μπορεί να προέρχονται από τις φόρμες. Με αυτό τον τρόπο, εάν η εφαρμογή δεχθεί κακόβουλη επίθεση από κάποια είσοδο από την φόρμα, η Laravel θα το απορρίψει, αφού θα το θεωρήσει μη έγκυρο SQL query. Ωστόσο, η επεξεργασία των δεδομένων που βρίσκονται στους πίνακες της βάσης γίνεται μέσω τον Models, τα οποία αντιστοιχούν με ένα πίνακα στην βάση δεδομένων [13].

4.7 Δεδομένα Βάσης Δεδομένων

Οι πίνακες που θεωρήθηκαν απαραίτητο να δημιουργηθούν στην βάση δεδομένων για την διαχείριση του συστήματος ήταν ο πίνακας users, valid_users, notifications, users_accessed. Πιο κάτω απεικονίζονται δειγματικά δεδομένα και οι στήλες για κάθε πίνακα τα οποία αποθηκεύτηκαν στην βάση:

Πίνακας users – Πίνακας διαχειριστή

Περιγραφή

Στον πίνακα users αποθηκεύονται τα στοιχεία του διαχειριστή (Εικόνα 4.2).

Στήλες:

- name: Ονοματεπώνυμο
- email: Email
- email_verified_at: Χρόνος επιβεβαίωσης email
- password: Απεικονίζεται το hash value του κωδικού που εισήγαγε ο διαχειριστής. Λόγω ασφαλείας δεν αποθηκεύεται ο κωδικός που δημιούργησε ο διαχειριστής.
- Image: Φωτογραφία του διαχειριστή
- Remember_token: Token που χρησιμοποιείται για "remember me" sessions.
- Created_at: Ημερομηνία δημιουργίας του διαχειριστή
- Updated_at: Ημερομηνία ανανέωσης στοιχείων του διαχειριστή

id	name	email	email_verified_at	password	image	remember_token	created_at	updated_at
1	Prodromos Georgiou	admin@admin.com	NULL	$2y$10$BEEfmT4tAgXKaG3ylBkf2etlM23BDqPv....	1584353213.jpg	NULL	2020-03-16 09:44:42	2020-03-16 10:06:54
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Εικόνα 4.2: Πίνακας users

Πίνακας valid_users

Περιγραφή

Στον πίνακα valid_users αποθηκεύονται τα στοιχεία των εγγεγραμμένων χρηστών. Οι εγγεγραμμένοι χρήστες καθορίζονται από τον διαχειριστή (Εικόνα 4.3).

Στήλες:

- FullName: Ονοματεπώνυμο εγγεγραμμένου χρήστη
- email: Email εγγεγραμμένου χρήστη

- Image: Φωτογραφία του εγγεγραμμένου χρήστη
- Created_at: Ημερομηνία δημιουργίας του εγγεγραμμένου χρήστη
- Updated_at: Ημερομηνία ανανέωσης στοιχείων εγγεγραμμένου χρήστη

id	FullName	email	image	created_at	updated_at
1	ChristianaCharalambous	cchara01@gmail.com	uploads/jjCcOWY33bMDO81klFW39ReWtbcytJV...	2020-03-16 10:23:27	2020-03-16 10:23:27
2	MenelaosArtemiou	martem01@cs.ucy.ac.cy	uploads/h8zpGrmKJBWvGC9IEk2dVxojZeYQtsEL...	2020-03-31 17:51:46	2020-03-31 17:51:46
3	ProdromosGeorgiou	testing@testing.com	uploads/0Zz7PMMdl8MEpOyj6m1C5kd4yllIm3NJ...	2020-04-02 06:35:39	2020-04-02 06:35:40
4	RafaelGeorgiou	rafael@gmail.com	uploads/1nG7UAcXyzfOPlrPm0Qi2ar2YCRTC1BS...	2020-04-03 19:12:41	2020-04-03 19:12:41
NULL	NULL	NULL	NULL	NULL	NULL

Εικόνα 4.3: Πίνακας valid_users

Πίνακας notifications

Περιγραφή

Στον πίνακα notifications αποθηκεύονται τα στοιχεία των ειδοποιήσεων που λαμβάνει ο διαχειριστής (Εικόνα 4.4).

Στήλες:

- Id: Μοναδικό χαρακτηριστικό για κάθε ειδοποίηση.
- type: Τύπος ειδοποίησης
- notifiable_type: Είδος χρήστη που ειδοποιείται. Στην συγκεκριμένη περίπτωση ο διαχειριστής.
- notifiable_id: ID ειδοποίησης
- data: Τι θα περιέχει το μήνυμα που θα λάβει ο διαχειριστής.
- read_at: Πότε διαβάστηκε το μήνυμα από τον διαχειριστή.
- created_at: Ημερομηνία δημιουργίας της συγκεκριμένης ειδοποίησης.
- updated_at: Ημερομηνία ανανέωσης στοιχείων στην συγκεκριμένη ειδοποίηση.

id	type	notifiable_type	notifiable_id	data	read_at	created_at	updated_at
32170545-179e-435e-ac60-b2505de21b72	App\Notifications\WarnAdministrator	App\User	1	{"data":"ChristianaCharalambous tried to access the house!"}	NULL	2020-04-06 08:43:12	2020-04-06 08:43:12
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Εικόνα 4.4: Πίνακας notifications

Πίνακας users_accessed

Περιγραφή

Στον πίνακα users_accessed απεικονίζονται τα στοιχεία των χρηστών που προσπάθησαν να εισέλθουν στο σπίτι και το σύστημα τους αναγνώρισε. Εάν το άτομο που προσπάθησε να εισέλθει στο σπίτι ήταν «άγνωστο» στο σύστημα στην βάση δεδομένων αποθηκεύεται ως «Unknown», αντιθέτως αν είναι «γνωστό» αποθηκεύεται το ονοματεπώνυμο του (Εικόνα 4.5).

Στήλες:

- full_name: Ονοματεπώνυμο ατόμου.
- time_accessed: Χρόνος που το σύστημα αναγνώρισε κάποιο άτομο.
- Created_at: Ημερομηνία δημιουργίας του ατόμου
- Updated_at: Ημερομηνία ανανέωσης στοιχείων του ατόμου

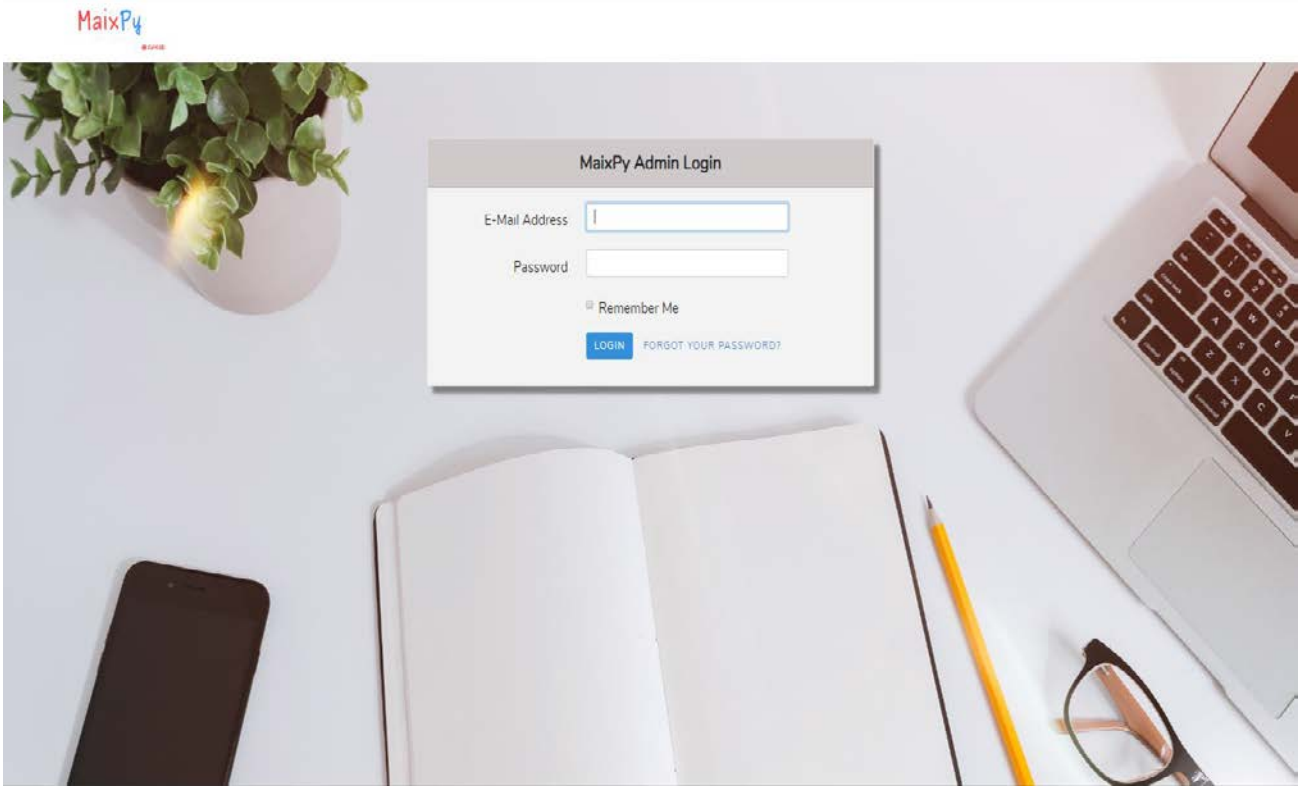
id	full_name	time_accessed	created_at	updated_at
1	ChristianaCharalambous	20:14:36	2020-04-03 18:50:29	2020-04-03 18:50:29
6	Unknown	16:07:38	2020-04-03 18:52:00	2020-04-03 18:52:00
27	Unknown	22:10:48	2020-04-03 19:11:03	2020-04-03 19:11:03
28	ProdromosGeorgiou	15:15:15	2020-04-06 08:36:24	2020-04-06 08:36:24
29	ChristianaCharalambous	11:42:30	2020-04-06 08:43:09	2020-04-06 08:43:09
NULL	NULL	NULL	NULL	NULL

Εικόνα 4.5: Πίνακας user_accessed

4.8 Laravel application website

Πιο κάτω παρουσιάζονται οι κύριες διεπιφάνειες από την ιστοσελίδα διαχείρισης του συστήματος. Η λειτουργίες που παρέχει η ιστοσελίδα παρουσιάζονται πιο λεπτομερώς στο Παράρτημα Α (Εικόνα 4.6).

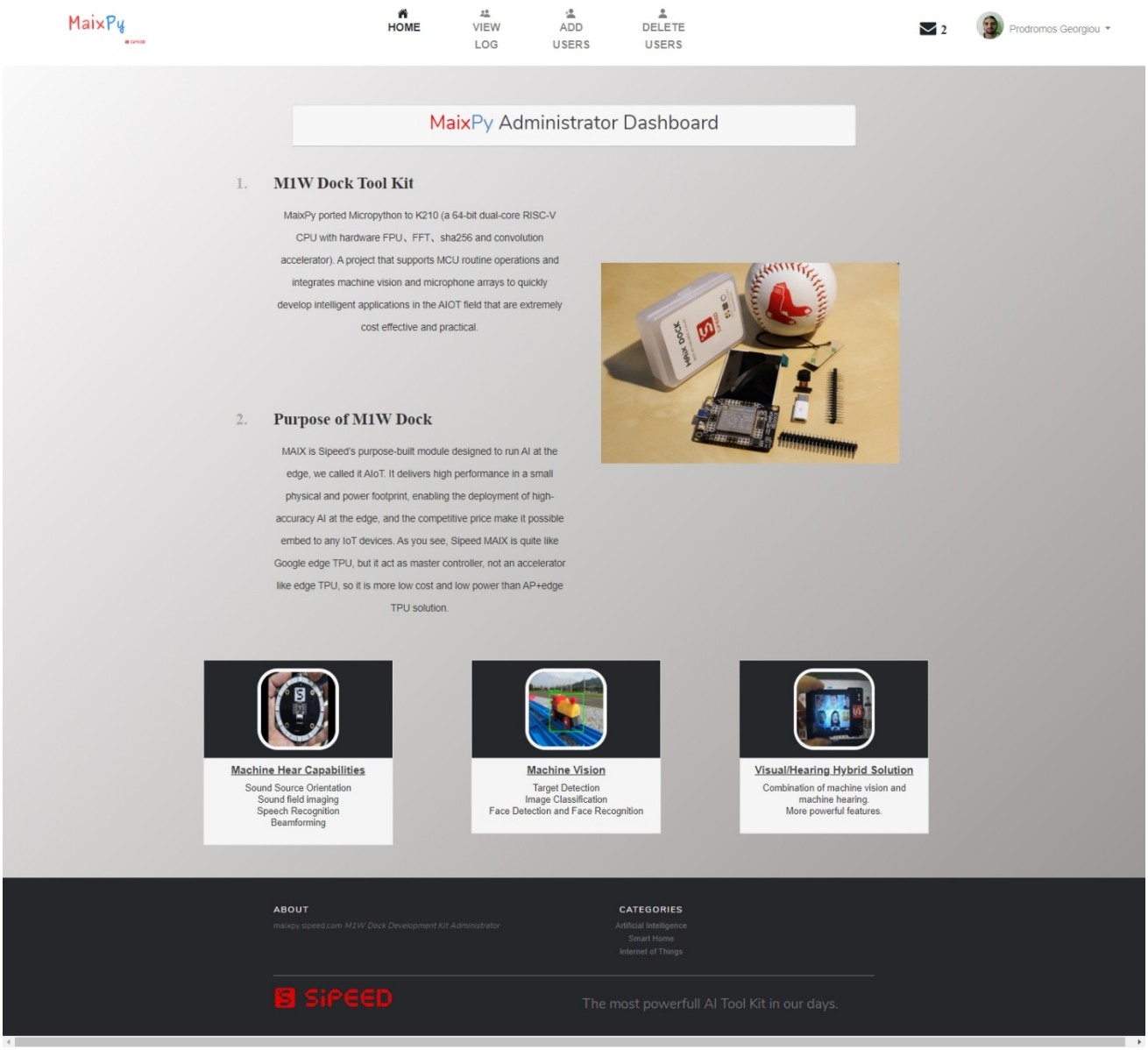
Διεπιφάνεια εισαγωγής στοιχείων διαχειριστή



Εικόνα 4.6: Διεπιφάνεια εισόδου διαχειριστή

Στην συγκεκριμένη διεπιφάνεια ο διαχειριστής καλείται να εισάγει το προσωπικό του email και κωδικό για να συνδεθεί με το σύστημα διαχείρισης. Του προσφέρεται η δυνατότητα επιλογής «Remember Me» των στοιχείων για να μην τα εισάγει κάθε φορά καθώς επίσης και η δυνατότητα επιλογής «FORGOT YOUR PASSWORD» μέσω του οποίου μπορεί να αντικαταστήσει τον παλιό του κωδικό με τον καινούργιο.

Αρχική διεπιφάνεια

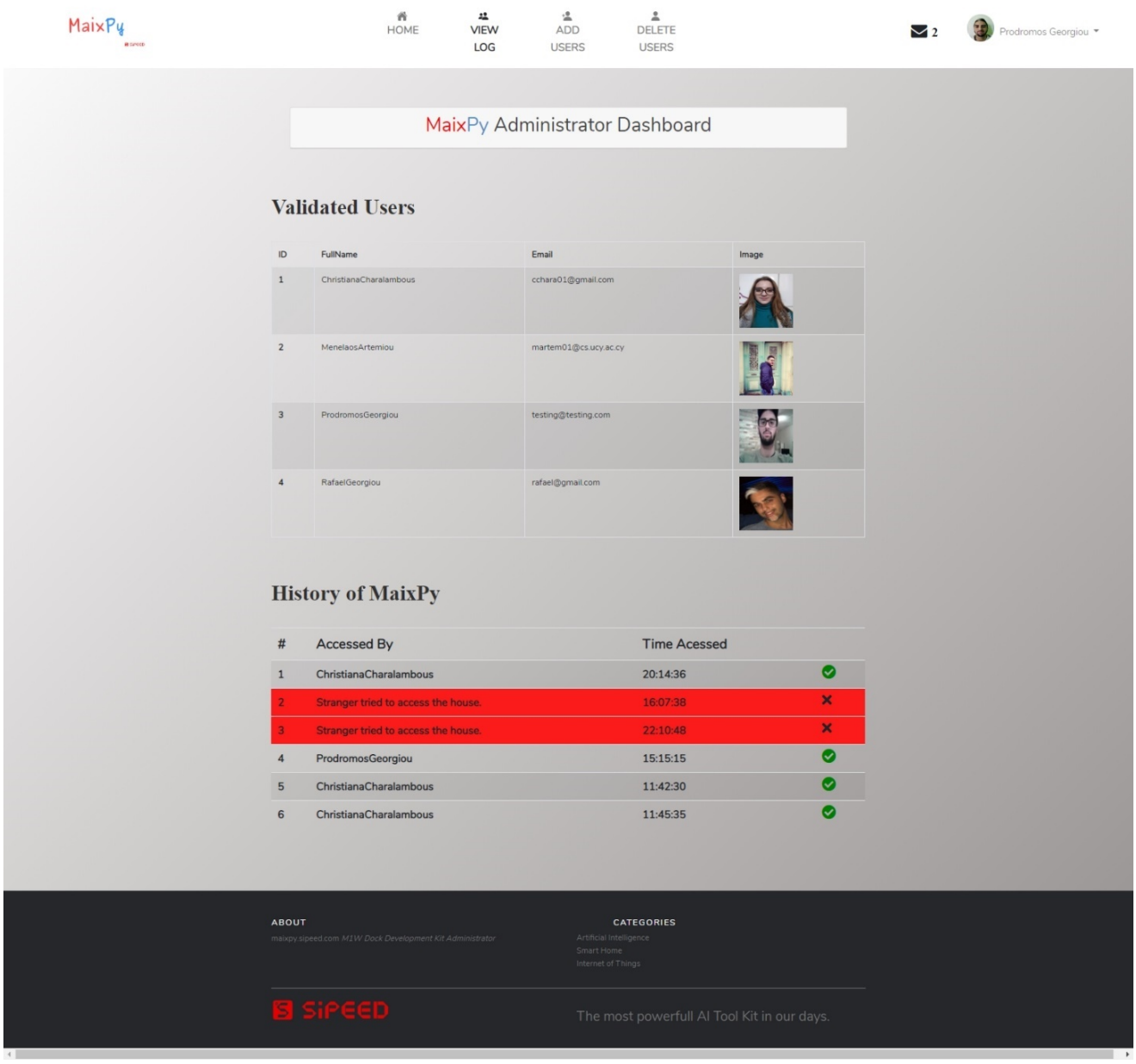


Εικόνα 4.7: Αρχική διεπιφάνεια

Πιο πάνω απεικονίζεται η αρχική διεπιφάνεια μετά την εισαγωγή στοιχείων του χρήστη. Στη συγκεκριμένη διεπιφάνεια απεικονίζονται κάποια γενικά λόγια για το M1W Dock καθώς επίσης και τρείς κύριους τομείς δυνατοτήτων που προσφέρει σε συνδυασμό με τον Kendryte K210. Στο

πάνω μέρος είναι το κύριο μενού πλοήγησης, η εικόνα προφίλ του χρήστη και τα «αδιάβαστα» μηνύματα – ειδοποιήσεις που υπάρχουν στο inbox του διαχειριστή (Εικόνα 4.7).

Διεπιφάνεια Ενημέρωσης

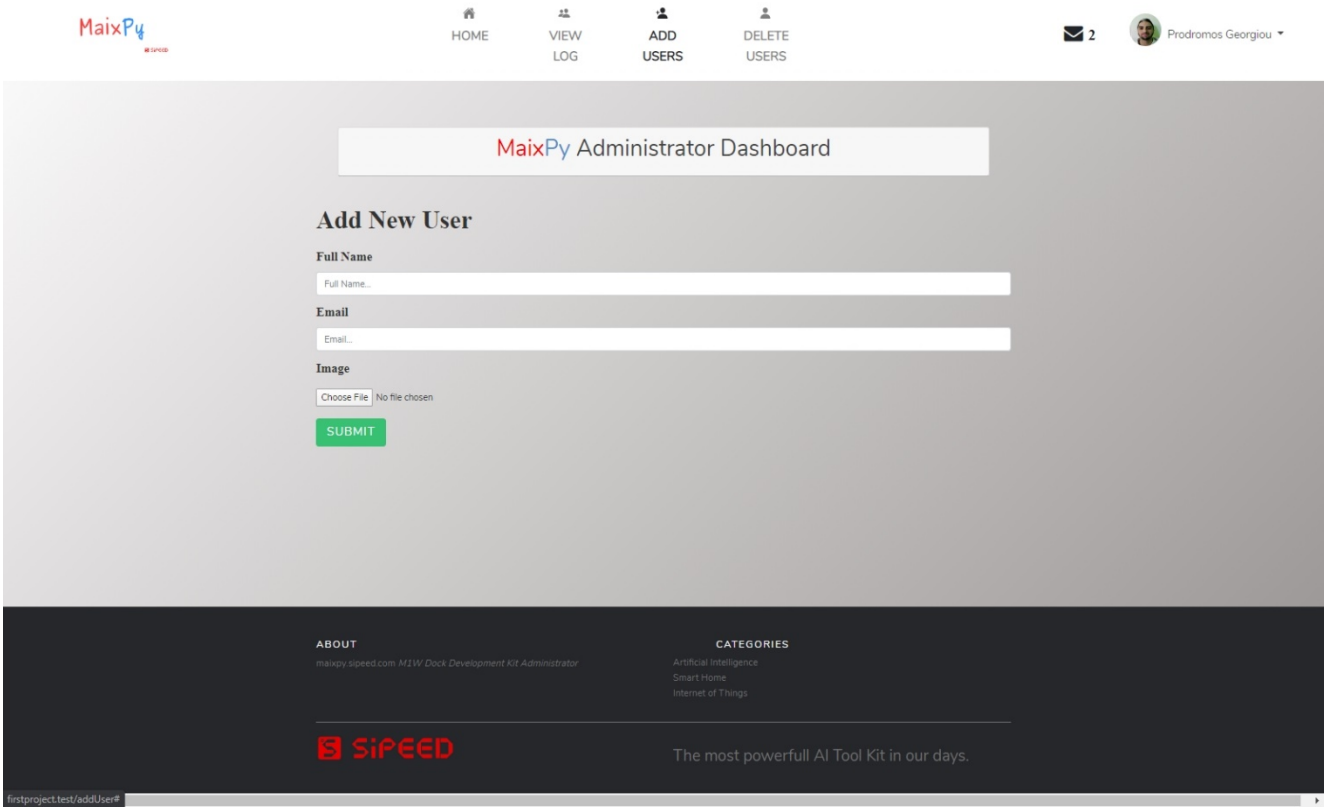


Εικόνα 4.8: Διεπιφάνεια Ενημέρωσης

Στην συγκεκριμένη διεπιφάνεια παρουσιάζεται στον διαχειριστή οι εγγεγραμμένοι χρήστες

και το ιστορικό από το σύστημα αναγνώρισης προσώπου. Πιο συγκεκριμένα φαίνονται τα στοιχεία των εγγεγραμμένων χρηστών (όνομα, προσωπικό email, φωτογραφία) και η ιστορία από το σύστημα. Δηλαδή εμφανίζεται το όνομα και η ώρα που ανιχνεύθηκε κάποιο άτομο. Όπως φαίνεται από την εικόνα οι χρήστες που είναι άγνωστοι στο σύστημα εμφανίζονται με κόκκινο χρώμα (Εικόνα 4.8).

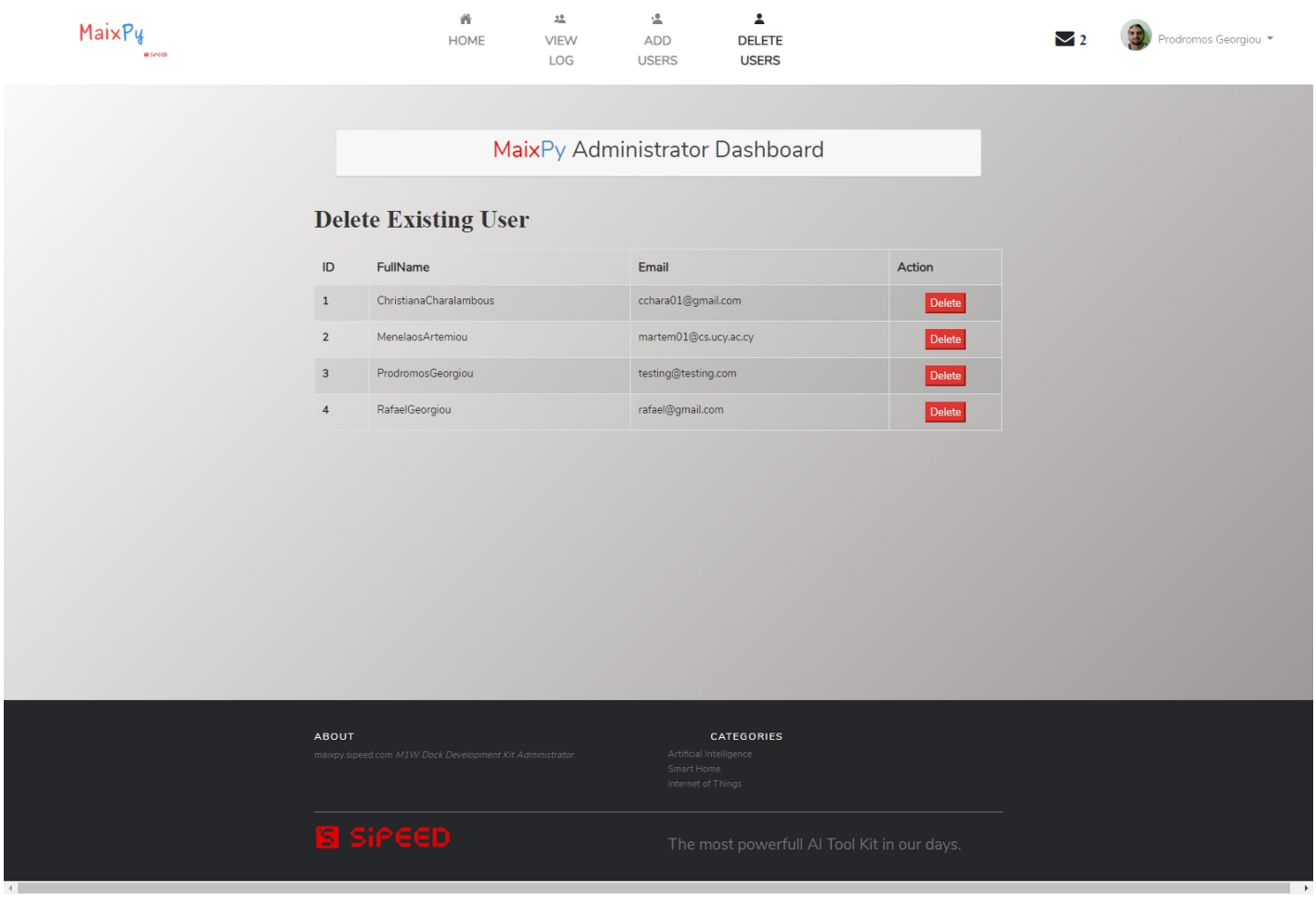
Διεπιφάνεια πρόσθεση χρήστη



Εικόνα 4.9: Διεπιφάνεια πρόσθεσης χρήστη

Άλλη δυνατότητα που παρέχεται στον διαχειριστή είναι η πρόσθεση καινούργιων χρηστών στο σύστημα. Ο διαχειριστής για την επιτυχή εγγραφή καινούργιου χρήστη στο σύστημα χρειάζεται να συμπληρώσει τα πεδία Full Name, Email και Image (Εικόνα 4.9).

Διεπιφάνεια διαγραφής χρήστη



Εικόνα 4.10: Διεπιφάνεια διαγραφής χρήστη

Τελευταία διεπιφάνεια της ιστοσελίδας διαχείρισης είναι η διεπιφάνεια διαγραφής χρήστη. Ο διαχειριστής έχει την δυνατότητα διαγραφής κάποιου ήδη εγγεγραμμένου χρήστη οποιαδήποτε στιγμή το επιθυμεί (Εικόνα 4.10).

Αβίαστα, λοιπόν, συνάγεται το συμπέρασμα ότι ο διαχειριστής του συστήματος έχει την πλήρη διαχείριση του συστήματος και των χρηστών από οπουδήποτε, οποιαδήποτε στιγμή το επιθυμεί. Ο βαθμός δυσκολίας χρήσης του συστήματος θεωρείται χαμηλός, αφού η ιστοσελίδα είναι εύκολα διαχειρίσιμη και δεν απαιτείται κάποια εξειδικευμένη γνώση για την χρήση της. Τέλος, το σύστημα σε κάθε επιλογή του διαχειριστή, του επιστρέφει μήνυμα επιτυχίας ή αποτυχίας, έτσι του παρέχει το αίσθημα της ικανοποίησης και της ασφάλειας.

Κεφάλαιο 5

Αξιολόγηση

5.1 Εισαγωγή

Για τον προσδιορισμό του πιο αποδοτικού αλλά και πιο ακριβή αλγόριθμου αναγνώρισης προσώπου, διεξάχθηκε μια διεξοδική μελέτη με βάση το θεωρητικό υπόβαθρο των αλγορίθμων και των *Haar Cascade Classifiers*. Εστίασα σε δύο σημαντικές πληροφορίες με βάση την θεωρία, την ανάλυση της μεθόδου «detectMultiScale» και των παραμέτρων της, αλλά και στην χρήση διαφορετικών φωτογραφιών που απάρτιζαν τα datasets ανάλογα με την φωτεινότητα. Στο πρώτο στάδιο, κάνοντας χρήση της μεθόδου «detectMultiScale» παρατηρήθηκαν δύο σημαντικές παράμετροι οι οποίες καθορίστηκαν απαραίτητες, καθώς επηρεάζουν την αποδοτικότητα των

αλγορίθμων σε σημαντικό βαθμό. Στο δεύτερο στάδιο, γνωρίζοντας την θεωρία του αλγορίθμου Eigenfaces θεωρήθηκε αναγκαίο να δημιουργηθούν datasets με διαφορετική φωτεινότητα, για να παρατηρηθεί η συμπεριφορά του σε συνθήκες διαφορετικού φωτισμού. Πιο συγκεκριμένα, δημιουργήθηκε μέθοδος αλλαγής φωτισμού και δημιουργήθηκαν τέσσερα διαφορετικά datasets, το κανονικό, το σκοτεινό, το ημι-σκοτεινό και το φωτεινό. Αναλυτικότερα, τα datasets περιείχαν φωτογραφίες παρμένες από διαφορετική γωνιά, φωτεινότητα και στάση του σώματος. Τέλος, δημιουργήθηκε dataset με φωτογραφίες παρμένες από το M1W Dock για να αναλυθεί η απόδοση των αλγορίθμων.

5.2 Μέθοδος detectMultiScale

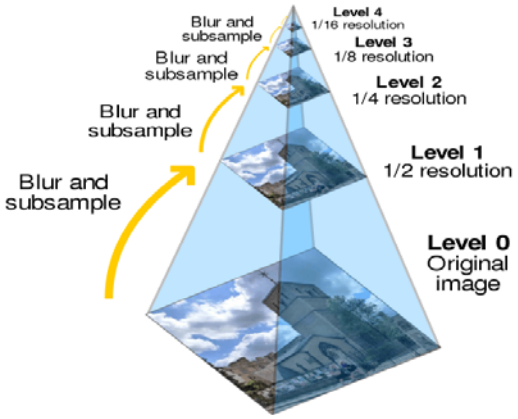
Η μέθοδος detectMultiScale λαμβάνει επτά παραμέτρους τις scaleFactor, minNeighbours, minSize, maxSize, gray_scale εικόνα, το flags και το objects. Χρησιμοποιώντας το minSize και maxSize, τα αντικείμενα (πρόσωπα) μικρότερα του minSize που είχε αρχικοποιηθεί ή μεγαλύτερα του MaxSize δεν συμπεριλαμβάνονται στην λύση. Στο συγκεκριμένο σύστημα δεν έγινε χρήση των δύο παραμέτρων, αφού θεωρήθηκε αναγκαίο να μην αποκλειστούν συγκεκριμένα αντικείμενα που ανιχνεύονται για να υπάρχει ο ακριβής αριθμός των προσώπων που εξάγουν οι αλγόριθμοι. Στο τέλος, το flags και το objects δεν χρησιμοποιήθηκε στην εύρεση των χαρακτηριστικών και της αναγνώρισης προσώπου [14].

Η χρήση του detectMultiScale αποσκοπεί στην εύρεση των ιδανικών τιμών που πρέπει να καθοριστούν, έτσι ώστε να ελαχιστοποιηθούν τα false positives και να μεγιστοποιηθούν τα true positives. Σημαντικό παράγοντας που επηρεάζει το τελικό αποτέλεσμα είναι το είδος της φωτογραφίας που εκπαιδεύεται, το ιδανικό είναι το πρόσωπο και τα μάτια να είναι σε εμφανή σημείο.

5.2.1 Παράμετρος scaleFactor

Η συγκεκριμένη παράμετρος χρησιμοποιείται στην δημιουργία της scale pyramid. Η scale pyramid είναι μια πολυδιάστατη αναπαράσταση μιας εικόνας. Πιο συγκεκριμένα, μια πολυδιάστατη αναπαράσταση εικόνας βοηθά στην εύρεση αντικειμένων σε διαφορετικές

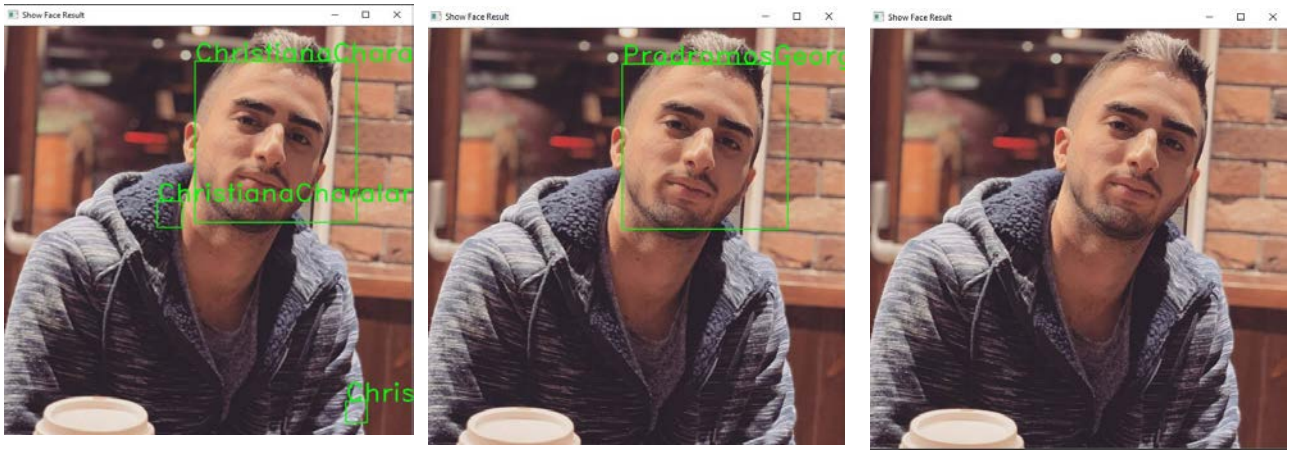
κλίμακες. Άρα, το scaleFactor αναπαριστά την αναλογία στην οποία η εικόνα θα επαναδιαμορφωθεί σε μικρότερο μέγεθος σε κάθε στάδιο της πυραμίδας έτσι ώστε να αναγνωρίζονται πιο εύκολα τα πρόσωπα που βρίσκονται στις φωτογραφίες. Όσο πιο μικρή τιμή τεθεί στο scaleFactor, τόσα περισσότερα επίπεδα θα υπάρχουν στην πυραμίδα, το οποίο κοστίζει σε χρόνο αφού η διαδικασία γίνεται αργή και ο φόρτος υπολογισμού πιο έντονος αλλά η ακρίβεια των αποτελεσμάτων είναι καλύτερη. Αντιθέτως, αν τεθεί πιο μεγάλη τιμή ο υπολογισμός είναι πιο γρήγορος αλλά υπάρχει πιθανότητα της αποτυχίας ανίχνευσης προσώπων [15,16](Εικόνα 5.1).



Εικόνα 5.1: Απεικόνιση Scale Pyramid

5.2.2 Παράμετρος minNeighbours

Η παράμετρος minNeighbours καθορίζει πόσους γείτονες πρέπει να διατηρήσει κάθε υποψήφιο τετράγωνο. Αναλυτικότερα, η συγκεκριμένη παράμετρος επηρεάζει την ποιότητα των αναγνωρισμένων προσώπων, δηλαδή πιο ψηλή τιμή οδηγεί σε λιγότερες αναγνωρίσεις αλλά με ψηλότερη ποιότητα. Συμπερασματικά, αν δοθεί υψηλή τιμή στην minNeighbours, μειώνονται τα false positives αλλά με ρίσκο στην μη αναγνώριση των true positive (Εικόνα 5.2) [16]. Χρησιμοποιεί την τεχνική του multiple scale style (σαν scale Pyramid) και sliding window strategy και επιστρέφει πολλαπλές ανταποκρίσεις για όλες τις περιοχές. Αν ο αριθμός των ανταποκρίσεων είναι μεγαλύτερος από την τιμή του minNeighbour τότε θεωρείται ως πρόσωπο.



Εικόνα 5.2: Min neighbour 1 (Αριστερά εικόνα), Min neighbour 4 (Μεσαία εικόνα), Min neighbour 15 (Δεξιά εικόνα)

5.3 Ανάλυση Κανονικού dataset, Σκοτεινού dataset, Ημι-σκοτεινού dataset, Φωτεινού dataset, MaixPy dataset

Για να αναλυθεί η συμπεριφορά των αλγορίθμων σε διαφορετικά περιβάλλοντα φωτισμού, έγινε επεξεργασία του κανονικού dataset. Έγινε μετατροπή του κανονικού dataset σε σκοτεινό, ημι-σκοτεινό και φωτεινό. (Εικόνα 5.3).

Εικόνα 5.3: Από αριστερά προς δεξιά Κανονική φωτογραφία (πρώτη εικόνα), Σκοτεινή φωτογραφία (δεύτερη εικόνα), Ημι-σκοτεινή φωτογραφία (Τρίτη εικόνα), Φωτεινή φωτογραφία (Τέταρτη φωτογραφία)

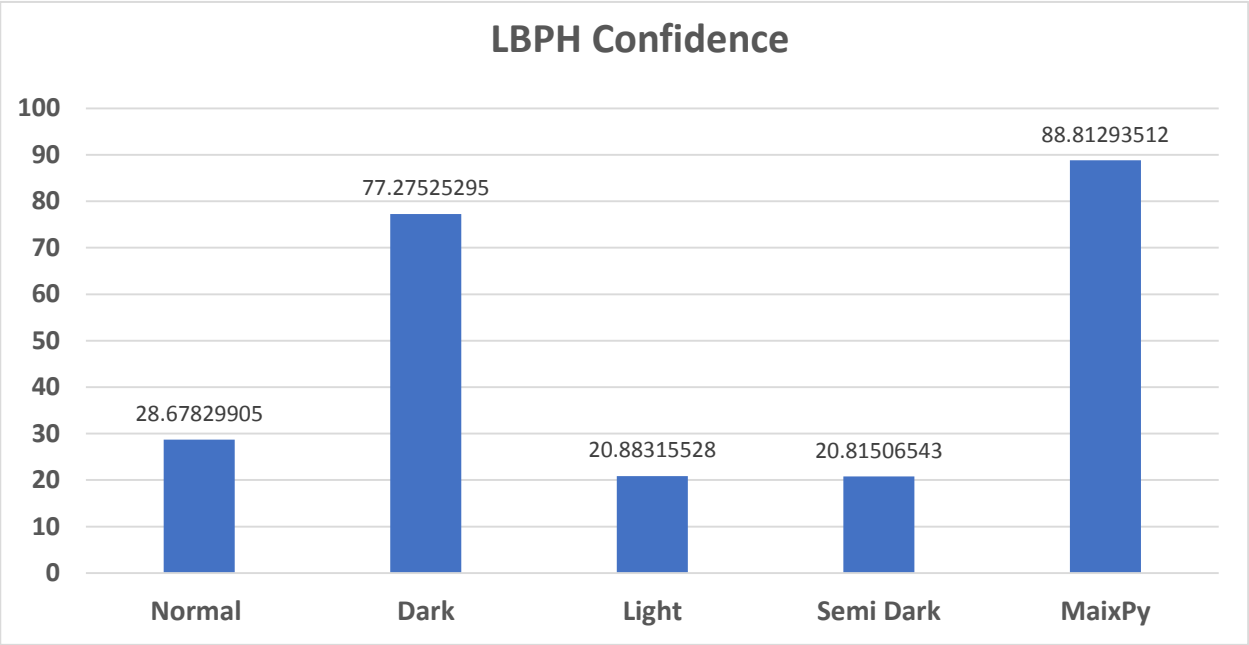
5.3.1 Ανάλυση Confidence

Το πρόγραμμα εξάγει για κάθε πρόβλεψη, τη τιμή label και confidence για την πρόβλεψη του ατόμου που βρίσκεται στην φωτογραφία. Η τιμή confidence, ουσιαστικά αντιπροσωπεύει την ομοιότητα της φωτογραφίας εισόδου σε σχέση με την πιο παρόμοια φωτογραφία που υπάρχει

μέσα στο dataset. Όσο πιο μεγάλη η τιμή του confidence, οι συγκρινόμενες φωτογραφίες τόσο λιγότερη ομοιότητα έχουν. Από την άλλη όψη, αν το confidence κατέχει μικρή τιμή οι φωτογραφίες που χρησιμοποιούνται στη σύγκριση είναι σχεδόν πανομοιότητες [17]. Όταν το confidence πάρει τιμή 0, οι φωτογραφίες που χρησιμοποιούνται στη σύγκριση, είναι στην ουσία όμοιες με ποσοστό ομοιότητας 100%. Στη περίπτωση του αλγόριθμου LBPH η τιμή του confidence υπολογίζεται με βάση την ευκλείδεια απόσταση μεταξύ δύο histograms [21]. Η τιμή confidence της εικόνας εισόδου, χρησιμοποιώντας τον Eigenfaces, υπολογίζεται μέσω συγκρίσεων των eigencoefficients της εικόνας εισόδου με τα coefficients των dataset. Επίσης, Στη συνέχεια, υπολογίζεται η ευκλείδεια απόσταση μεταξύ του eigenfaces της εικόνας εισόδου και του eigenfaces των dataset [18]. Ομοίως, στον αλγόριθμο Fisherfaces, η απόσταση μεταξύ της εικόνας εισόδου (confidence) και του dataset εικόνων υπολογίζεται με την χρήση της ευκλείδειας απόστασης [14]. Αξίζει να αναφερθεί ότι οι τιμές confidence που εξάγει ο κάθε αλγόριθμος δεν συσχετίζονται με την τιμή που εξάγει άλλος αλγόριθμος, δηλαδή κάθε αλγόριθμος έχει το δικό του εύρος της τιμής confidence.

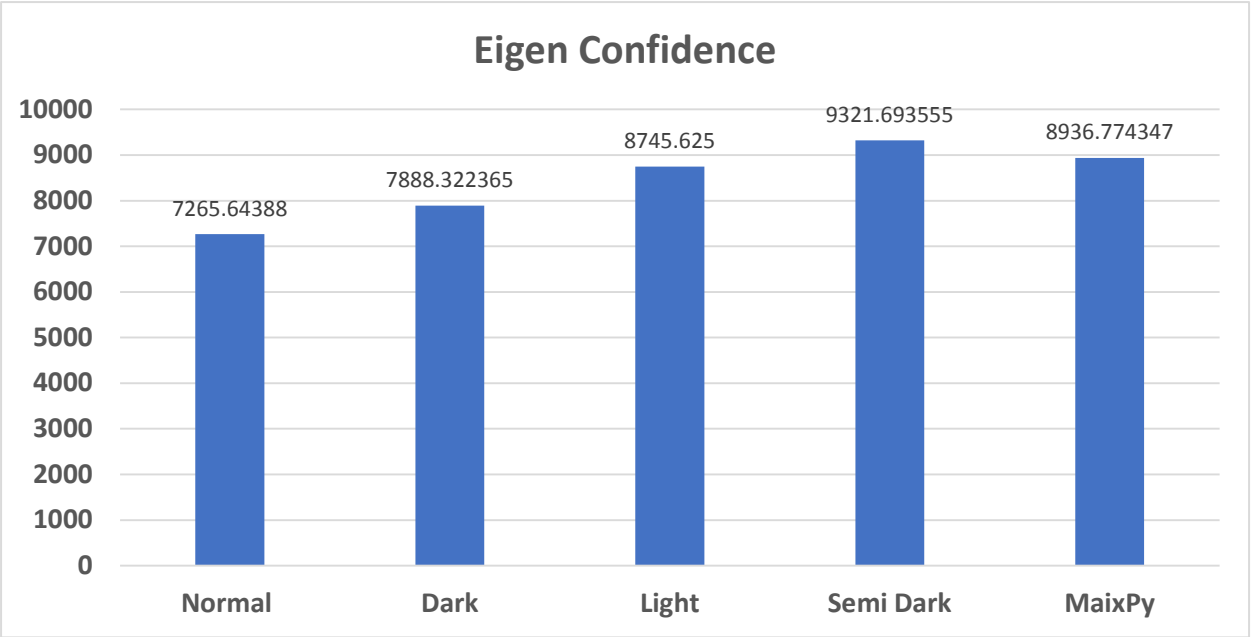
$$\sqrt{\sum_{i=1}^{n}(hist1_i - hist2_i)^2}$$

Για τους τρεις αλγορίθμους πάρθηκαν οι μέσοι όροι της τιμής confidence που εξήγαγε το πρόγραμμα για το κάθε dataset με συνολικό αριθμό δειγμάτων είκοσι (n_s = 20). Πιο συγκεκριμένα, πάρθηκαν δέκα δείγματα από το dataset του ατόμου «0» και δέκα δείγματα από το dataset του ατόμου «1» και το κάθε dataset περιείχε συνολικά σαράντα πέντε φωτογραφίες εκπαίδευσης (n_d = 45). Αξίζει να σημειωθεί, ότι η φωτογραφία που ελεγχόταν κάθε φορά προερχόταν από το κανονικό dataset. Η παράμετρος που δόθηκε στο detectMultiScale είναι scaleFactor = 1.2 και minNeighbour = 5.



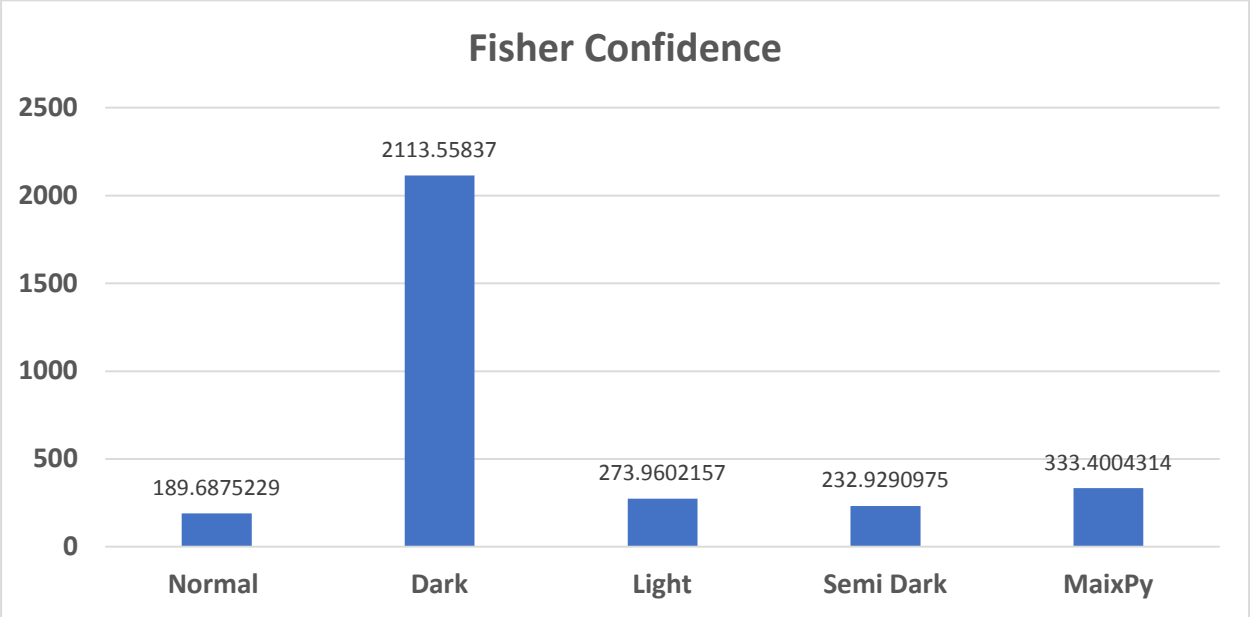
Εικόνα 5.4: Απεικόνιση Γραφικής LBPH Confidence

Πιο πάνω απεικονίζεται η γραφική παράσταση του μέσου όρου του confidence που εξάγει ο αλγόριθμος LBPH για κάθε dataset (Εικόνα 5.4). Αρχικά φαίνεται, πως οι τιμές των confidence κυμαίνονται στο εύρος 20 – 29 στο κανονικό dataset, φωτεινό dataset και ημι-σκοτεινό dataset. Ο μέσος όρος κυμαίνεται γύρω στο 77 και 88 για το σκοτεινό και MaixPy dataset, αντίστοιχα. Αρχική παρατήρηση είναι πως στις φωτογραφίες, στις οποίες το πρόσωπο του ατόμου είναι εμφανές, ο μέσος όρος τιμών κυμαίνεται σε χαμηλά επίπεδα (από 20-28). Αντιθέτως, στο σκοτεινό και MaixPy dataset, η τιμή confidence κυμαίνεται σε πολύ ψηλότερα επίπεδα από τις φωτογραφίες που φαίνεται ξεκάθαρα το πρόσωπο. Ο λόγος που συμβαίνει αυτό είναι γιατί η ευκλείδεια απόσταση μεταξύ των histograms της εικόνας εισόδου με της κάθε φωτογραφίας που ανήκουν στα dataset είναι μεγάλη. Εν τέλει, αυτό αποδεικνύει πως ο αλγόριθμος για φωτογραφίας με χαμηλό gamma value (σκοτεινό dataset) το οποίο ισοδυναμεί με φωτογραφίες στο πιο σκοτεινό μέρος του οπτικού φάσματος αδυνατεί να εξάγει ορθό αποτέλεσμα αφού σχεδόν όλα pixels της εικόνας ήταν μαύρα με αποτέλεσμα να μην αναγνωρίζονται τα χαρακτηριστικά [19]



Εικόνα 5.5: Απεικόνιση Γραφικής Eigenfaces Confidence

Πιο πάνω απεικονίζεται η γραφική παράσταση του μέσου όρου του confidence που εξάγει ο αλγόριθμος Eigenfaces σε κάθε dataset (Εικόνα 5.5). Φαίνεται πως ότι οι τιμές των confidence σε όλα τα dataset κυμαίνεται στο εύρος 7265 – 9321. Στον αλγόριθμο Eigen φαίνεται πως ο φωτισμός επηρεάζει σημαντικά (p-value = 0.036 < 0.05) την αποδοτικότητα του. Πιθανός λόγος επιρροής στην αποδοτικότητα του αλγορίθμου λαμβάνοντας υπόψη το θεωρητικό υπόβαθρο ότι ο αλγόριθμος είναι οι διαφορετικές καταστάσεις περιβάλλοντος. Πιο αναλυτικά, είναι ευάλωτος σε συνθήκες φωτισμού, στην γωνιά λήψης, στην μορφή που θα έχει το άτομο, ακόμη και στην απόσταση του ατόμου από την φωτογραφία, π.χ. όταν το άτομο βρίσκεται σε μακρινή θέση στην φωτογραφία και τα χαρακτηριστικά του προσώπου δεν βρίσκονται σε εμφανή σημείο. Παραδείγματος χάριν, παρατηρώντας το μέσο όρο της τιμής confidence στο σκοτεινό dataset σε σχέση με το ημι-σκοτεινό dataset, παρατηρείται μία ανεξήγητη συμπεριφορά αφού ο μέσος όρος του σκοτεινού σε σχέση με το ημι-σκότεινο dataset είναι 7888.322, ενώ από την άλλη είναι 9321.6935.



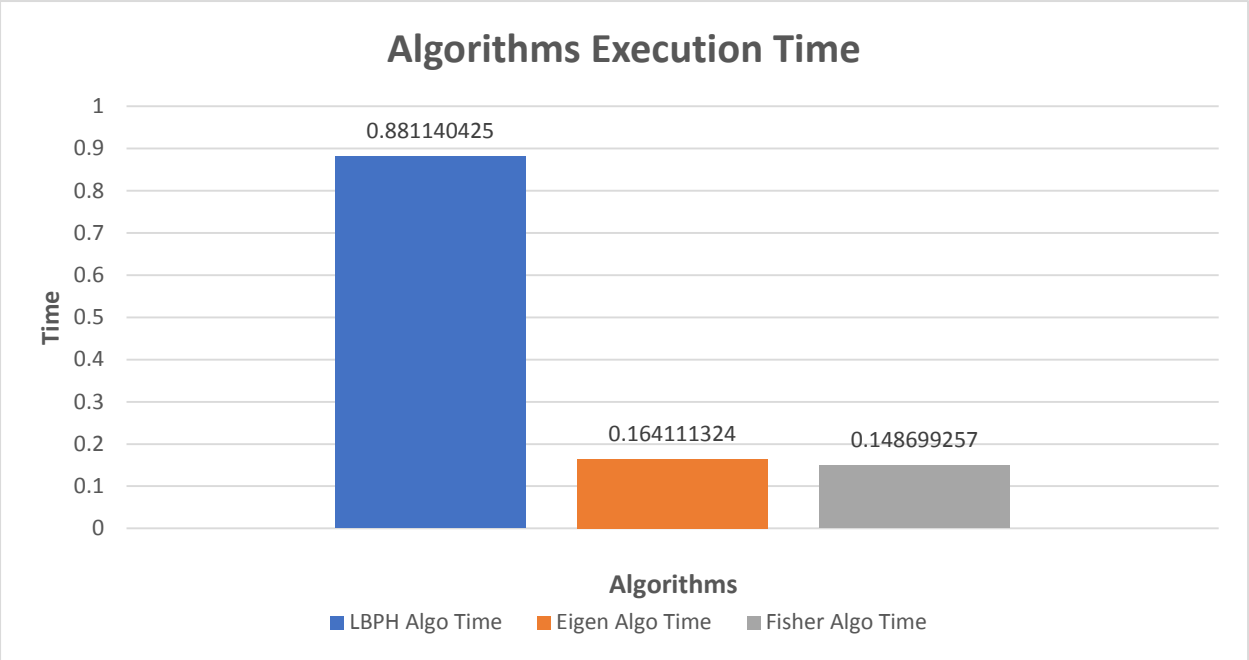
Εικόνα 5.6: Απεικόνιση Γραφικής Fisherfaces Confidence

Πιο πάνω απεικονίζεται η γραφική παράσταση του μέσου όρου του confidence που εξάγει ο αλγόριθμος Fisherfaces σε κάθε dataset (Εικόνα 5.6). Μια ενδιαφέρον παρατήρηση που εξάγεται από την Εικόνα 23 είναι ότι οι τιμές των confidence σε όλα τα dataset εκτός του σκοτεινού κυμαίνονται στο εύρος 189-333, ενώ του σκοτεινού dataset στο 2113.55.

Με βάση την θεωρία που αναλύθηκε στο κεφάλαιο 3, ο συγκεκριμένος αλγόριθμος είναι μια βελτιστοποιημένη έκδοση του αλγορίθμου Eigenfaces. Αυτό μπορεί να εξακριβωθεί βλέποντας τις τιμές των μέσων όρων confidence που πάρθηκαν, αφού είναι πιο μικρές σε σχέση με τις τιμές των μέσων όρων του αλγορίθμου Eigenfaces. Όπως είναι φυσιολογικό ο αλγόριθμος στο σκοτεινό dataset εκπαιδεύεται σε φωτογραφίες με σκοτάδι (χαμηλού φωτισμού), άρα δίνοντας ως είσοδο μια φωτογραφία κανονικού φωτισμού ο αλγόριθμος δεν καταφέρνει να εξάγει τα σωστά χαρακτηριστικά και το confidence value είναι πολύ υψηλό. Σε γενικές γραμμές, ο συγκεκριμένος αλγόριθμος δίνει πιο αξιόπιστα αποτελέσματα από τον αλγόριθμο Eigenfaces ασχέτως από το μειονέκτημα που αναφέρθηκε [14].

5.3.2 Ανάλυση χρόνου

5.3.2.1 Ανάλυση χρόνου πρόβλεψης φωτογραφίας

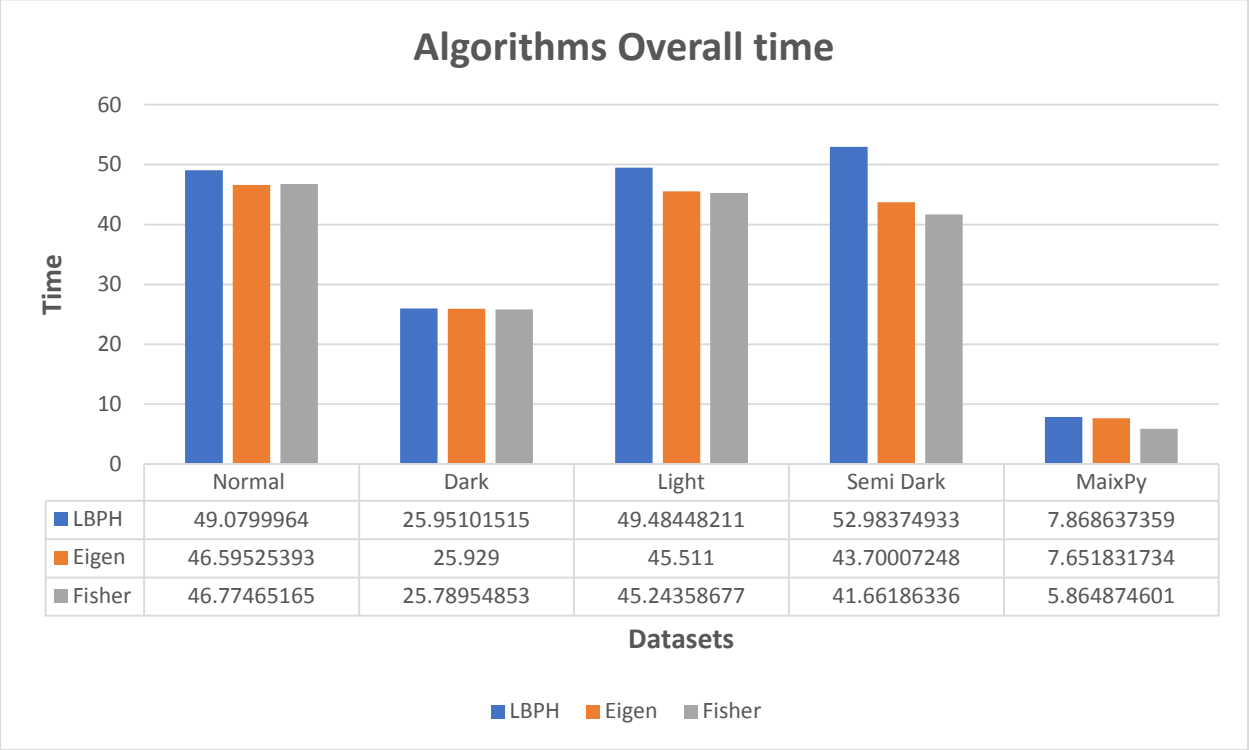


Εικόνα 5.7: Μέσος χρόνος εκτέλεσης αλγορίθμων από όλα τα dataset

Ένα σημαντικός παράγοντας αξιολόγησης των αλγορίθμων είναι ο χρόνος εκτέλεσης που απαιτείται για την πρόβλεψη του ατόμου στην φωτογραφία εισόδου. Στην Εικόνα 5.7, φαίνεται ο μέσος χρόνος εκτέλεσης του κάθε αλγόριθμου ξεχωριστά από όλα τα dataset. Παρατηρείται ότι ο μέσος χρόνος εκτέλεσης του αλγορίθμου LBPH είναι 0.8811s, του Eigenfaces 0.1641s και του Fisherfaces 0.1486s. Ο LBPH λόγω της παραγωγής των histograms καθυστερεί την αναγνώριση προσώπου, απαιτεί πολύ μεγαλύτερο χρονικό διάστημα από τους άλλους δύο αλγορίθμους. Ο LBPH είναι σχεδόν 5.8 φορές πιο αργός, αφού γίνεται σύγκριση μεταξύ όλων των histograms που δημιουργούνται για κάθε φωτογραφία. Αντιθέτως, οι άλλοι δύο αλγόριθμοι λόγω της ομοιότητας στην λειτουργία τους χρειάζονται σχεδόν όμοιο χρόνο εκτέλεσης, με το Fisherfaces να είναι ελάχιστα πιο γρήγορος από τον Eigenfaces [18].

5.3.2.2 Ανάλυση ολικού χρόνου προγράμματος

Ένας άλλος εξίσου σημαντικός παράγοντας για την ανάλυση των αλγορίθμων είναι ο ολικός χρόνος του προγράμματος. Ο συνολικός χρόνος εκτέλεσης του προγράμματος περιλαμβάνει την διαδικασία εκπαίδευσης των εικόνων στα datasets αλλά και την διαδικασία σύγκρισης με την εικόνα εισόδου.



Εικόνα 5.8: Ολικός χρόνος εκτέλεσης προγράμματος

Στην εικόνα 5.8, απεικονίζεται ο ολικός χρόνος εκτέλεσης του προγράμματος από κάθε αλγόριθμο ξεχωριστά για κάθε dataset. Συγκρίνοντας αρχικά τα datasets, παρατηρείται ότι το MaixPy έχει τον χαμηλότερο χρόνο εκτέλεσης, ακολουθεί το σκοτεινό dataset και τέλος τα υπόλοιπα τρία κυμαίνονται στο ίδιο εύρος χρόνου εκτέλεσης. Πιο συγκεκριμένα το σκοτεινό dataset απαιτεί το μισό χρόνο εκτέλεσης λόγω της μορφής του (σκοτεινές φωτογραφίες με ελάχιστο φωτισμό), άρα λιγότερη επεξεργασία. Πιθανή εξήγηση για τη ταχύτατη λειτουργία του MaiPy που να τεκμηριώνει το συγκεκριμένο αποτέλεσμα, με βάση την δική μου μελέτη και εμπειρία με το συγκεκριμένο υλικό, είναι η χαμηλή ποιότητα φωτογραφίας που εξάγει το

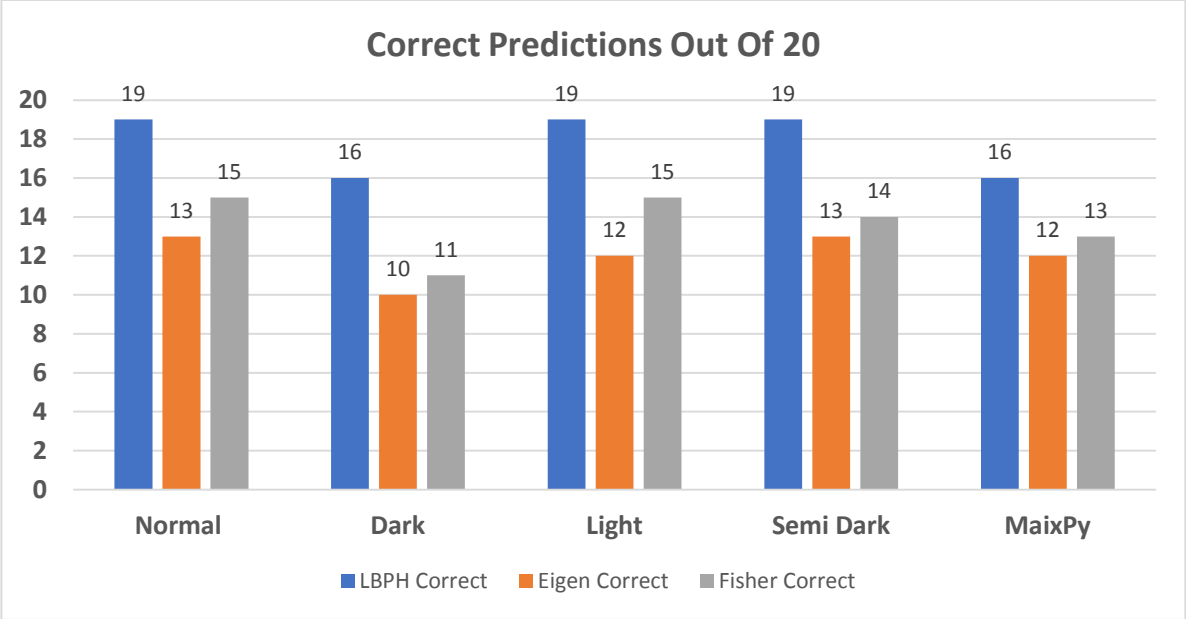
σύστημα (low resolution). Πιο συγκεκριμένα, οι φωτογραφίες που εκπαιδεύονταν στα υπόλοιπα datasets είχαν μέγεθος από 75KB μέχρι και 850KB ενώ το MaixPy dataset από 4KB μέχρι 10KB. Όπως αναφέρθηκε πιο πάνω, έτσι και τώρα ο χρόνος εκτέλεσης των αλγορίθμων ακολουθεί το ίδιο μοτίβο, δηλαδή ο πιο γρήγορος αλγόριθμος είναι ο αλγόριθμος Fisherfaces, ακολουθεί ο Eigenfaces και ο πιο αργός ο LBPH.

Αποδοτικότητα αλγορίθμων

Η αποδοτικότητα των αλγορίθμων υπολογίζεται με βάση τις σωστές προβλέψεις που επιτυγχάνουν. Όπως προαναφέρθηκε για την λήψη των πιο πάνω στατιστικών πάρθηκε από δείγμα 20 διαφορετικών φωτογραφιών. Ακολούθως, απεικονίζεται το ποσοστό επιτυχίας πρόβλεψης του κάθε αλγορίθμου σε κάθε dataset στην μορφή πίνακα αλλά και στην μορφή γραφήματος (Πίνακας 5.1; Εικόνα 5.9).

Πίνακας 5.1: Ακρίβεια αλγορίθμων

Datasets	LBPH Correct (%)	Eigen Correct (%)	Fisher Correct (%)
Normal	95	65	75
Dark	80	50	55
Light	95	60	75
Semi Dark	95	65	70
MaixPy	80	60	65

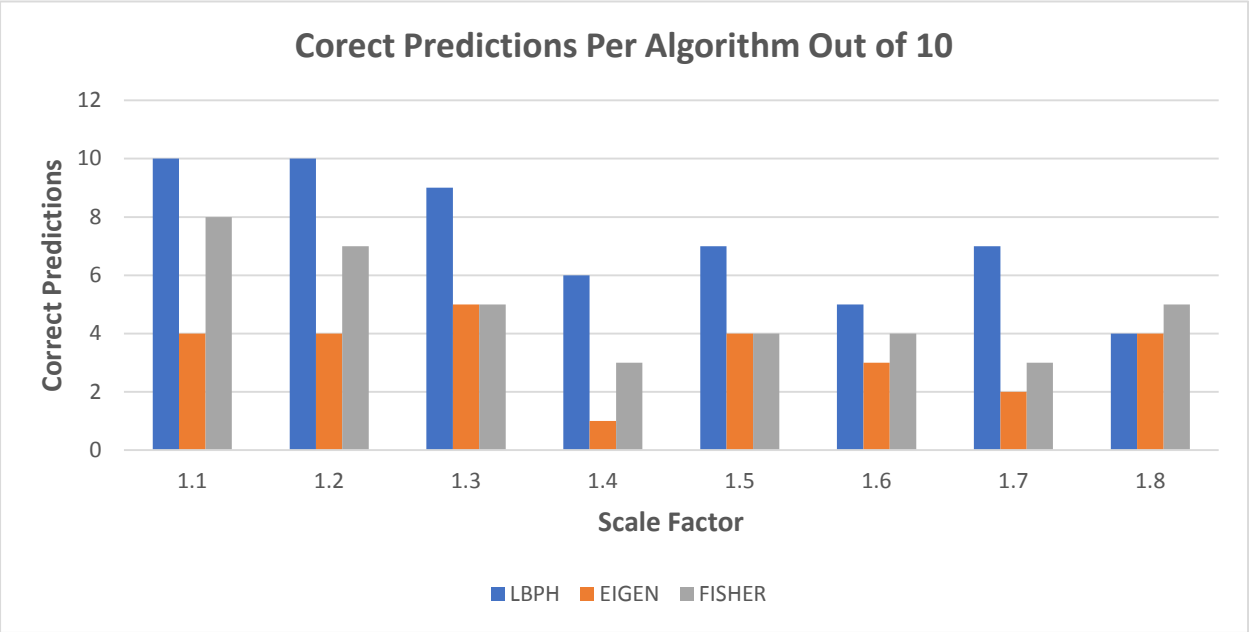


Εικόνα 5.9: Σωστές προβλέψεις αλγορίθμων στα datasets

Με βάση τα πιο πάνω δεδομένα, ο καλύτερος αλγόριθμος από τους τρεις που εξάγει το περισσότερο αριθμό ορθών προβλέψεων είναι ο αλγόριθμος LBPH με ποσοστό σωστής πρόβλεψης 80% στην χειρότερη περίπτωση και 95% στην καλύτερη (Πίνακας 5.1). Αντιθέτως, χειρότερος από τους τρεις είναι ο Eigenfaces με εύρος ποσοστού σωστής πρόβλεψης από 50% μέχρι 65%. Ο Fisherfaces αποτελεί τον δεύτερο καλύτερο αλγόριθμο με χειρότερα αποτελέσματα σωστής πρόβλεψης 55%, ενώ η καλύτερη απόδοση του έφτανε το 75%. Ο Eigenfaces φαίνεται να έχει την χειρότερη απόδοση από τους τρεις αλγορίθμους σε οποιοδήποτε dataset (Πίνακας 5.1; Εικόνα 5.9). Ο LBPH φαίνεται ξεκάθαρα να είναι ο πιο αποτελεσματικός και ακριβής αλγόριθμος, αφού δεν επηρεάζεται σε συνθήκες φωτισμού και είναι ικανός να αποκωδικοποιεί τις λεπτομέρειες στις φωτογραφίες. Αντιθέτως, ο αλγόριθμος Eigenfaces είναι ευαίσθητος σε συνθήκες φωτισμού, στη στάση του σώματος στην φωτογραφία, την γωνιά λήψης και στις διαφορετικές εκφράσεις του προσώπου. Όπως αναφέρθηκε στο κεφάλαιο 3 ο Fisherfaces εξαρτάται σε μεγάλο βαθμό στα δεδομένα εισόδου. Ένα επιπλέον μειονέκτημα που πιθανόν να προκαλεί το συγκεκριμένο αποτέλεσμα, είναι η μεγάλη διασκόρπιση ανάμεσα στις τάξεις τότε συνεπάγεται και με μεγάλη διασκόρπιση των εξωτερικών κλάσεων. [20]

5.3.3 Ανάλυση scaleFactor

Το scaleFactor θεωρήθηκε ένας σημαντικός παράγοντας στην απόδοση της επίτευξης αναγνώρισης προσώπου, προκειμένου να ερευνηθεί πως επηρεάζει κρατήθηκε σταθερό το minNeighbour με αριθμό 5 και το scaleFactor άλλαζε με εύρος τιμών από 1.1 μέχρι 1.8. Για την εύρεση των υπόλοιπων στατιστικών έγινε χρήση του κανονικού dataset με συνολικό αριθμό δειγμάτων ήταν 10 (n = 10).



Εικόνα 5.10: Ορθές κατηγοριοποιήσεις αλγορίθμων σε σχέση με την μεταβολή του scaleFactor.

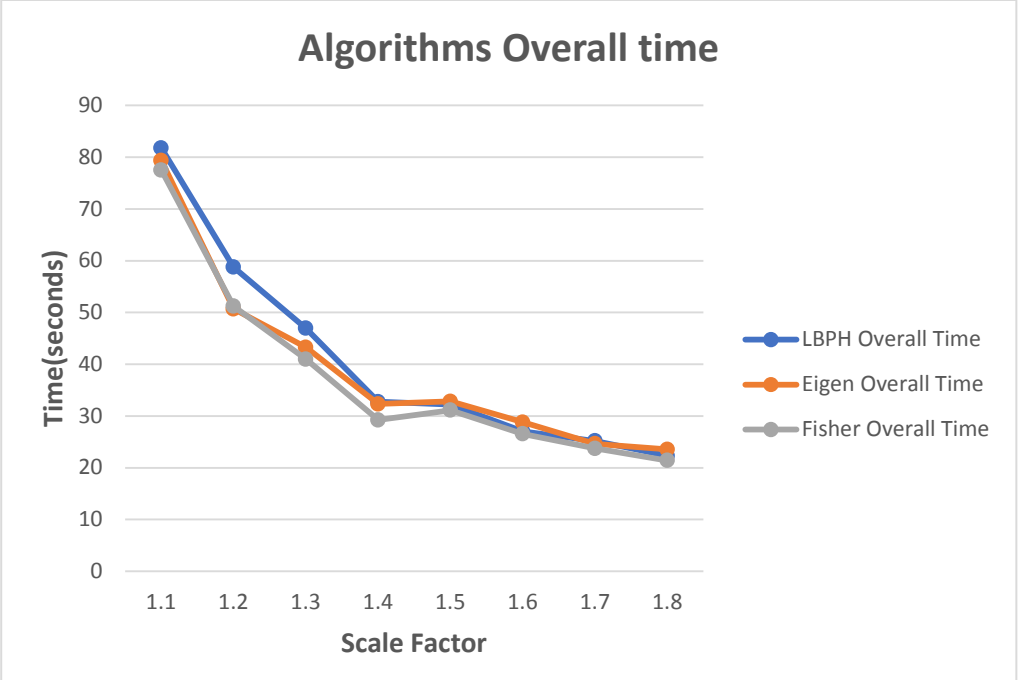
Στην Εικόνα 5.10, απεικονίζονται οι σωστές προβλέψεις των αλγορίθμων αυξάνοντας σταδιακά την παράμετρο scaleFactor. Όπως φαίνεται από τη γραφική, αλλά και όπως ειπώθηκε ήδη προηγουμένως, ο αλγόριθμος LBPH επιτυγχάνει περισσότερες ορθές προβλέψεις σε σύγκριση με τους άλλους δύο. Όσο πιο μικρή τιμή λαμβάνει η παράμετρος scaleFactor, τόσο περισσότερα επίπεδα υπάρχουν στην scale pyramid και περεταίρω ανάλυση της εικόνας, άρα μεγαλύτερη πιθανότητα ανίχνευσης προσώπων. Καθώς αυξάνεται η τιμή, παρατηρείται σταδιακή μείωση των ορθών προβλέψεων και από τους τρεις αλγορίθμους.

Για επιπλέον ανάλυση της συγκεκριμένης παραμέτρου, παρουσιάζονται αναλυτικά τα στατιστικά που καταγράφτηκαν καθώς αυξάνεται η τιμή του scaleFactor (Πίνακας 5.2). Πιο αναλυτικά παρουσιάζονται για κάθε αλγόριθμο ξεχωριστά οι αποτυχημένες προσπάθειες εύρεσης προσώπου, οι λανθασμένες κατηγοριοποιήσεις σε τυχόν εύρεση προσώπου και οι ορθές προβλέψεις. Κοινό χαρακτηριστικό των τριών αλγορίθμων που προκύπτει καθώς αυξάνεται το scaleFactor είναι η αύξηση αποτυχίας ανίχνευσης προσώπου, αφού υπάρχει μείωση των επιπέδων στην scale pyramid.

Όταν τεθεί το scaleFactor ίσο με 1.1, σημαίνει ότι το στάδιο μείωσης της φωτογραφίας κάθε φορά είναι 10%. Πιο συγκεκριμένα, το μοντέλο κατά την διάρκεια εκπαίδευσης έχει σταθερό μέγεθος, άρα θέτοντας μικρό βήμα μείωσης, αυξάνονται οι πιθανότητες να βρεθεί ένα αντίστοιχο μέγεθος με το μοντέλο ανίχνευσης (1.2 ισοδυναμεί με μείωση 20%, 1.3 ισοδυναμεί με μείωση 30% κ.ο.κ).

Πίνακας 5.2: Σωστές προβλέψεις, αποτυχία ανίχνευσης προσώπου (FtD) και λανθασμένη πρόβλεψη προσώπου (WD) ανάλογα με την αλλαγή του Scale Factor από 1.1 - 1.8

Overall 10	**LBPH**		**Eigen**		**Fisher**		**Correct Predictions**		
Scale Factor	**FtD**	**WD**	**FtD**	**WD**	**FtD**	**WD**	**LBPH**	**Eigen**	**Fisher**
1.1	0	0	0	6	0	2	10	4	8
1.2	0	0	1	5	1	2	10	4	7
1.3	0	1	2	3	2	3	9	5	5
1.4	2	2	4	5	4	3	6	1	3
1.5	1	2	5	1	5	1	7	4	4
1.6	4	1	6	1	6	0	5	3	4
1.7	1	2	6	2	6	1	7	2	3
1.8	6	0	4	2	4	1	4	4	5



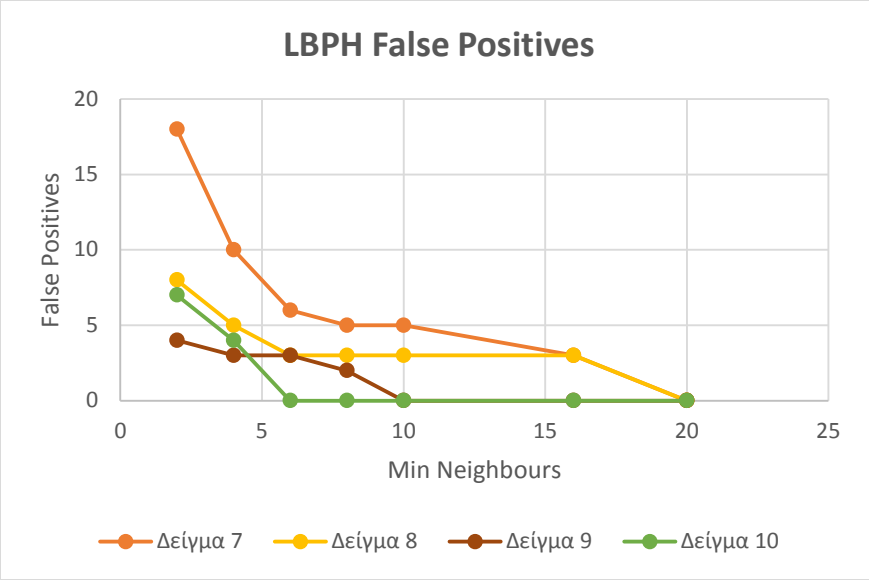
Εικόνα 5.11: Συνολικός χρόνος εκτέλεσης αλγορίθμων σε σχέση με την μεταβολή του scaleFactor

Καθώς αυξάνεται η παράμετρος scaleFactor ο ολικός χρόνος εκτέλεσης των αλγορίθμων (εκπαίδευση φωτογραφιών στην βάση δεδομένων και η διάρκεια αναγνώρισης προσώπου με την φωτογραφία εισόδου) μειώνεται (Εικόνα 5.11). Όταν έχει μικρή τιμή το scaleFactor υπάρχουν περισσότερα επίπεδα επεξεργασίας (μικρές μειώσεις του μεγέθους της φωτογραφίας), με αποτέλεσμα να απαιτείται περισσότερος χρόνος εκπαίδευσης και ανάλυσης της φωτογραφίας εισόδου. Καθώς αυξάνεται τα επίπεδα επεξεργασίας συνεπάγεται σε λιγότερη χρονική διάρκεια που χρειάζονται οι αλγόριθμοι για την εκπαίδευση τους. Με άλλα λόγια, η παράμετρος scaleFactor αποτελεί πολύ σημαντική παράμετρο για την χρονική διάρκεια της εκπαίδευσης και σύγκρισης του αλγόριθμου. Τέλος, ο συνολικός χρόνος με την αλλαγή του scaleFactor ακολουθεί παρόμοια πτωτική πορεία και για τους τρείς αλγορίθμους με σημαντική αλλαγή στη κλίση των γραμμών από τον scaleFactor 1.1 – 1.4 και στο τέλος αυτή να ομαλοποιείται.

5.3.4 Ανάλυση minNeighbour

Η δεύτερη σημαντική παράμετρος που χρησιμοποιήθηκε είναι η minNeighbour. Όπως εξηγήθηκε πιο πάνω η συγκεκριμένη παράμετρος καθορίζει τον αριθμό των «προσώπων» που θα

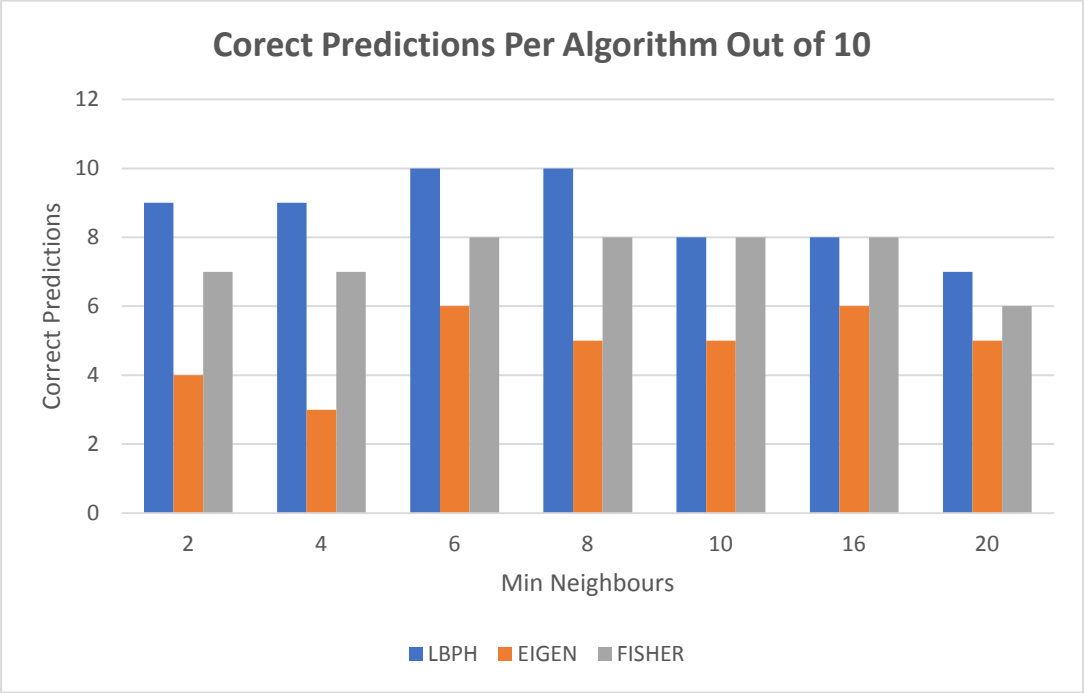
ανιχνευθούν, των false positives και τον true positives. Αποτελεί ένα σημαντικό παράγοντα στην απόδοση της επίτευξης αναγνώρισης προσώπου και προκειμένου να ερευνηθεί πως επηρεάζει την απόδοση των αλγορίθμων, κρατήθηκε σταθερό το scaleFactor με τιμή 1.1, ενώ το minNeighbour άλλαζε από 2 μέχρι 20. Αξίζει να αναφερθεί ότι οι αλγόριθμοι Eigenfaces και Fisherfaces μόνο σε μια περίπτωση από τις δέκα, εξήγαγαν false positives και έτσι δεν υλοποιήθηκε γραφική παράσταση απεικόνισης των false positives για τους αλγορίθμους αυτούς (Εικόνα 5.12). Αντιθέτως, ο αλγόριθμος LBPH είναι πιο ευάλωτος στην τιμή που τέθηκε στο minNeighbours και εξάγει πολύ περισσότερα false positives. Μέσω των δέκα τυχαίων δειγμάτων που λήφθηκαν επιλέχθηκαν τα τέσσερα με τα περισσότερα false positives έτσι ώστε να καταστρωθεί η πιο κάτω γραφική.



Εικόνα 5.12: LBPH False Positives Τεσσάρων Δειγμάτων

Θέτοντας με χαμηλή τιμή την παράμετρο minNeighbours παρατηρούνται τα περισσότερα false positives (Εικόνα 5.12). Αυξάνοντας σταδιακά την τιμή του, παρατηρείται μείωση στα false positives, αλλά δεν υπάρχει το ίδιο αντίκτυπο σε κάθε φωτογραφία. Λόγω της δομής της κάθε φωτογραφίας και του μοναδικού περιβάλλοντος της κάθε μιας, η τιμή του minNeighbours πρέπει να εναλλάσσεται ανάλογα, έτσι έπρεπε να βρεθεί μια τιμή όπου στην περίπτωση της αναγνώρισης προσώπου με haar cascade frontal face να μην εξάγει false positives. Με βάσει τα

υπόλοιπα δεδομένα επιλέχθηκε μια «μέση» ικανοποιητική τιμή του minNeighbours χωρίς να υπάρξουν false positives αλλά και ταυτόχρονα χωρίς να υπάρξει απώλεια των προσώπων, ως η τιμή 5. Γι' αυτό επιλέχθηκε η τιμή 5 για την εύρεση των υπόλοιπων στατιστικών και απορρίφθηκε η τιμή 20 ως το τελικό minNeighbours, λόγω απώλειας αληθινών προσώπων (true positives).

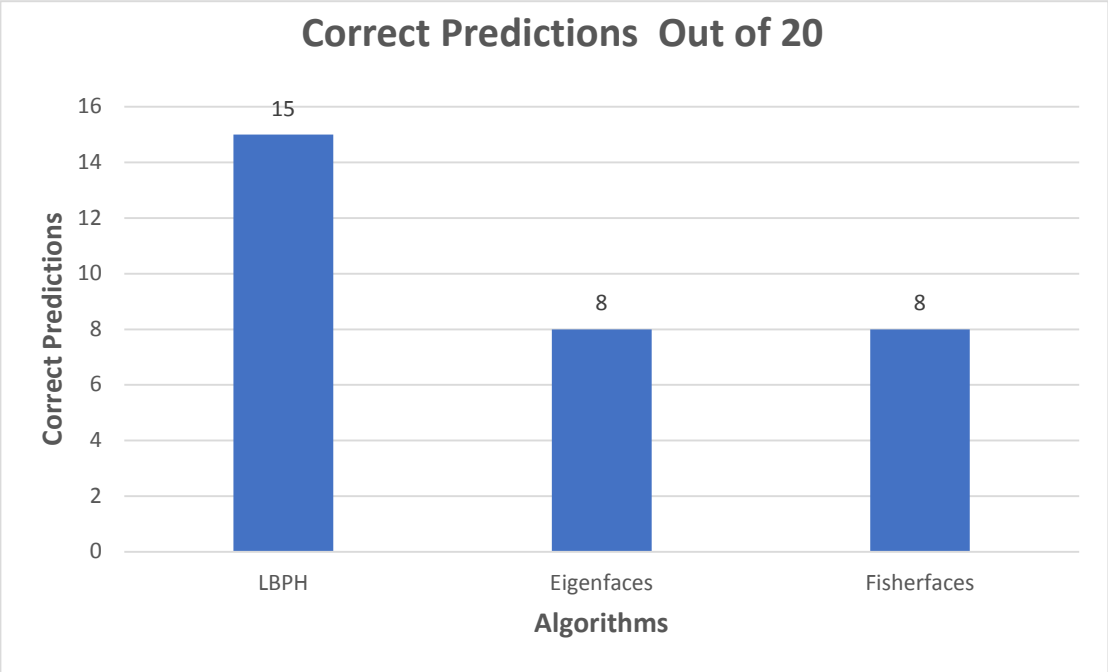


Εικόνα 5.13: Σωστές προβλέψεις αλγορίθμων

Παρατηρώντας την Εικόνα 5.13, συμπεραίνεται η ίδια παρατήρηση με τις υπόλοιπες γραφικές των ορθών προβλέψεων. Δηλαδή, τα περισσότερα ορθά αποτελέσματα τα εξάγει ο αλγόριθμος LBPH, ακολουθεί ο Fisherfaces και με τα λιγότερα ορθά αποτελέσματα ο Eigenfaces. Παρατηρείται εν τέλει, ότι καθώς αυξάνεται η τιμή του minNeighbours μειώνεται η πιθανότητα ανίχνευσης των αληθινών προσώπων που βρίσκονται στις φωτογραφίες (loss of true positives). Η τιμή που αρχικοποιείται το minNeighbour καθορίζει το μέγεθος της γειτονιάς που απαιτείται να διατηρήσει για να καθοριστεί ένα τετράγωνο ως πρόσωπο, άρα θέτοντας το μεγάλο οι πιθανότητες να ξεπερνιέται η συγκεκριμένη τιμή είναι μικρότερες. Έτσι αυξάνοντας την τιμή αυτή η εύρεση των true positives μειώνονται. [16]

5.3.5 Ανάλυση για φωτογραφίες με δύο άτομα

Θεωρήθηκε επίσης ενδιαφέρον να ελεγχθούν οι φωτογραφίες εισόδου που περιείχαν δύο άτομα προκειμένου να αναλυθεί η συμπεριφορά των αλγορίθμων σε πιο σύνθετες συνθήκες. Οι παράμετροι που δόθηκαν στο πρόγραμμα ήταν ο minNeighbour ίσος με 5, ο scaleFactor ίσος με 2 και ο συνολικός αριθμός δειγμάτων ήταν 10. Κατ' επέκταση η μέγιστη δυνατή επίτευξη επιτυχημένων προβλέψεων στο σύνολο ήταν 20.



Εικόνα 5.14: Σωστές προβλέψεις Αλγορίθμων με δύο άτομα

Στην Εικόνα 5.14, απεικονίζονται οι ορθές προβλέψεις του κάθε αλγορίθμου ξεχωριστά για τις φωτογραφίες εισόδου υπήρχαν δύο άτομα. Όπως, φαίνεται η συμπεριφορά των αλγορίθμων είναι παρόμοια και με τις υπόλοιπες δοκιμές, δηλαδή ο LBPH δίνει τα καλύτερα αποτελέσματα και πιο συγκεκριμένα με 15 επιτυχημένες προσπάθειες. Αντιθέτως οι αλγόριθμοι eigenfaces και Fisherfaces εξάγουν ορθά αποτελέσματα μόλις στις 8 προσπάθειες από τις 20. Το αποτέλεσμα αυτό οφείλεται στα μειονεκτήματα των αλγορίθμων που προαναφέρθηκαν πιο πάνω.

Κεφάλαιο 6

Συμπεράσματα

6.1 Γενικά Συμπεράσματα

Με την διεκπεραίωση της διπλωματικής εργασίας κατέληξα σε αρκετά συμπεράσματα σχετικά με το συγκεκριμένο εργαλείο, την βιβλιοθήκη OpenCV και τους αλγορίθμους που χρησιμοποιήθηκαν. Καθώς περνούν τα χρόνια οι τεχνολογίες αναπτύσσονται με ραγδαίους ρυθμούς και μέρα με την μέρα ολοένα και ενσωματώνονται στην ζωή μας. Παρατηρούνται εργαλεία όπως το M1W Dock Tool Kit τα οποία προσφέρουν άπειρες δυνατότητες machine vision με ελάχιστο οικονομικό κόστος. Με τα συγκεκριμένα αντικείμενα και με τον σωστό χειρισμό η ασφάλεια του ανθρώπου διασφαλίζεται σε μεγάλο βαθμό, ενώ παράλληλα οι λειτουργίες που παρέχουν διευκολύνουν σε διάφορους τομείς την ζωή του. Εν κατακλείδι, ο διαχειριστής μπορεί με σχετική ευκολία να διαχειρίζεται οποιοδήποτε τέτοιο σύστημα ασφαλείας ανά πάσα στιγμή, από οπουδήποτε, μέσω κάποιας συσκευής.

6.2 Συμπεράσματα Αλγορίθμων

Στην διπλωματική εργασία χρησιμοποιήθηκαν τρεις διαφορετικοί αλγόριθμοι για την δημιουργία του συστήματος ασφαλείας, ο κάθε ένας με τα πλεονεκτήματα αλλά και τα μειονεκτήματα του. Ένα σύστημα ασφαλείας αναγνώρισης προσώπου αποτελεί μια βιομετρική μέθοδο αναγνώρισης, η οποία αποσκοπεί στην άμεση ταυτοποίηση του ατόμου αλλά και στην προειδοποίηση από

κακόβουλες ενέργειες. Όπως είναι γνωστό, σε ένα σύστημα ασφαλείας υπάρχουν κάποιοι παράγοντες οι οποίοι το καθιστούν επιτυχημένο. Στο συγκεκριμένο σύστημα, οι παράγοντες που καθορίστηκαν απαραίτητοι για να θεωρηθεί επιτυχημένο, είναι η ταχύτητα αναγνώρισης, η ακρίβεια και η αποδοτικότητα των αλγορίθμων.

Για την αξιολόγηση και λήψη συμπερασμάτων σχετικά με τους αλγορίθμους έγινε ανάλυση των τιμών confidence, που εξάγουν την αποδοτικότητα και εξετάστηκε ο χρόνος εκπαίδευσης και σύγκρισης των φωτογραφιών του dataset με την φωτογραφία εισόδου. Πρώτα εξάγεται το συμπέρασμα ότι ο Eigenfaces παράγει το υψηλότερο confidence, έπειτα ακολουθεί ο Fisherfaces, ενώ ο LBPH παρέχει το χαμηλότερο και άρα το πιο επιθυμητό. Αξίζει να αναφερθεί ότι ο κάθε αλγόριθμος εξάγει διαφορετικό εύρος τιμής confidence, και η κάθε τιμή confidence δεν σχετίζεται με την τιμή των άλλων αλγορίθμων, δηλαδή ο LBPH περίπου 20-90, ο fisherfaces 100-350 και ο eigenfaces 7000-9500. Παρά το γεγονός ότι ο LBPH είναι πιο αργός στην εκπαίδευση των φωτογραφιών σε σχέση με τους άλλους δύο αλγορίθμους, εντούτοις, είναι ο πιο αποδοτικός από τους άλλους δύο, αφού σε όλες τις προσπάθειες, αλλάζοντας τις παραμέτρους, δίνει τα καλύτερα αποτελέσματα. Εξάγεται το συμπέρασμα ότι ο LBPH είναι ο ιδανικότερος, αφού αποτελεί τον αλγόριθμο που επιφέρει τις περισσότερες επιτυχημένες προσπάθειες αναγνώρισης προσώπου αλλά και την ανθεκτικότητα του σε αλλαγές περιβάλλοντος. Αντιθέτως, οι άλλοι δύο αλγόριθμοι έχουν το μειονέκτημα του φωτισμού, κυρίως ο Eigenfaces, επηρεάζοντας έτσι το αποτέλεσμα τους. Η απόδοση των τριών αλγορίθμων εξαρτάται σε μεγάλο βαθμό από τις εικόνες εκπαίδευσης, τις παραμέτρους που λαμβάνει η μέθοδος detectMultiScale και από τον haar cascade classifier.

Οι κύριες παράμετροι που ξεχώρισαν ήταν:

- Φωτισμός της φωτογραφίας
- Πόζα ατόμου (στάση)
- Γωνιά λήψης φωτογραφίας
- Φωτογραφία μπροστινής όψης (πρόσωπο)
- Μέγεθος των datasets
- Απόσταση λήψης φωτογραφίας

6.3 Μελλοντικές Προτάσεις

Μετά από πειραματισμό με το εργαλείο M1W Dock Tool Kit επιτεύχθηκε η ενσωμάτωση αρκετών δυνατοτήτων στην παρούσα διπλωματική εργασία. Μια επιπλέον δυνατότητα που θα μπορούσε να προσφέρει το εργαλείο αυτό, είναι η διασύνδεση στο διαδίκτυο, κάτι το οποίο δεν αναπτύχθηκε εδώ. Πιο συγκεκριμένα, για ένα πλήρως αυτοματοποιημένο σύστημα, απαιτείται η ένωση του εργαλείου στο διαδίκτυο μέσω Wi-Fi, για να γίνεται περαιτέρω επεξεργασία σε εξωτερικά περιβάλλοντα. Εστιάζοντας μόνο στις δυνατότητες που προσφέρει το εργαλείο εσωτερικά -χωρίς την σύνδεση στο Wi-Fi- εντοπίζονται κάποιοι περιορισμοί (π.χ. μνήμη συστήματος, γλώσσα προγραμματισμού – περιορισμένες βιβλιοθήκες). Μια δεύτερη πρόταση, είναι η αναγνώριση προσώπων σε αληθινό χρόνο που θα ανιχνεύονταν από το σύστημα μέσω video. Κλείνοντας, προτείνεται περαιτέρω αξιολόγηση και σύγκριση με άλλους αλγορίθμους αναγνώρισης προσώπου όπως αλγορίθμους Deep Neural Networks (DNN) ή Convolutional Neural Networks (CNN), για επιπλέον βελτιστοποίηση του συστήματος.

Βιβλιογραφία

[1] Cohen-Almagor, R., 2013. Internet history. In *Moral, ethical, and social dilemmas in the age of technology: Theories and practice* (pp. 19-39). IGI Global.

[2] Andrew Braun, 2019, History of IoT: *A Timeline of Development, IoT Tech Explained*, viewed 20 April 2020, <https://www.iottechtrends.com/history-of-iot/>

[3] Gruszczyńska, B., 2004. Crime in Central and Eastern European countries in the enlarged Europe. *European Journal on Criminal Policy and Research*, 10(2-3), pp.123-136.

[4] Tan, L. and Wang, N., 2010, August. Future internet: The internet of things. In *2010 3rd international conference on advanced computer theory and engineering (ICACTE)* (Vol. 5, pp. V5-376). IEEE.

[5] Sinha G. Gaurav, 2018, The evolution of Smart Home Technology, BCC Research, viewed 20 April 2020, <http://blog.bccresearch.com/the-evolution-of-smart-home-technology>

[6] Margaret Rouse, n.d., facial recognition, viewed April 22, <https://searchenterpriseai.techtarget.com/definition/facial-recognition>

[7] Divyesh Dharaiya, 2020, History of Facial Recognition Technology and its Bright Future, viewed April 22, <https://readwrite.com/2020/03/12/history-of-facial-recognition-technology-and-its-bright-future/>

[8] Dinalankara, L., 2017. Face detection & face recognition using open computer vision classifies. *ResearchGate*.

[9] Soo, S., 2014. Object detection using Haar-cascade Classifier. *Institute of Computer Science, University of Tartu*, pp.1-12.

[10] Sipeed M1 Dock Review, n.d., viewed April 26, <https://educ8s.tv/sipeed-m1-dock-review/>

[11] MaixPy Sipeed Documentation, n.d., viewed April 26 <https://maixduino.sipeed.com/en/hardware/k210.html>

[12] Neo Ighodaro, n.d., <https://blog.pusher.com/laravel-mvc-use/>

[13] Laravel Documentation, n,d, viewed April 28, < https://laravel.com/docs/7.x>

[14] Docs OpenCV, n.d., Face Recognition with OpenCV, <https://docs.opencv.org/3.4/da/d60/tutorial_face_main.html>

[15] Minichino, J. and Howse, J., 2015. *Learning OpenCV 3 Computer Vision with Python*. Packt Publishing Ltd.

[16] OpenCV. Cascade Classification., n.d., viewed May 01, 2020, <https://docs.opencv.org/2.4/modules/objdetect/doc/cascade_classification.html#cascade-classification>

[17] OpenCV, cv::Face::FaceRecognizer Class Reference, viewed May 01,2020, <https://docs.opencv.org/master/dd/d65/classcv_1_1face_1_1FaceRecognizer.html#ab0d593e53ebd9a0f350c989fcac7f251>

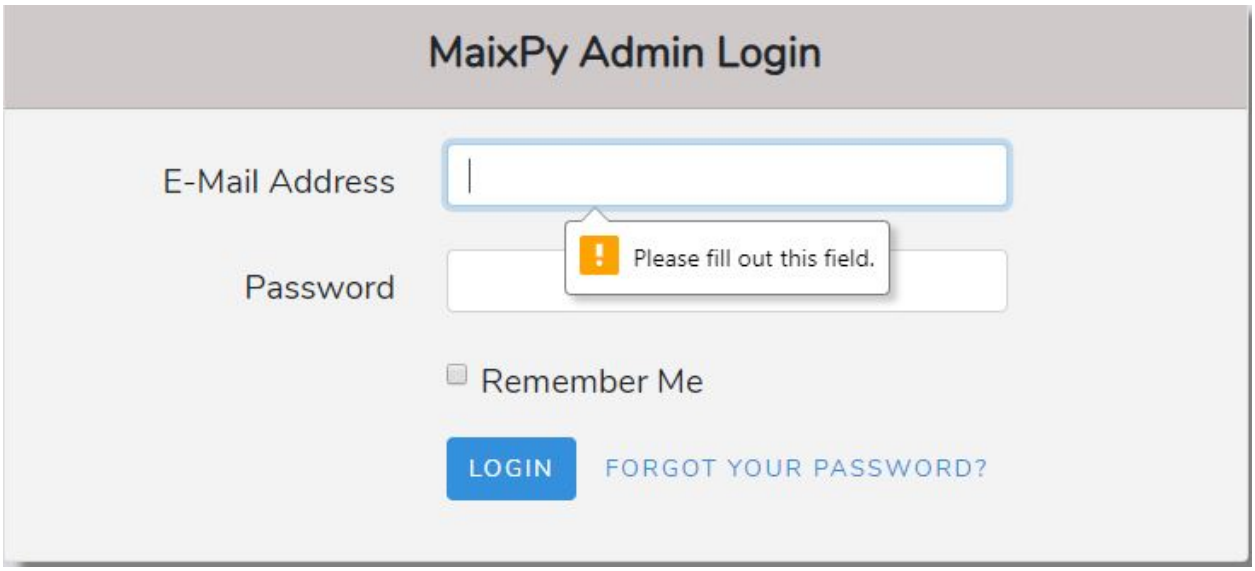
[18] Çarıkçı, M. and Özen, F., 2012. A face recognition system based on eigenfaces method. *Procedia Technology*, *1*, pp.118-123.

[19] Rosebrock A., 2015, OpenCV Gamma Corerection, Viewed 10 April 2020, <https://www.pyimagesearch.com/2015/10/05/opencv-gamma-correction/>

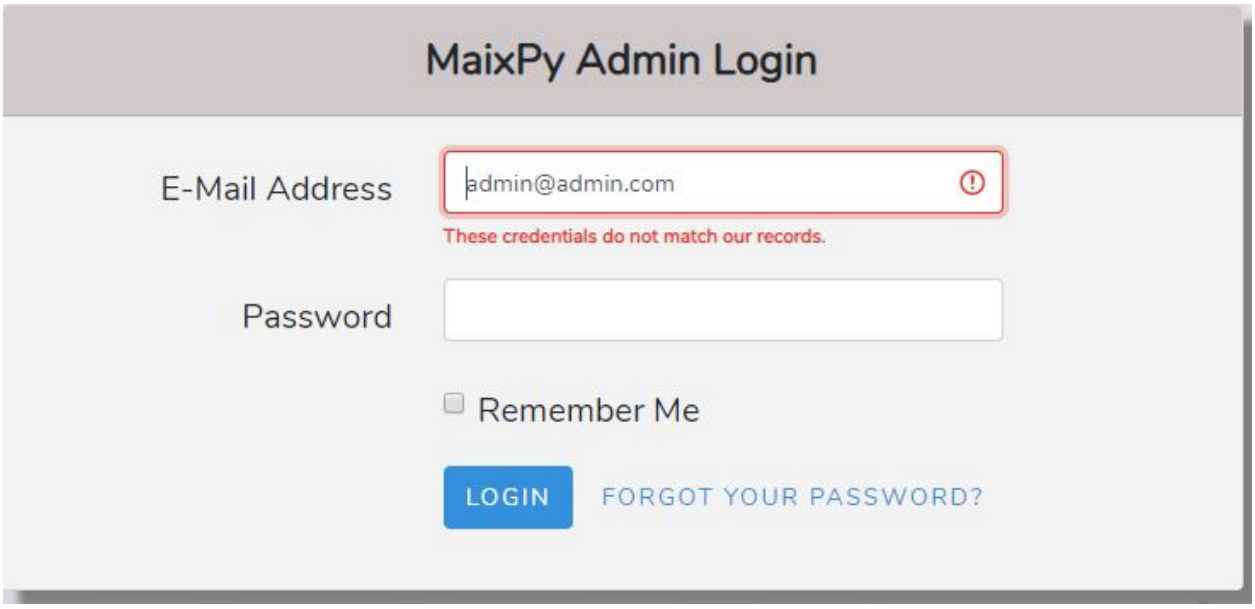
[20] Khurana, L., Chauhan, A. and Singh, P., 2020, January. Comparative Analysis of OpenCV Recognisers for Face Recognition. In *2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence)* (pp. 485-490). IEEE.

[21] Kelvin Salton, 2017, Face Recognition: Understanding LBPH Algorithm, <https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b>

Παράρτημα Α

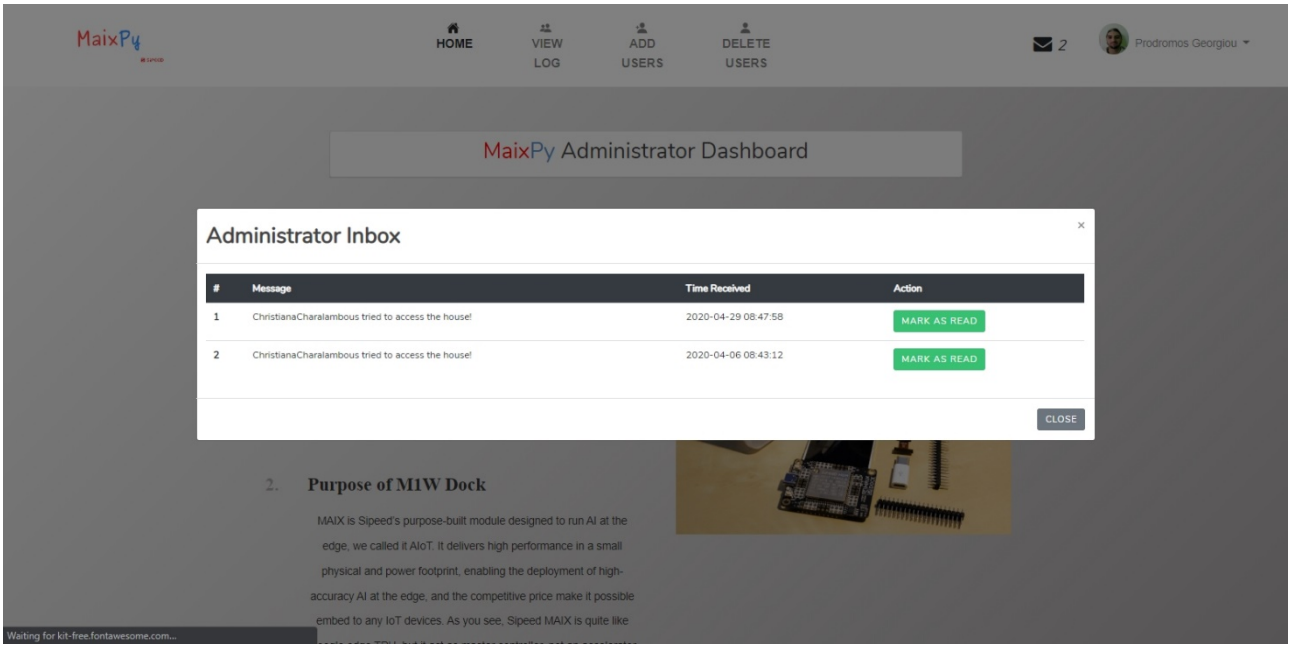


Πιο πάνω απεικονίζονται τα προειδοποιητικά μηνύματα που εμφανίζονται όταν ο χρήστης δεν εισάγει τον κωδικό ή το ηλεκτρονικό του email.

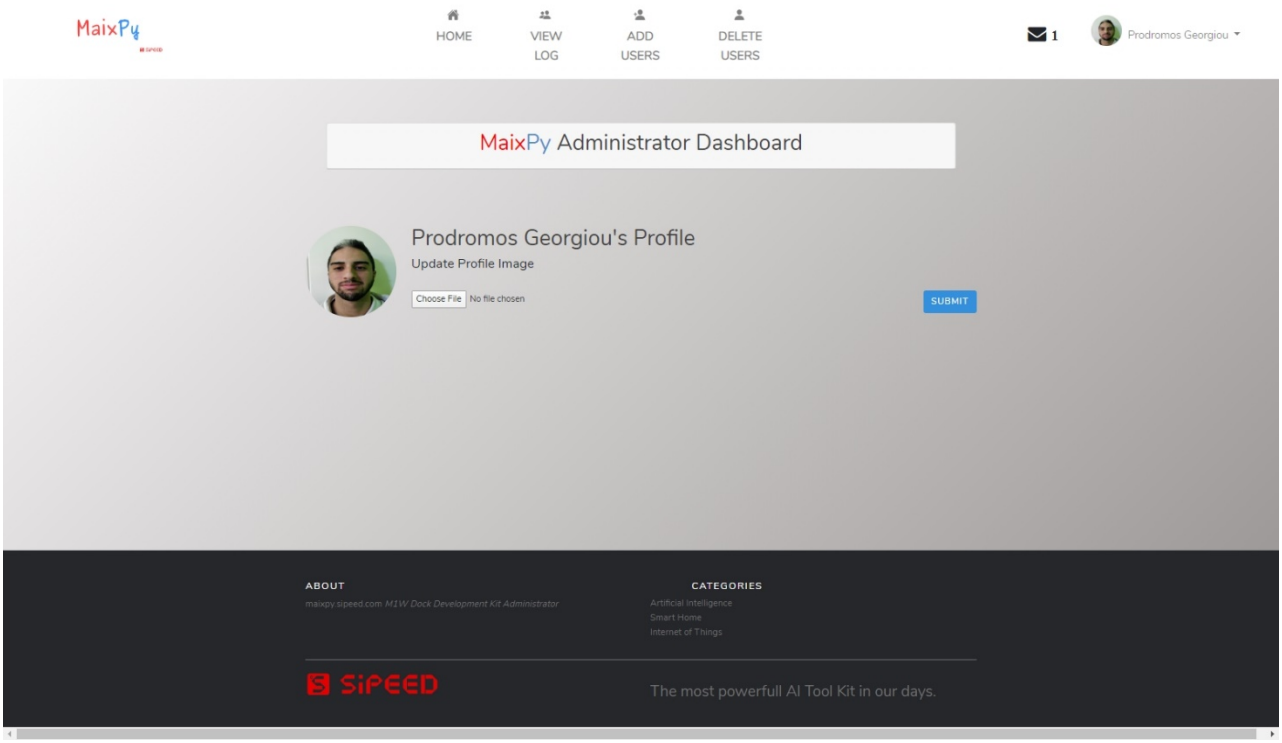


Πιο πάνω απεικονίζονται τα μηνύματα λάθους που εμφανίζονται όταν ο χρήστης εισάγει λανθασμένο email ή λανθασμένο κωδικό.

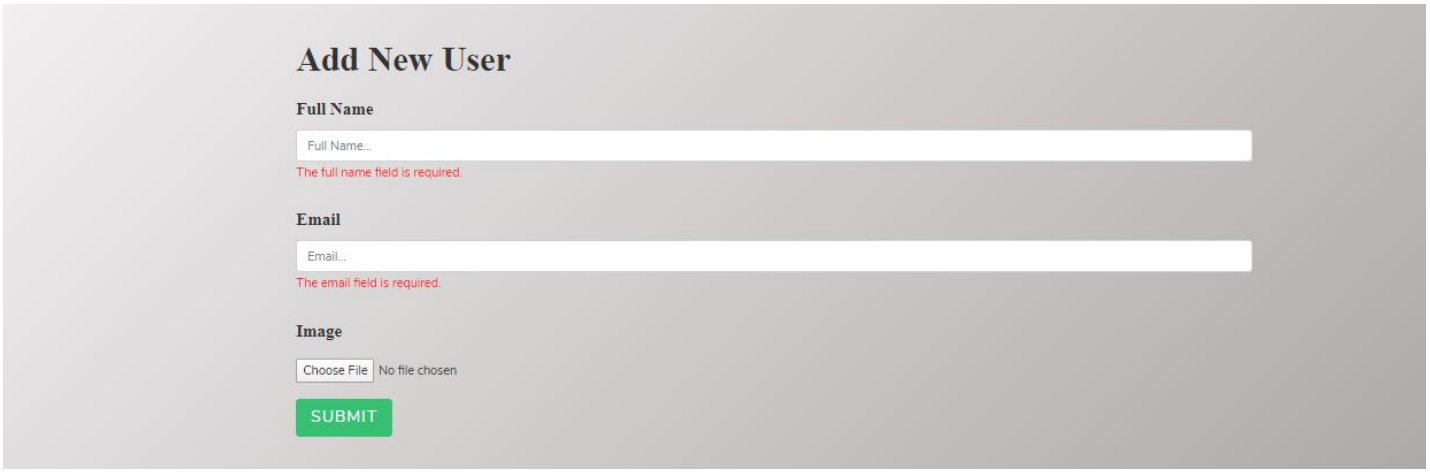
Πιο πάνω απεικονίζεται το μενού πλοήγησης και είναι ευδιάκριτο το ενεργό link που βρίσκεται ο διαχειριστής. Αριστερά εμφανίζεται το logo του MaixPy το οποίο επιλέγοντας το ανακατευθύνεται στο home webpage. Επιλέγοντας το όνομα του διαχειριστή εμφανίζεται ένα drop-down menu στο οποίο έχει την επιλογή να πλοηγηθεί.



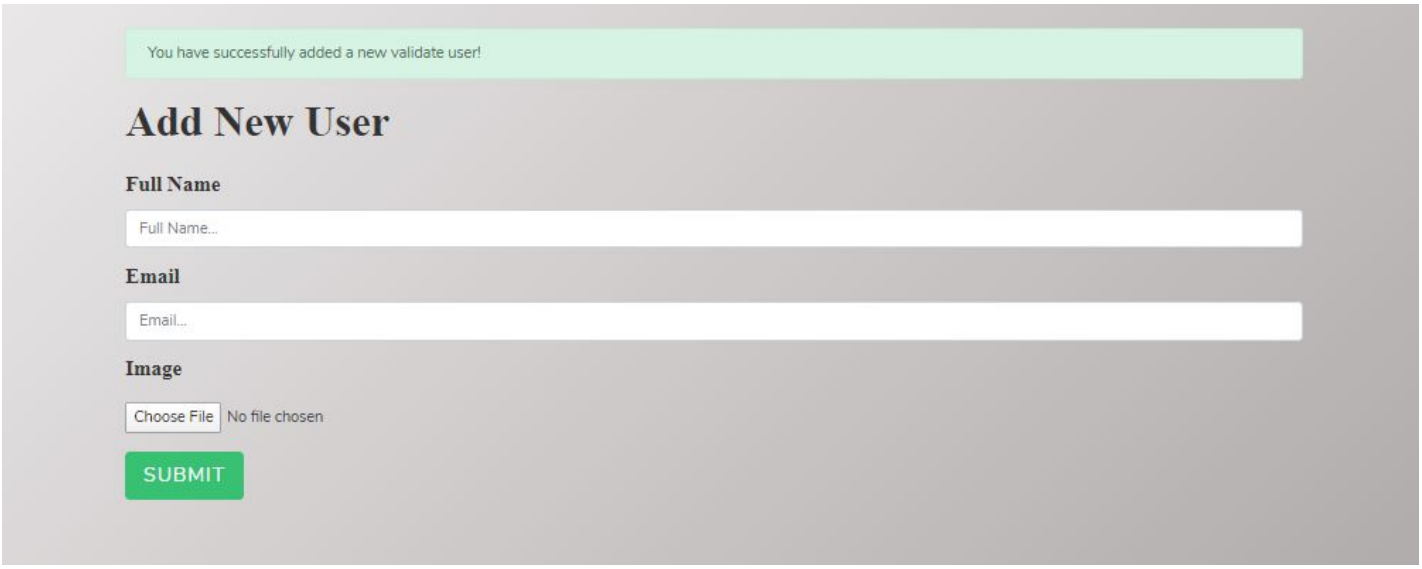
Επιλέγοντας το εικονίδιο φακέλου στο μενού πλοήγησης εμφανίζεται ένα pop up παράθυρο στο οποίο εμφανίζονται λεπτομέρειες για τα άτομα που ανιχνεύθηκαν από το σύστημα. Πιο συγκεκριμένα φαίνεται το μήνυμα, η ώρα και η επιλογή Mark as Read, το οποίο εάν το επιλέξει θεωρείται ως διαβασμένο μήνυμα.



Επιλέγοντας την επιλογή profile στο drop-down μενού, ανακατευθύνεται στην συγκεκριμένη διεπιφάνεια. Ο διαχειριστής έχει την επιλογή να επιλέξει εικόνα προφίλ αλλά έχει και την δυνατότητα να την αφήσει κενή.



Εμφάνιση μηνυμάτων σφάλματων κατά την διάρκεια δημιουργίας καινούργιου χρήστη. Η επιλογή εικόνας στον εγγεγραμμένο χρήστη είναι προαιρετική.



Επιτυχής δημιουργία καινούργιου εγγεγραμμένου χρήστη και εμφάνιση μηνύματος επιτυχίας.

Διαγραφή υφιστάμενου εγγεγραμμένου χρήστη. Εμφάνιση μηνύματος για την επιτυχή διαγραφή του χρήστη.