Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής- Ανάπτυξη Λογισμικού και Τεχνητής Νοημοσύνης»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Σχεδίαση και υλοποίηση εφαρμογής ταυτοποίησης με βιομετρικά στοιχεία και αναγνώριση εγγράφων με χρήση κινητών συσκευών** **Design and development of mobile application for biometric based identification**
Ονοματεπώνυμο Φοιτητή	**Ειρήνη Σιάχου**
Πατρώνυμο	**Αθανάσιος**
Αριθμός Μητρώου	**ΜΠΣΠ/ 20047**
Επιβλέπων	**Ευάγγελος Σακκόπουλος, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Νοέμβριος 2024**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Ε. Σακκόπουλος Αναπληρωτής Καθηγητής	Ε. Αλέπης Καθηγητής	Κ. Χρυσαφιάδη Επίκουρη Καθηγήτρια

Σύνοψη

Η επαλήθευση ταυτότητας μέσω εφαρμογών έχει γίνει ένα από τα πιο διαδεδομένα μέσα διασφάλισης της ψηφιακής ασφάλειας σε διάφορους τομείς, όπως οι τραπεζικές συναλλαγές, οι κρατικές υπηρεσίες και οι πλατφόρμες κοινωνικής δικτύωσης. Οι εφαρμογές αυτές χρησιμοποιούν τεχνολογίες όπως βιομετρικούς ελέγχους (σάρωση προσώπου, δακτυλικών αποτυπωμάτων), επαλήθευση μέσω ταυτοποιητικών εγγράφων και πιστοποιητικών, καθώς και δύο παραγόντων αυθεντικοποίηση (2FA).

Η αξιοπιστία τους βασίζεται στη δυνατότητα διασταύρωσης δεδομένων και στον έλεγχο της αυθεντικότητας σε πραγματικό χρόνο, κάτι που καθιστά δύσκολη την πλαστογράφηση ή την παράκαμψη των μηχανισμών ασφαλείας. Ωστόσο, η επιτυχία τους εξαρτάται από την ευχρηστία και την προστασία των προσωπικών δεδομένων, με πολλές εφαρμογές να επενδύουν σε προηγμένα συστήματα κρυπτογράφησης και αποθήκευσης πληροφοριών.

Η παρούσα μεταπτυχιακή εργασία παρουσιάζει μια λύση η οποία έχει εφαρμογή σε κινητά τηλέφωνα Android και αφορά της μεθόδους επαλήθευσης ταυτότητας. Για το σκοπό αυτό χρησιμοποιήθηκε το σύνολο εργαλείων ανάπτυξης λογισμικού και βιβλιοθηκών (Software Development Kit) της FaceTec.

Η εφαρμογή αποτελεί ένα σύστημα αυθεντικοποίησης, το οποίο επαληθεύει μέσω μιας διαδικασίας αναγνώρισης προσώπου ή μέσω κάποιων κωδικών username και password την ταυτότητα του χρήστη. Η εφαρμογή συγκρίνει το πρόσωπο του χρήστη με τη φωτογραφία του διπλώματός του και ταυτόχρονα κάνει οπτική αναγνώριση του κειμένου του διπλώματός για να επαληθεύσει τα στοιχεία του. Όταν ο χρήστης ανοίξει ξανά την εφαρμογή, η αναγνώριση προσώπου επαληθεύει το 3D liveness και το συγκρίνει με το αποθηκευμένο 3D Face Map. Έτσι, συνδέεται στην εφαρμογή χωρίς τη χρήση κωδικών πρόσβασης.

Abstract

Identify verification through application has become one of the most widespread means of ensuring digital security across various fields such as banking transactions, government services and social media platforms. These applications use technologies like biometric checks (facial scanning, fingerprint scanning), verification via identity documents and certificates, as well as two-factor authentication (2FA).

Their reliability is based on the ability to cross-check data and authenticate in real-time, making it difficult to forge or bypass security mechanisms. However, their success depends on ease of use and the protection of personal data, with many applications investing in advanced encryption and information storage systems.

This master's thesis presents a solution applicable to Android mobile phones concerning identity verification methods. For this purpose, the FaceTec software development kit and libraries (Software Development Kit) were used.

The application acts as an authentication system, which verifies the user's identity through a facial recognition process or using username and password codes. The application compares the user's face with the photo of their license and simultaneously performs optical character recognition of the license's text to verify the user's details. When the user reopens the application, facial recognition verifies the 3D liveness and compares it with the stored 3D Face Map, allowing access to the application without using username/password.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1ο

1. ΕΙΣΑΓΩΓΗ

Η αναγνώριση προσώπου μέσω εφαρμογών Android έχει εξελιχθεί σημαντικά, προσφέροντας στους χρήστες και τις επιχειρήσεις έναν γρήγορο και ασφαλή τρόπο ταυτοποίησης. Με τη βοήθεια του FaceTec SDK, οι εφαρμογές Android μπορούν πλέον να εκτελούν αξιόπιστες διαδικασίες αναγνώρισης προσώπου σε πραγματικό χρόνο, αυξάνοντας τα επίπεδα ασφάλειας και ενισχύοντας την εμπειρία χρήστη. Το FaceTec SDK προσφέρει ολοκληρωμένα εργαλεία που επιτρέπουν στους προγραμματιστές να ενσωματώσουν προηγμένες δυνατότητες 3D αναγνώρισης προσώπου στις εφαρμογές τους, προστατεύοντας από τις παραδοσιακές απάτες, όπως η χρήση φωτογραφιών ή βίντεο. Η αναγνώριση προσώπου είναι ιδιαίτερα χρήσιμη σε εφαρμογές όπως τραπεζικές εφαρμογές, ψηφιακά πορτοφόλια και εφαρμογές κρατικών υπηρεσιών, όπου η ασφάλεια των δεδομένων είναι προτεραιότητα.

Στην παρούσα μεταπτυχιακή διατριβή θα παρουσιαστεί μια λύση 3D Liveness Authentication βασισμένη στο SDK που παρέχει η FaceTec. Αυτή η λύση έχει εφαρμογή σε κινητά τηλέφωνα τεχνολογίας Android και μπορεί να αποτελέσει βελτίωση στις υπάρχουσες μεθόδους επαλήθευσης ταυτότητας.

Στο επόμενο κεφάλαιο γίνεται αναφορά σε λύσεις που υπάρχουν διαθέσιμες σχετικά με το registration και authentication με 3D liveness. Στο 3ο κεφάλαιο, περιγράφονται οι απαιτήσεις, η ανάλυση και ο σχεδιασμός της εφαρμογής που υλοποιήθηκε. Στο 4ο κεφάλαιο, περιγράφεται η υλοποίηση και ορισμένα κρίσιμα στοιχεία του κώδικα της εφαρμογής. Στο 5ο κεφάλαιο, παρουσιάζεται η εφαρμογή με παραδείγματα. Στο 6ο κεφάλαιο, παρουσιάζονται τα συμπεράσματα που προέκυψαν από τη μελέτη αυτή, και ιδέες για περαιτέρω βελτίωση της εφαρμογής. Τέλος, ακολουθεί η παράθεση των βιβλιογραφικών πηγών που αξιοποιήθηκαν.

Κεφάλαιο 2ο

1. ΕΙΣΑΓΩΓΗ – ΑΝΑΣΚΟΠΗΣΗ ΠΕΔΙΟΥ

Η βιομετρία έχει εισέλθει δυναμικά στην καθημερινή χρήση των κινητών τηλεφώνων και των υπολογιστών, προσφέροντας έναν γρήγορο και ασφαλή τρόπο ταυτοποίησης των χρηστών. Οι πιο δημοφιλείς βιομετρικές μέθοδοι που χρησιμοποιούνται στις συσκευές αυτές περιλαμβάνουν την αναγνώριση δακτυλικών αποτυπωμάτων, την αναγνώριση προσώπου και, σε ορισμένες περιπτώσεις, την σάρωση ίριδας. Η τεχνολογία αυτή επιτρέπει στους χρήστες να ξεκλειδώνουν τις συσκευές τους, να έχουν πρόσβαση σε εφαρμογές ή να πραγματοποιούν αγορές χωρίς την ανάγκη για κωδικούς πρόσβασης, καθιστώντας τη διαδικασία πιο εύκολη και ασφαλή.

Στα smartphones, η βιομετρική αναγνώριση έχει γίνει αναπόσπαστο κομμάτι της εμπειρίας χρήστη. Για παράδειγμα, η αναγνώριση προσώπου, που χρησιμοποιείται από εταιρείες όπως η Apple με το Face ID, έχει προχωρήσει σε τέτοιο βαθμό που μπορεί να αναγνωρίσει τον χρήστη ακόμα και υπό κακές συνθήκες φωτισμού ή με αλλαγές στην εμφάνισή του. Παράλληλα, οι σαρωτές δακτυλικών αποτυπωμάτων που είναι ενσωματωμένοι στα κουμπιά ή τις οθόνες πολλών συσκευών προσφέρουν ταχύτητα και ακρίβεια, καθιστώντας τις βιομετρικές μεθόδους ιδιαίτερα δημοφιλείς.

Η ανίχνευση ζωντάνιας (liveness detection) είναι μια τεχνολογία που χρησιμοποιείται στα βιομετρικά συστήματα για να διασφαλίσει ότι το βιομετρικό δείγμα, όπως το πρόσωπο ή το αποτύπωμα, προέρχεται από έναν ζωντανό άνθρωπο και όχι από κάποια πλαστή αναπαράσταση, όπως φωτογραφίες ή καλούπια. Η τεχνολογία αυτή είναι κρίσιμη για την πρόληψη επιθέσεων πλαστοπροσωπίας και την ενίσχυση της ασφάλειας. Χρησιμοποιεί δύο κύριες μεθόδους: ενεργή ανίχνευση, που απαιτεί από το χρήστη να κάνει κάποια κίνηση, όπως να ανοιγοκλείσει τα μάτια, και παθητική ανίχνευση, που βασίζεται σε ανάλυση φυσιολογικών χαρακτηριστικών, όπως η ροή αίματος ή οι μικροκινήσεις των μυών.

Εταιρείες όπως η Oloid και η IDEMIA παρέχουν τέτοιες λύσεις, χρησιμοποιώντας τεχνολογίες τεχνητής νοημοσύνης και αισθητήρες βάθους για ανίχνευση ζωντάνιας σε συστήματα αναγνώρισης προσώπου και άλλες βιομετρικές μεθόδους. Άλλες εταιρείες είναι η FaceTec με λύσεις που συνδυάζουν αναγνώριση προσώπου και πολυεπίπεδους ελέγχους ζωντάνιας για ασφαλή ταυτοποίηση, η BioID που βασίζεται σε αλγορίθμους που ελέγχουν αν το πρόσωπο που παρουσιάζεται είναι πραγματικό και ζωντανό, αποτρέποντας επιθέσεις με φωτογραφίες ή βίντεο και πολλές άλλες που προσφέρουν εξελιγμένες τεχνολογίες για την προστασία της ψηφιακής ταυτότητας και την αποτροπή εξαπάτησης μέσω βιομετρικών δεδομένων.

2.1.1 Πάροχοι ανίχνευσης ζωντάνιας

Αρκετοί πάροχοι προσφέρουν λύσεις ανίχνευσης ζωντάνιας (liveness detection) για τη βιομετρική ταυτοποίηση. Αυτοί οι πάροχοι χρησιμοποιούν τεχνολογίες όπως τεχνητή νοημοσύνη και αναγνώριση βάθους για να ανιχνεύσουν εάν το βιομετρικό δείγμα προέρχεται από ζωντανό άτομο. Μερικοί από τους κορυφαίους παρόχους είναι:

FaceTec (ΗΠΑ)
Παρέχει προηγμένη αναγνώριση προσώπου και πολυεπίπεδη ανίχνευση ζωντάνιας, η οποία χρησιμοποιείται σε τομείς όπως οι τραπεζικές συναλλαγές και η επαλήθευση ταυτότητας.

BioID (Γερμανία)
Εξειδικεύεται στην παθητική ανίχνευση ζωντάνιας μέσω χαρακτηριστικών προσώπου, προσφέροντας λύσεις σε επιθέσεις με φωτογραφίες ή βίντεο.

IDEMIA (Γαλλία)
Προσφέρει λύσεις βιομετρικής αναγνώρισης με ανίχνευση ζωντάνιας σε ευρεία γκάμα εφαρμογών, όπως σε κυβερνητικά και εμπορικά περιβάλλοντα.

Innovatrics (Σλοβακία)
Παρέχει προηγμένη ανίχνευση ζωντάνιας με χρήση τόσο ενεργών όσο και παθητικών μεθόδων, ενσωματωμένη σε λύσεις ταυτοποίησης προσώπου.

NEC Corporation (Ιαπωνία)
Η NEC είναι γνωστή για τις λύσεις αναγνώρισης προσώπου της με ανίχνευση ζωντάνιας, που χρησιμοποιούνται σε αεροδρόμια και δημόσιες υπηρεσίες για την αποτροπή πλαστογραφιών και spoofing.

ZKTeco (Κίνα)
Η ZKTeco παρέχει βιομετρικές λύσεις που περιλαμβάνουν ανίχνευση ζωντάνιας σε αναγνώριση προσώπου και αποτυπωμάτων. Οι λύσεις της χρησιμοποιούνται ευρέως σε κυβερνητικούς οργανισμούς.

SenseTime (Κίνα)
Η SenseTime, μια κορυφαία εταιρεία τεχνητής νοημοσύνης, χρησιμοποιεί την αναγνώριση προσώπου για διάφορες εφαρμογές, συμπεριλαμβανομένης της ασφάλειας και της παρακολούθησης.

iProov (Ηνωμένο Βασίλειο)
Παρέχει παγκόσμια λύσεις για ασφαλή ψηφιακή ταυτοποίηση με χρήση της τεχνολογίας ανίχνευσης ζωντάνιας, ειδικά σε εφαρμογές χρηματοοικονομικών υπηρεσιών και ψηφιακών ταυτοτήτων.

Veridium (ΗΠΑ)
Η Veridium προσφέρει πολυτροπικές βιομετρικές λύσεις, όπως αναγνώριση προσώπου με ανίχνευση ζωντάνιας, για τη βελτίωση της ασφάλειας και την αποτροπή επιθέσεων πλαστοπροσωπίας.

Onfido (Ηνωμένο Βασίλειο)
Παρέχει προηγμένες λύσεις ανίχνευσης ζωντάνιας και ταυτοποίησης για χρηματοοικονομικές υπηρεσίες, ασφαλίσεις και άλλους τομείς που απαιτούν υψηλά επίπεδα ασφαλείας. Χρησιμοποιεί τεχνολογία τεχνητής νοημοσύνης για να ανιχνεύσει πλαστοπροσωπία σε πραγματικό χρόνο.

Daon (ΗΠΑ)
Εξειδικεύεται σε πολυτροπικές βιομετρικές λύσεις, συνδυάζοντας ανίχνευση ζωντάνιας και ταυτοποίηση προσώπου, φωνής και αποτυπωμάτων.Οι λύσεις της Daon χρησιμοποιούνται σε τράπεζεςκαι ασφαλιστικές υπηρεσίες.

Veridium (ΗΠΑ)
Η Veridium προσφέρει πολυτροπικές βιομετρικές λύσεις που περιλαμβάνουν ανίχνευση ζωντάνιας για αναγνώριση προσώπου και δακτυλικών αποτυπωμάτων, εστιάζοντας στην ασφάλεια ψηφιακών ταυτοτήτων και τραπεζικών εφαρμογών.

Gemalto (τώρα Thales Group) (Γαλλία)
Μετά την εξαγορά της από την Thales, η Gemalto συνεχίζει να προσφέρει λύσεις βιομετρικής αναγνώρισης και ανίχνευσης ζωντάνιας, με εφαρμογές σε κυβερνητικά και εμπορικά συστήματα.

Trueface (ΗΠΑ)
Η Trueface παρέχει λύσεις αναγνώρισης προσώπου με ανίχνευση ζωντάνιας, εστιάζοντας σε τομείς όπως η ασφάλεια και η παρακολούθηση, χρησιμοποιώντας αλγόριθμους τεχνητής νοημοσύνης.

Acuant (ΗΠΑ)
Η Acuant προσφέρει λύσεις ταυτοποίησης με ανίχνευση ζωντάνιας που χρησιμοποιούνται σε τομείς όπως οι χρηματοοικονομικές υπηρεσίες και η υγειονομική περίθαλψη, για την αποτροπή της απάτης και την επιβεβαίωση ταυτότητας.

Civica (Ηνωμένο Βασίλειο)
Ειδικεύεται στη διαχείριση ταυτότητας και προσφέρει λύσεις ανίχνευσης ζωντάνιας για δημόσιες υπηρεσίες και ιδιωτικές επιχειρήσεις, επικεντρώνοντας την προσοχή στην ασφάλεια και την προστασία δεδομένων.

Aware, Inc. (ΗΠΑ)
Η Aware παρέχει λύσεις βιομετρικής αναγνώρισης με δυνατότητες ανίχνευσης ζωντάνιας, χρησιμοποιούμενες σε ασφαλείς εφαρμογές ταυτοποίησης και κυβερνητικά συστήματα.

Mobius (ΗΠΑ)
Η Mobius ειδικεύεται σε βιομετρικές λύσεις που περιλαμβάνουν ανίχνευση ζωντάνιας για τον τομέα της ασφάλειας, χρησιμοποιώντας τεχνολογία αναγνώρισης προσώπου και αποτυπωμάτων.

SecuGen (ΗΠΑ)
Παρέχει λύσεις βιομετρικής ταυτοποίησης με ανίχνευση ζωντάνιας, επικεντρωμένες σε δακτυλικά αποτυπώματα και αναγνώριση προσώπου για εφαρμογές σε διάφορους τομείς.

2.1.2 Συστήματα αναγνώρισης προσώπου

IDEMIA

Το *MorphoFace* είναι ένα από τα πιο προηγμένα συστήματα αναγνώρισης προσώπου της IDEMIA. Προσφέρει υψηλής ακρίβειας αναγνώριση, ειδικά σχεδιασμένο για χρήση σε συστήματα ασφαλείας και ελέγχου ταυτότητας. Το MorphoFace ενσωματώνει αλγόριθμους τεχνητής νοημοσύνης (AI) και μηχανικής μάθησης για να επεξεργάζεται με ακρίβεια τα χαρακτηριστικά του προσώπου, ακόμη και σε πολυσύχναστα περιβάλλοντα. Χρησιμοποιείται σε συστήματα ασφαλείας αεροδρομίων, κρατικές υπηρεσίες και τράπεζες, προσφέροντας γρήγορη ταυτοποίηση και έλεγχο πρόσβασης. Χρησιμοποιείται επίσης σε λύσεις *smart city* για έλεγχο πρόσβασης σε δημόσιους χώρους.

Το *MorphoWave* είναι μια καινοτόμος συσκευή για βιομετρική αναγνώριση που συνδυάζει πολλαπλά βιομετρικά χαρακτηριστικά, όπως αναγνώριση προσώπου και αποτύπωμα παλάμης. Το σύστημα σαρώνει ένα χέρι ή το πρόσωπο σε πραγματικό χρόνο, και είναι σχεδιασμένο για γρήγορη αναγνώριση σε περιβάλλοντα με υψηλή κυκλοφορία. Χρησιμοποιείται σε σημεία ασφαλείας αεροδρομίων και δημόσιους χώρους όπου απαιτείται γρήγορη, χωρίς επαφή ταυτοποίηση.

INNOVATRICS

Το *Digital Onboarding Toolkit* της Innovatrics είναι ένα σύστημα που διευκολύνει την ταυτοποίηση προσώπου για εγγραφή χρηστών εξ αποστάσεως, ιδιαίτερα χρήσιμο για τράπεζες και χρηματοπιστωτικά ιδρύματα. Περιλαμβάνει τεχνολογία αναγνώρισης προσώπου και 3D *liveness detection* για να διασφαλίζει ότι ο χρήστης που πραγματοποιεί την εγγραφή είναι πραγματικό άτομο. Χρησιμοποιείται σε Εφαρμογές *Know Your Customer* (KYC), τραπεζικές εγγραφές και άλλες υπηρεσίες που απαιτούν από απόσταση εγγραφή χρηστών με υψηλή ασφάλεια. Χρησιμοποιούνται σε συστήματα επιτήρησης και ασφάλειας σε πόλεις, κυβερνητικά κτίρια, αεροδρόμια, και καταστήματα λιανικής.

Το ABIS είναι μια πλήρης πλατφόρμα ταυτοποίησης που συνδυάζει πολλαπλές βιομετρικές λύσεις, όπως αναγνώριση προσώπου, δακτυλικών αποτυπωμάτων και ίριδας. Η πλατφόρμα υποστηρίζει μεγάλες βάσεις δεδομένων για διασταύρωση βιομετρικών πληροφοριών. Χρησιμοποιείται κυρίως σε κυβερνητικά προγράμματα για την ταυτοποίηση πολιτών και την επιβολή του νόμου.

NEC Corporation

Η *NeoFace Suite* περιλαμβάνει λύσεις όπως το *NeoFace Watch* (αναγνώριση προσώπου σε πραγματικό χρόνο για επιτήρηση), το *NeoFace Reveal* (χρησιμοποιείται από τις αρχές για την ταυτοποίηση υπόπτων από εικόνες ή βίντεο) και το *NeoFace Access Control* (για ασφαλή πρόσβαση σε περιορισμένες περιοχές). Αυτά τα συστήματα έχουν εγκατασταθεί σε πάνω από 70 χώρες και χρησιμοποιούνται σε εφαρμογές όπως η αστυνόμευση, ο έλεγχος συνόρων και η ασφάλεια επιχειρήσεων.

Το *NeoFace Cloud,* μια λύση αναγνώρισης προσώπου βασισμένη σε cloud, που επιτρέπει την κλιμάκωση και την ευκολία ενσωμάτωσης. Υποστηρίζει πολλές συσκευές, συμπεριλαμβανομένων των smartphones και tablets, καθιστώντας το κατάλληλο για τομείς όπως οι χρηματοοικονομικές υπηρεσίες και οι εξωτερικοί χώροι εργασίας.

Η NEC έχει αναπτύξει επίσης ένα πολυτροπικό σύστημα που συνδυάζει την αναγνώριση προσώπου με την αναγνώριση ίριδας, προσφέροντας υψηλά επίπεδα ακρίβειας. Αυτό το σύστημα, σχεδιασμένο για περιβάλλοντα που απαιτούν αυστηρή ταυτοποίηση, προσφέρει ανέπαφη ταυτοποίηση ακόμη και σε προκλήσεις όπως η χρήση μάσκας ή γαντιών. Χρησιμοποιείται σε χώρους υψηλής ασφάλειας, όπως κυβερνητικές εγκαταστάσεις, εργοστάσια και νοσοκομεία.

2.1.3 Πληροφορίες για την εταιρεία FaceTec

Η *FaceTec* είναι μια καινοτόμος εταιρεία που παρέχει λύσεις βιομετρικής αναγνώρισης μέσω 3D τεχνολογίας. Ιδρύθηκε το 2013 και έχει την έδρα της στο Λας Βέγκας, Νεβάδα. Η κύρια εξειδίκευσή της αφορά τη διαδικασία ταυτοποίησης και επαλήθευσης ταυτότητας μέσω της αναγνώρισης προσώπου, συνδυάζοντας βίντεο και 3D ανίχνευση προσώπου για τον έλεγχο ταυτοτήτων και την ανίχνευση πλαστογραφίας. Η FaceTec χρησιμοποιεί μια σειρά από καινοτόμες τεχνολογίες για να παρέχει λύσεις βιομετρικής αναγνώρισης και ταυτοποίησης μέσω προσώπου. Ακολουθούν ορισμένες από τις βασικές τεχνολογίες τους.

3D Liveness Detection: Αυτή η τεχνολογία επιτρέπει την ανίχνευση αν το πρόσωπο που εξετάζεται είναι ζωντανό και όχι πλαστό (π.χ. μέσω φωτογραφίας ή μάσκας). Η FaceTec χρησιμοποιεί τρισδιάστατη ανίχνευση βάθους και χαρακτηριστικά του δέρματος για την επιβεβαίωση της παρουσίας του χρήστη.

3D Face Matching: Η πλατφόρμα της FaceTec εκμεταλλεύεται την τρισδιάστατη απεικόνιση του προσώπου, επιτρέποντας την ακριβή σύγκριση μεταξύ της εικόνας του χρήστη και μιας αποθηκευμένης φωτογραφίας. Αυτό διασφαλίζει υψηλή ακρίβεια και μειώνει την πιθανότητα ψευδών θετικών αποτελεσμάτων.

AI και Machine Learning: Η FaceTec ενσωματώνει προηγμένους αλγόριθμους τεχνητής νοημοσύνης και μηχανικής μάθησης, οι οποίοι επιτρέπουν τη βελτιωμένη ανάλυση προσώπου και την ταυτοποίηση, ακόμη και σε δύσκολες συνθήκες φωτισμού ή με μεταβολές στην εμφάνιση του χρήστη.

Cross-Platform Integration: Η τεχνολογία της FaceTec είναι συμβατή με πολλές πλατφόρμες, περιλαμβάνοντας mobile και web εφαρμογές. Αυτό επιτρέπει την ευκολότερη υιοθέτηση της τεχνολογίας από επιχειρήσεις σε διάφορους τομείς.

Age Estimation: Μια από τις πιο πρόσφατες δυνατότητες που πρόσθεσε η FaceTec είναι η εκτίμηση της ηλικίας του χρήστη, βασισμένη στη μορφολογία του προσώπου, με στόχο την ενίσχυση της ταυτοποίησης και της ασφάλειας.

2.1.4 Συνεργασίες εταιρειών με τη FaceTec

Η FaceTec συνεργάζεται με πολλές εταιρείες σε διάφορους τομείς, χρησιμοποιώντας την τεχνολογία βιομετρικής αναγνώρισης προσώπου και ανίχνευσης ζωντάνιας (liveness detection). Παρακάτω, παρουσιάζονται ορισμένες από τις πιο γνωστές εταιρείες που χρησιμοποιούν τις λύσεις της FaceTec.

Onfido: Μια πλατφόρμα ψηφιακής επαλήθευσης ταυτότητας που έχει ενσωματώσει την τεχνολογία της FaceTec στο Face Authenticate service, συνδυάζοντας την ανίχνευση ζωντάνιας με την επαλήθευση ταυτότητας.

Veritran: Η Veritran συνεργάζεται με την FaceTec για να ενσωματώσει τη βιομετρική τεχνολογία 3D στην ασφάλεια των ψηφιακών χρηματοοικονομικών υπηρεσιών.

ZenGo: Ένα πορτοφόλι κρυπτονομισμάτων που χρησιμοποιεί τις βιομετρικές λύσεις της FaceTec για να ασφαλίσει την πρόσβαση και την αποκατάσταση λογαριασμών.

Gulf Data International (gDi): Αυτή η εταιρεία έχει εφαρμόσει την τεχνολογία της FaceTec για λύσεις απομακρυσμένης επαλήθευσης πελατών, συνεργαζόμενη με την μεγαλύτερη τράπεζα στα Ηνωμένα Αραβικά Εμιράτα.

Humanode: Αυτή η πλατφόρμα χρησιμοποιεί την τεχνολογία της FaceTec για την ασφάλεια της αποσυνδεδεμένης πλατφόρμας της μέσω βιομετρικής επαλήθευσης.

Κεφάλαιο 3ο

1. ΣΥΛΛΗΨΗ ΑΝΑΓΚΩΝ

Σε αυτό το κεφάλαιο θα γίνει η καταγραφή και η ανάλυση των απαιτήσεων του συστήματος μας. Θα γίνει δηλαδή η περιγραφή των διάφορων λειτουργιών που θα εκτελεί το σύστημά μας με βάση τα παρακάτω:

- Ανάλυση Αναγκών (Need Analysis)
- Ανάλυση Χρηστών (User Analysis)
- Ανάλυση Εργασιών (Task Analysis)

2. ΑΝΑΛΥΣΗ ΑΝΑΓΚΩΝ

Το σύστημα που θα υλοποιήσουμε είναι μια εφαρμογή android που θα εκτελεί κάποιες εργασίες. Για το λόγο αυτό πρέπει να ορίσουμε τις απαιτήσεις αλλά και τον τρόπο με τον οποίο θα τις υλοποιήσουμε. Η εφαρμογή θα υλοποιηθεί σε περιβάλλον Visual Code με τη χρήσητ ης τεχνολογίας Flutter. Γίνεται διασύνδεση με το sdk της FaceTec μέσα από το περιβάλλον του Android Studio όπου γίνονται όποιες αλλαγές χρειάζονται για να εξυπηρετηθεί το σύστημά μας. Επίσης χρησιμοποιούμε την Firebase Database και το Storage της για να αποθηκεύουμε τα δεδομένα μας και να μπορούμε να τα αξιοποιήσουμε για τις λειτουργίες της εφαρμογής.

3. ΑΝΑΛΥΣΗ ΧΡΗΣΤΩΝ

Στην εφαρμογή που υλοποιήθηκε, ο χρήστης θα έχει τη δυνατότητα να εκτελέσει κάποιες λειτουργίες.

Αυτές οι λειτουργίες είναι οι παρακάτω:

- Εγγραφή στην εφαρμογή
- Αντιστοίχιση διπλώματος με φωτογραφία
- Προβολή και Αποθήκευση Φωτογραφιών
- Σύνδεση στην εφαρμογή με username/password
- Σύνδεση στην εφαρμογή με Face Authentication
- Προβολή Πληροφοριών/Φωτογραφιών του χρήστη

4. ΑΝΑΛΥΣΗ ΕΡΓΑΣΙΩΝ

Στο σημείο αυτό θα αναλύσουμε τα τμήματα της εφαρμογής ώστε να γίνει πιο εύκολα κατανοητή η υλοποίησή της και οι εργασίες που εκτελούνται.

Αρχικά δημιουργήθηκε η βάση δεδομένων (χρησιμοποιήθηκε η Firebase Database) στην οποία αποθκεύονται τα δεδομένα της εφαρμογής μας. Η δομή της βάσης θα καθορίζει τον τρόπο με τον οποίο αποθηκεύονται τα δεδομένα αλλά και πως θα ανακαλούται κάθε φορά που η εφαρμογή εκτελεί τις εργασίες.

Στη συνέχεια δημιουργούμε τα widgets με την τεχνολογία Flutter, τα οποία θα αποτελέσουν τα βασικά σημεία της εφαρμογής και θα αποτελέσουν τη γέφυρα σύνδεσης με το sdk της FaceTec.

Τέλος, ακολουθεί η διασύνδεση της βάσης δεδομένων με τα widgets της εφαρμογής. Με την χρήση της εφαρμογής από τον χρήστη, θα γίνεται η σύνδεση της εφαρμογής με τη βάση δεδομένων για να καταχωρούνται ή να ανακτούνται τα δεδομένα ανάλογα με την εργασία που εκτελείται.

5. ΣΧΕΔΙΑΣΜΟΣ

Στην ενότητα αυτού του κεφαλαίου θα παρουσιαστεί η λειτουργικότητα του συστήματός μας μέσα από την καταγραφή των Περιπτώσεων Χρήσης.

3.5.1 Εγγραγή – Sign Up

Τίτλος	Εγγραφή – Registration
ID	UC-01
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί εγγραφή στην εφαρμογή
Προϋπόθεση	Ο χρήστης πρέπει να έχει email
Αποτέλεσμα	Ο χρήστης έκανε εγγραφή στην εφαρμογή
Βασικό μονοπάτι	
1.	Ο χρήστης ανοίγει την εφαρμογή
2.	Ο χρήστης επιλέγει από το μενού την επιλογή «Sign Up»
3.	Ο χρήστης συμπληρώνει το email και το password
4.	Αν συμπληρωθούν σωστά τα πεδία, η εγγραφή είναι επιτυχής
5.	Η περίπτωση χρήσης τελειώνει
Εναλλακτικό μονοπάτι (Α)	

1.	Αν ο χρήστης δεν συμπληρώσει σωστά τα πεδία email/password
2.	Εμφανίζεται μήνυμα που αφορά τη σωστή συμπλήρωση των πεδίων
3.	Αν γίνει ξανά λάθος, εμφανίζεατι ξανά μήνυμα για τη σωστή συμπλήρωσή τους

Εναλλακτικό μονοπάτι (Β)	
1.	Αν ο χρήστης κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.1: Εγγραφή – Sign Up

3.5.2 Αντιστοίχιση διπλώματος με φωτογραφία – Photo Id Match

Τίτλος	Αντιστοίχιση διπλώματος με φωτογραφία – Photo Id Match
ID	UC-02
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί αντιστοίχιση ταυτότητας με φωτογραφία
Προϋπόθεση	Ο χρήστης θα πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή ή σύνδεση στην εφαρμογή
Αποτέλεσμα	Ο χρήστης θα έχει πραγματοποιήσει αντιστοίχιση διπλώματος με φωτογραφία
Βασικό μονοπάτι	
1.	Ο χρήστης επιλέγει το button "Photo Id Match"
2.	Πραγματοποιείται 3D FaceScan
3.	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου 3D facescan στο FaceTec Server SDK
4.	Επιβεβαιώνεται το liveness
5.	Πραγματοποιείται το Front Id Scan
6.	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου Front ID Scan στο FaceTec Server SDK
7.	Πραγματοποιείται σάρωση του Front Id Scan
8.	Πραγματοποιείται έλεγχος ότι το 3d face scan ταιριάζει με το αναγνωριστικό (δίπλωμα)
9.	Πραγματοποιείται το Back Id Scan
10.	Πραγματοποιείται μεταφόρτωση κρυπτογραφημένου Back ID Scan στο FaceTec Server SDK
11.	Ο χρήστης πραγματοποιεί έλεγχο στοιχείων του διπλώματος και επιλέγει επιβεβαίωση
12.	Πραγματοποιείται μεταφόρτωση των επιβεβαιωμένων στοιχείων στο FaceTec Server SDK και στη Firebase

13.	Πραγματοποιείται ενημέρωση ότι ολοκληρώθηκε ο έλεγχος του διπλώματος
14.	Η περίπτωση χρήσης τελεινώνει

Εναλλακτικό μονοπάτι (Α)	
1.	Αν δεν είναι ευδιάκριτο το 3D FaceScan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το 3D FaceScan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το 3D FaceScan
Εναλλακτικό μονοπάτι (Β)	
1.	Αν δεν είναι ευδιάκριτο το Front ID Scan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το Front ID Scan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το Front ID Scan
Εναλλακτικό μονοπάτι (Γ)	
1.	Αν δεν είναι ευδιάκριτο το Back ID Scan
2.	Εμφάνιση μηνύματος ότι πρέπει να πραγματοποιηθεί εκ νέου το Back ID Scan
3.	Υπάρχει περίπτωση επανάληψης μέχρι να είναι ευδιάκριτο το Back ID Scan
Εναλλακτικό μονοπάτι (Δ)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.2: Αντιστοίχιση διπλώματος με φωτογραφία – Photo ID Match

3.5.3 View Photos

Τίτλος	View Photos
ID	UC-03
Παράγοντας	Χρήστης

Περιγραφή	Ο χρήστης βλέπει τις φωτογραφίες που έχουν αποθηκευτεί
Προϋπόθεση	Ο χρήστης πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή ή σύνδεση στην εφαρμογή
Αποτέλεσμα	Ο χρήστης βλέπει τις φωτογραφίες που έχουν αποθηκευτεί στο Storage της Firebase
Βασικό μονοπάτι	
1.	Ο χρήστης επιλέγει το button “View Photos”
2.	Ο χρήστης βλέπει τις φωτογραφίες του
3.	Η περίπτωση χρήσης τελειώνει
Εναλλακτικό μονοπάτι (Α)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.3: View Photos

3.5.4 Σύνδεση – Login

Τίτλος	Σύνδεση – Login
ID	UC-04
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί σύνδεση στην εφαρμογή
Προϋπόθεση	Ο χρήστης πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή στην εφαρμογή
Αποτέλεσμα	Ο χρήστης συνδέθηκε επιτυχώς στην εφαρμογή
Βασικό μονοπάτι	
1.	Ο χρήστης επιθυμεί να χρησιμοποιήσει την εφαρμογή
2.	Ο χρήστης ανοίγει την εφαρμογή
3.	Ο χρήστης επιλέγει το button “Login” από το μενού
4.	Ο χρήστης συμπληρώνει τα πεδία email/password
5.	Αν τα πεδία email/password συμπληρωθούν σωστά συνδέεται επιτυχώς στην εφαρμογή
6.	Η περίπτωση χρήσης τελειώνει
Εναλλακτικό μονοπάτι (Α)	

1.	Αν ο χρήστης δεν συμπληρώσει σωστά τα πεδία email/password
2.	Εμφανίζεται μήνυμα συμπλήρωσης ή διόρθωσης των πεδίων
3.	Μπορεί να υπάρξει επανάληψη μέχρι τα πεδία να συμπληρωθούν σωστά
Εναλλακτικό μονοπάτι (Β)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.4: Σύνδεση - Login

3.5.5 Σύνδεση – Face Authentication

Τίτλος	Σύνδεση – Face Authentication
ID	UC-05
Παράγοντας	Χρήστης
Περιγραφή	Ο χρήστης πραγματοποιεί σύνδεση στην εφαρμογή με επαλ
Προϋπόθεση	Ο χρήστης πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή στην εφαρμογή
Αποτέλεσμα	Ο χρήστης συνδέθηκε επιτυχώς στην εφαρμογή
Βασικό μονοπάτι	
1.	Ο χρήστης επιθυμεί να χρησιμοποιήσει την εφαρμογή
2.	Ο χρήστης ανοίγει την εφαρμογή
3.	Ο χρήστης επιλέγει το button “Login” από το μενού
4.	Ο χρήστης συμπληρώνει τα πεδία email/password
5.	Αν τα πεδία email/password συμπληρωθούν σωστά συνδέεται επιτυχώς στην εφαρμογή
6.	Η περίπτωση χρήσης τελειώνει
Εναλλακτικό μονοπάτι (Α)	
1.	Αν ο χρήστης δεν συμπληρώσει σωστά τα πεδία email/password
2.	Εμφανίζεται μήνυμα συμπλήρωσης ή διόρθωσης των πεδίων
3.	Μπορεί να υπάρξει επανάληψη μέχρι τα πεδία να συμπληρωθούν σωστά
Εναλλακτικό μονοπάτι (Β)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή

2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.5: Σύνδεση – Face Authentication

3.5.6 User Information

Τίτλος	User Information
ID	UC-06
Παράγοντας	Χρήστης
Περιγραφή	Εμφάνιση πληροφοριών του χρήστη
Προϋπόθεση	Ο χρήστης πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή στην εφαρμογή
Αποτέλεσμα	Ο χρήστης βλέπει της πληροφορίες του διπλώματος του που έχουν καταχωρηθεί στη βάση δεδομένων
Βασικό μονοπάτι	
1.	Ο χρήστης συνδέεται στην εφαρμογή
2.	Ο χρήστης βλέπει τις πληροφορίες του διπλώματός του
3.	Η περίπτωση χρήσης τελειώνει
Εναλλακτικό μονοπάτι (Α)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.6: User Information

3.5.7 User Photos

Τίτλος	User Photos
ID	UC-07
Παράγοντας	Χρήστης

Περιγραφή	Εμφάνιση φωτογραφιών του χρήστη
Προϋπόθεση	Ο χρήστης πρέπει να έχει πραγματοποιήσει επιτυχώς εγγραφή στην εφαρμογή και να επιλέξει το button “View Photos”
Αποτέλεσμα	Ο χρήστης βλέπει τις φωτογραφίες του
Βασικό μονοπάτι	
1.	Ο χρήστης συνδέεται στην εφαρμογή
2.	Ο χρήστης βλέπει τις πληροφορίες του διπλώματός του
3.	Ο χρήστης επιλέγει το button “View Photos”
4.	Ο χρήστης βλέπει τις φωτογραφίες που έχουν αποθηκευτεί στη βάση
5.	Η περίπτωση χρήσης τελειώνει
Εναλλακτικό μονοπάτι (Α)	
1.	Αν ο χρήστης επιλέξει να κλείσει την εφαρμογή
2.	Η περίπτωση χρήσης τελειώνει

Πίνακας 5.5: User Photos

Κεφάλαιο 4ο

1. ΥΛΟΠΟΙΗΣΗ – ΚΩΔΙΚΑΣ ΕΦΑΡΜΟΓΗΣ

Σε αυτό το κεφάλαιο θα παρουσιάσουμε αναλυτικά την υλοποίηση της εφαρμογής αλλά και κάποια κομμάτια κώδικα στα οποία φαίνονται οι βασικές λειτουργίες της εφαρμογής.

Η εφαρμογή δημιουργήθηκε με την τεχνολογία Flutter, ένα open-source UI kit ανάπτυξης λογισμικού εφαρμογών πολλαπλών πλατφορμών. Για να επικοινωνήσει η εφαρμογή με το sdk της Facetec, συμπεριλαμβάνουμε στο κώδικα μια κλάση που περιέχει κάποιες μεταβλητές. Οι μεταβλητές αυτές αρχικοποιούνται με τις τιμές που μας δίνονται απο την εταιρεία, όταν δημιουργούμε λογαριασμό για να χρησιμοποιήσουμε το sdk της. (Εικόνα 1)

Για την αποθήκευση των δεδομένων του χρήστη, χρησιμοποιήθηκε η βάση Firebase Realtime. Τα δεδομένα στη Realtime database αποθηκεύονται με τη μορφή JSON. Όταν προστίθονται δεδομένα, τότε δημιουργείται ένας κόμβος στην υπάρχουσα δομή JSON με ένα σχετικό κλειδί. Επίσης, χρησιμοποιήθηκε το Firebase Storage για να αποθηκευτούν αλλά και να μπορούν να ανακτηθούν οι φωτογραφίες του χρήστη. (Εικόνα 2, Εικόνα 3)

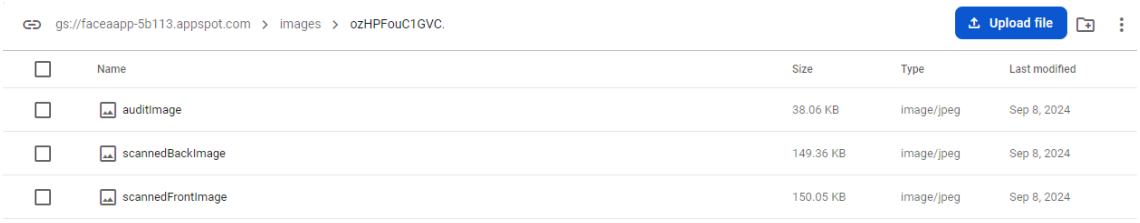
```
class FaceTecConfig {
  // Available at https://dev.facetec.com/account
  static const String deviceKeyIdentifier = "dOypJpyMQ4MHAWdrCe5BnPOYrwTGQ7cK";

  static String BaseURL = "https://api.facetec.com/api/v3.1/biometrics";

  // The FaceScan Encryption Key you define for your application.
  // Please see https://dev.facetec.com/facemap-encryption-keys for more information.
  static const String publicFaceScanEncryptionKey = '''
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5PxZ3DLj+zP6T6HFgzzk
M77LdzP3fojBoLasw7EfzvLMnJNUlyRb5m8e5QyyJxI+wRjsALHvFgLzGwxM8ehz
DqqBZed+f4w33GgQXFZOS4AOvyPbALgCYoLehigLAbbCNTkeY5RDcmmSI/sbp+s6
mAiAKKvCdIqe17bltZ/rfEoL3gPKEfLXeN549LTj3XBp0hvG4loQ6eC1E1tRzSkf
GJD4GIVvR+j12gXAaftj3ahfYxioBH7F7HQxzmWkwDyn3bqU54eaiB7f0ftsPpWM
ceUaqkL2DZUvgN0efEJjnWy5y1/Gkq5GGWCROI9XG/SwXJ30BbVUehTbVcD70+ZF
8QIDAQAB
-----END PUBLIC KEY-----''';
}
```

Εικόνα 1: FaceTec Config

Εικόνα 2: Δεδομένα της Firebase Realtime database



Εικόνα 3: Δεδομένα του Firebase Storage

4.1.1 Εγγραφή χρήστη (Sign Up)

```
void createUser(BuildContext context, currentEmail, String currentFullName, String currentPassword, String registermsgController) async
  try {
    final ref = FirebaseDatabase.instance.ref('Users');
    FirebaseAuth myAuth = FirebaseAuth.instance;
    UserCredential userCredential = await myAuth.createUserWithEmailAndPassword(
    email: currentEmail,
    password: currentPassword,
  );

    // User successfully registered
    User? user = userCredential.user;

    if (user != null) {
      await ref.child(user.uid).set({
          'email'   : currentEmail,
          'fullname': currentFullName,
          'password': currentPassword,
      });
      navigateToFaceTec(context, user.uid);
    }else {
      ScaffoldMessenger.of(context).showSnackBar(
      const SnackBar(
        content: Text('Something is wrong'),
      ), // SnackBar
    );
    }

  } on FirebaseAuthException catch (e) {
    // Handle error
    if (e.code == 'weak-password') {
      ScaffoldMessenger.of(context).showSnackBar(···
    } else if (e.code == 'email-already-in-use') {
      ScaffoldMessenger.of(context).showSnackBar(
      const SnackBar(
        content: Text('The account already exists for that email.'),
      ), // SnackBar
    );
    } else {
      ScaffoldMessenger.of(context).showSnackBar(
        SnackBar(
          content: Text('Error: ${e.code}'),
        ), // SnackBar
      );
    }
  } catch (e) {
    // Handle any other errors
    ScaffoldMessenger.of(context).showSnackBar(
      SnackBar(
        content: Text('Error: $e'),
      ), // SnackBar
    );
  }
}
```

Εικόνα 4: Υλοποίηση της εγγραφής του χρήστη

4.1.2 Photo ID Match

```
Future<void> startLiveness() async {

  try {
    String data = await faceTecSDK.invokeMethod("startLiveness", {
      "deviceKeyIdentifier"          : FaceTecConfig.deviceKeyIdentifier,
      "publicFaceScanEncryptionKey"  : FaceTecConfig.publicFaceScanEncryptionKey,
      "latestExternalDatabaseRefID"  : externalDatabaseRefID,
      "BaseURL"                      : FaceTecConfig.BaseURL
    });

    setState(() {
      isLivenessEnabled = false;
      isLoading = true;
    });
```

Εικόνα 5: Κλήση της διαδικασίας Photo ID Match

4.1.3 Αποτελέσματα του Photo ID Match (OCR Results)

```
Map<String, dynamic>    results    = jsonDecode(data),
                        ocrResults = jsonDecode(results['ocrResults']);

if (results["success"]) {
  List<dynamic>  groups       = ocrResults['ocrResults']['userConfirmed']['groups'],
                 info         = groups[0]['fields'],
                 photoDetails = groups[1]['fields'];

  String lastName  = info[0]['value'];
  String firstName = info[1]['value'];

  DateFormat dateFormat      = DateFormat("dd.MM.yyyy");
  DateFormat outputFormat    = DateFormat('dd/MM/yyyy');

  String dateOfBirthString   = info[2]['value'];
  DateTime dateTime          = dateFormat.parse(dateOfBirthString);
  String dateOfBirth         = outputFormat.format(dateTime);

  String idNumber   = photoDetails[0]['value'];
  String idNumber2  = photoDetails[1]['value'];

  String issueDateString  = photoDetails[2]['value'];
  DateTime issueDateTime  = dateFormat.parse(issueDateString);
  String issueDate        = outputFormat.format(issueDateTime);

  String expireDateString  = photoDetails[3]['value'];
  DateTime expireDateTime  = dateFormat.parse(expireDateString);
  String expireDate        = outputFormat.format(expireDateTime);
```

Εικόνα 6: Αποτελέσματα του Photo ID Match

4.1.4 Εισαγωγή δεδομένων στη Realtime Database

```
final ref = FirebaseDatabase.instance.ref('Users');
final snapshot = await ref.child(widget.userid!).get();

if (snapshot.exists) {
    email = snapshot.child('email').value.toString();
}
 await ref.child(widget.userid ?? '').update({
      'lastName'              : lastName,
      'firstName'             : firstName,
      'dateOfBirth'           : dateOfBirth,
      'issueDate'             : issueDate,
      'expireDate'            : expireDate,
      'idNumber'              : idNumber,
      'idNumber2'             : idNumber2,
      'idScan'                : results["idScan"],
      'idScanFrontImage'      : results["idScanFrontImage"],
      'idScanBackImage'       : results["idScanBackImage"],
      'scanResultBlob'        : results["scanResultBlob"],
      'externalDatabaseRefID' : results["externalDatabaseRefID"],
      'auditImage'            : results["auditImage"]
  });

  latestExternalDatabaseRefID = results["externalDatabaseRefID"];

  Uint8List auditImagebytes       = base64.decode(results["auditImage"]);
  Uint8List idScanFrontImagebytes = base64.decode(results["idScanFrontImage"]);
  Uint8List idScanBackImagebytes  = base64.decode(results["idScanBackImage"]);
  Uint8List scanResultBlob        = base64.decode(results["scanResultBlob"]);
```

Εικόνα 7: Αποθήκευση των δεδομένων στη Realtime Database

4.1.5 Αποθήκευση φωτογραφιών-latestExternalRefID στο Storage

```
Future<void> uploadImagesToFirebaseStorage(Uint8List auditImagebytes, Uint8List idScanFrontImagebytes, Uint8List idScanBackImagebytes, Uint8List scanResultBlob, String latestEx
try {
  // Create a reference to the Firebase Storage path
  final imageStorageRef = FirebaseStorage.instance.ref().child('images');
  final latestExternalRefIdStorageRedf = FirebaseStorage.instance.ref().child('latestExternalRefId');

  final storageRefscannedImage      = imageStorageRef.child('$userkey/auditImage');
  final storageRefscannedFrontImage = imageStorageRef.child('$userkey/scannedFrontImage');
  final storageRefscannedBackImage  = imageStorageRef.child('$userkey/scannedBackImage');

  final latestExternalRefId = latestExternalRefIdStorageRedf.child('latestExternalDatabaseRefID');


  // Upload the file to Firebase Storage
  await storageRefscannedImage.putData(auditImagebytes, SettableMetadata(contentType: 'image/jpeg'));
  await storageRefscannedFrontImage.putData(idScanFrontImagebytes,  SettableMetadata(contentType: 'image/jpeg'));
  await storageRefscannedBackImage.putData(idScanBackImagebytes,  SettableMetadata(contentType: 'image/jpeg'));
  await latestExternalRefId.putString(latestExternalDatabaseRefID);


} catch (e) {
  ScaffoldMessenger.of(context).showSnackBar(
  SnackBar(
    content: Text('Error uploading file: $e'),
  )); // SnackBar
}
```

Εικόνα 8: Αποθήκευση φωτογραφιών/latestExternalRefID στο Storage

4.1.6 Login χρήστη

```
doesUserExist(String currentEmail,  String currentPassword) async{
  try {
    UserCredential userCredential = await FirebaseAuth.instance.signInWithEmailAndPassword(
      email: currentEmail,
      password: currentPassword
    );

    String uid = FirebaseAuth.instance.currentUser?.uid ?? '';
    // Reference to the user's data in the Realtime Database
    DatabaseReference userRef = FirebaseDatabase.instance.ref().child('Users/$uid');
    // Fetch the data once
    DatabaseEvent event = await userRef.once();
     // Check if the snapshot exists and contains data
    if (event.snapshot.exists) {
      Map<dynamic, dynamic>? userData = event.snapshot.value as Map<dynamic, dynamic>;

      navigateToPersonalInfo(context, userData, uid);

    } else {
      ScaffoldMessenger.of(context).showSnackBar(
        const SnackBar(
        content: Text('User not found.'),
        )); // SnackBar
    }

    } on FirebaseAuthException catch (e) {
      if (e.code == 'user-not-found') {
        ScaffoldMessenger.of(context).showSnackBar(
          const SnackBar(
          content: Text('No user found for that email.'),
        )); // SnackBar
      } else if (e.code == 'wrong-password') {
          ScaffoldMessenger.of(context).showSnackBar(
          const SnackBar(
          content: Text('Wrong password provided for that user.'),
        )); // SnackBar
      } else if (e.code == 'invalid-credential'){
        ScaffoldMessenger.of(context).showSnackBar(
          const SnackBar(
          content: Text('Invalid credentials.'),
        )); // SnackBar
      } else  {
          ScaffoldMessenger.of(context).showSnackBar(
          const SnackBar(
          content: Text('Something wrong happened.'),
        )); // SnackBar
      }
  }
}
```

Εικόνα 9: Υλοποίηση Login του χρήστη

4.1.7 Face Authentication χρήστη

```
Future<void> authenticate() async {

    if (latestExternalDatabaseRefID == '') {
      ScaffoldMessenger.of(context).showSnackBar(
        const SnackBar(content: Text('No registered user found.')),
      );
      return;
    }
    String data = await faceTecSDK.invokeMethod("authenticate", {
        "deviceKeyIdentifier"          : FaceTecConfig.deviceKeyIdentifier,
        "publicFaceScanEncryptionKey"  : FaceTecConfig.publicFaceScanEncryptionKey,
        "latestExternalDatabaseRefID"  : latestExternalDatabaseRefID,
        "BaseURL"                      : FaceTecConfig.BaseURL
     });

    setState(() {
      isLivenessEnabled = false;
      isLoading = true;
    });
```

Εικόνα 10: Υλοποίηση της διαδικασίας Face Authentication

4.1.8 Έλεγχος υπαρκτού RefID χρήστη

```
final usersRef = FirebaseDatabase.instance.ref('Users');
final DatabaseEvent event = await usersRef.once();
Results resultsData;

// Check if there are any users
if (event.snapshot.exists) {
  Map<dynamic, dynamic> usersMap = event.snapshot.value as Map<dynamic, dynamic>;

  // Iterate through the users to find the specific email
  usersMap.forEach((key, value) {
    if (value['externalDatabaseRefID'] == results["externalDatabaseRefID"]) {
      resultsData = Results(value['email'],
                            value['lastName'],
                            value['firstName'],
                            value['dateOfBirth'],
                            value['idNumber'],
                            value['idNumber2'],
                            value['issueDate'],
                            value['expireDate']);
      controlNavigation(resultsData, key);
    }
  });
}
```

Εικόνα 11: Έλεγχος υπαρκτού RefID χρήστη

4.1.9 Εμφάνιση δεδομένων χρήστη

```
navigateToPersonalInfo(context, userData, uid) {
  Results currentUserData = Results(userData['email'],
                                    userData['lastName'],
                                    userData['firstName'],
                                    userData['dateOfBirth'],
                                    userData['idNumber'],
                                    userData['idNumber2'],
                                    userData['issueDate'],
                                    userData['expireDate']);
  Navigator.push(
    context,
    MaterialPageRoute(
    builder: (context) => PersonalInfo(currentUserData,  uid, userData['email']))
  ).then((_) {
    // Clear the controllers after returning
    emailController.clear();
    passwordController.clear();
  });
}
```

Εικόνα 12: Εμφάνιση δεδομένων χρήστη (μετά το Login)

```
Future<void> controlNavigation(Results resultsData, String userid) async {
  Navigator.push(
      context,
      MaterialPageRoute(builder: (context) =>  PersonalInfo(resultsData,  userid, resultsData.email))
  );
}
```

Εικόνα 13: Εμφάνιση δεδομένων χρήστη (μετά το Face Authentication)

4.1.10 Εμφάνιση φωτογραφιών χρήστη

```dart
Future<List<String>> loadImages(String? userid) async {
  // List<String> imageUrls = [];
  List<String> cachedImages = [];
  List<String> imagePaths = [
    'images/$userid/auditImage',
    'images/$userid/scannedFrontImage',
    'images/$userid/scannedBackImage',
  ];

  if (imageUrls.isEmpty) {
  for (String path in imagePaths) {
    try {
      var cachedFile = await DefaultCacheManager().getFileFromCache(path);
      if (cachedFile != null && cachedFile.file.existsSync()) {
        // Image found in cache
        cachedImages.add(path);
      } else {
        String downloadUrl = await FirebaseStorage.instance.ref(path).getDownloadURL();
        final response = await http.get(Uri.parse(downloadUrl));

        if (response.statusCode == 200) {
          imageUrls.add(downloadUrl);
        } else {
          ScaffoldMessenger.of(context).showSnackBar(
            SnackBar(content: Text('Error loading image: Status code ${response.statusCode}')),
          );
        }
      }
    } catch (e) {
      ScaffoldMessenger.of(context).showSnackBar(
        SnackBar(content: Text('Error loading image: $e')),
      );
    }
  }
}

  return imageUrls;
}
```

Εικόνα 14: Εμφάνιση φωτογραφιών χρήστη

```dart
import 'package:flutter_cache_manager/flutter_cache_manager.dart';

class CustomCacheManager {
  static CacheManager instance = CacheManager(
    Config(
      'customCacheKey',  // Unique cache key
      stalePeriod: const Duration(days: 7),  // Keep images for 7 days
      maxNrOfCacheObjects: 10,  // Max number of images cached
    ), // Config
  ); // CacheManager
}
```

Εικόνα 15: Οι εικόνες αποθηκεύονται τοπικά

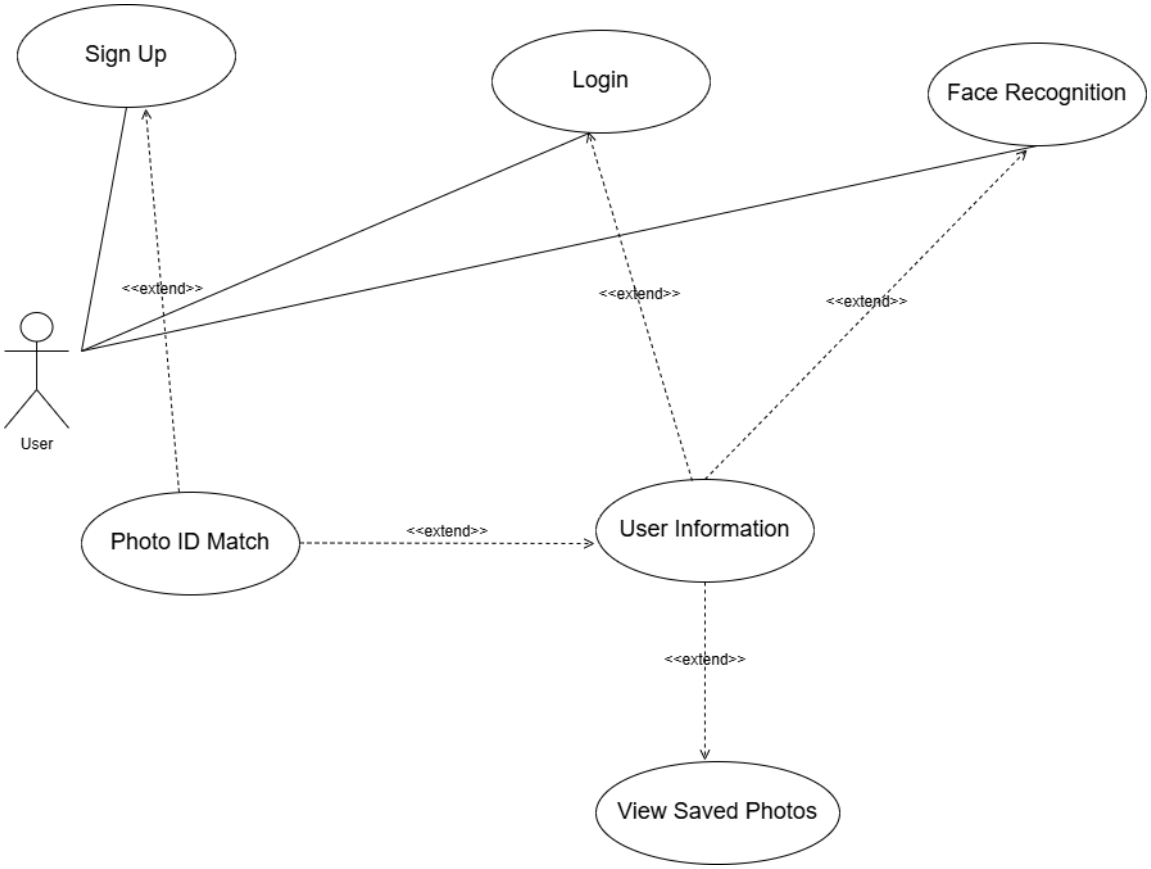
Κεφάλαιο 5ο

1. ΕΦΑΡΜΟΓΗ FACEAPP

5.1.1 Εισαγωγή

Η εφαρμογή FaceApp, συγκρίνει το πρόσωπο του εγγεγραμμένου χρήστη με τη φωτογραφία του στο δίπλωμα οδήγησης, πραγματοποιείται οπτική αναγνώριση κειμένου του διπλώματος, επαληθεύει τα στοιχεία του και εξάγει δεδομένα όπως το ονοματεπώνυμο, ημερομηνία γέννησης, ΑΦΜ, ημερομηνία έκδοσης και λήξης διπλώματος και αριθμός διπλώματος. Εφόσον ο χρήστης ανοίξει εκ νέου την εφαρμογή ο έλεγχος ταυτότητας προσώπου αποδεικνύεται μέσω 3D liveness το οποίο συγκρίνεται με το ήδη καταχωρημένο 3D Face Map και πραγματοποιεί είσοδο στην εφαρμογή χωρίς να απαιτείται κωδικός πρόσβασης.

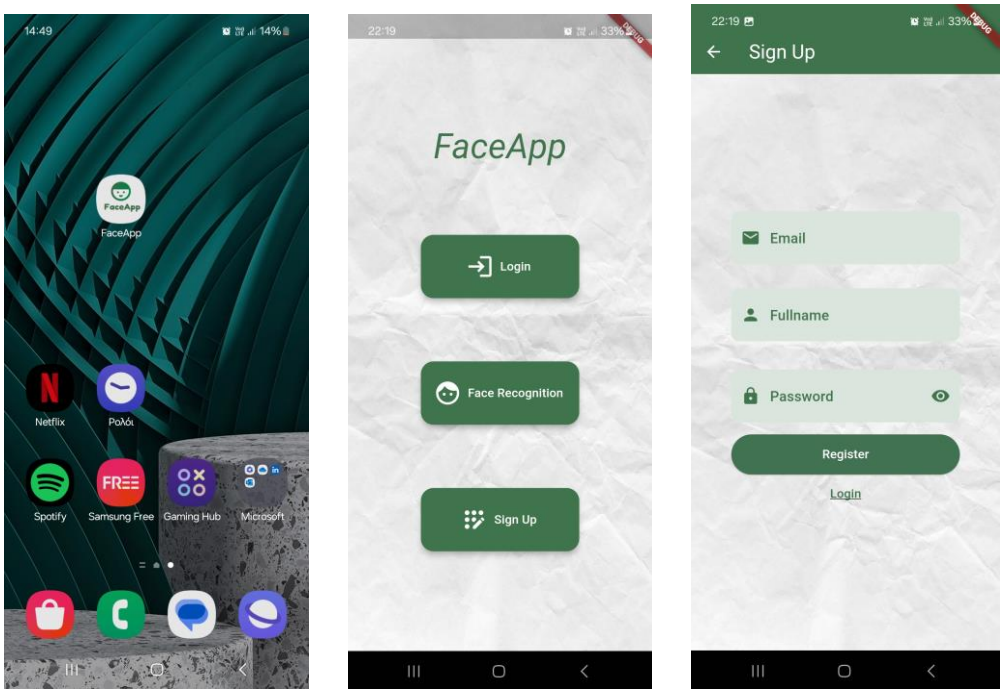
5.1.2 Use Case Diagram



Εικόνα 16: Use Case Diagram της εφαρμογής

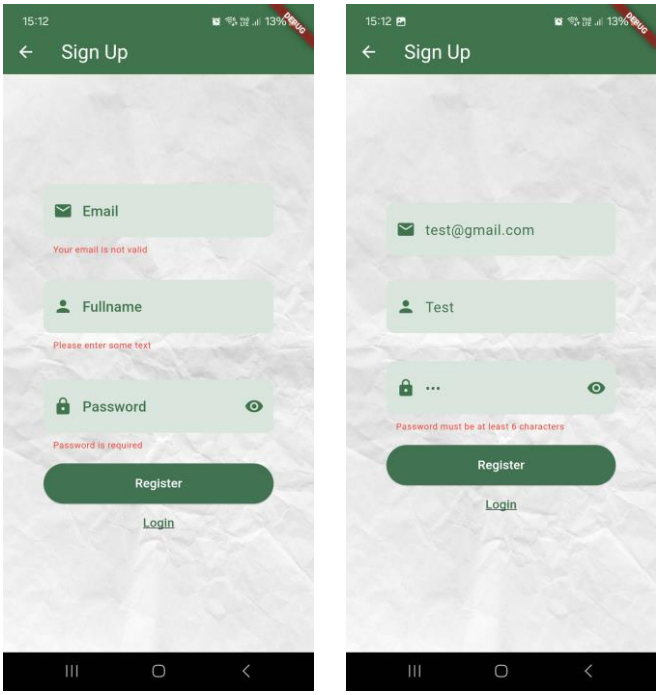
5.1.3 Ροή εφαρμογής

Ο χρήστης επιλέγει την εφαρμογή και εμφανίζεται στην οθόνη το μενού της εφαρμογής. Ο χρήστης επιλέγει το button «Sign Up» ώστε να κάνει εγγραφή στην εφαρμογή. Εμφανίζεται η οθόνη της εγγραφής, όπου ο χρήστης πρέπει να συμπληρώσει τα πεδία «email», «fullname» και «password».



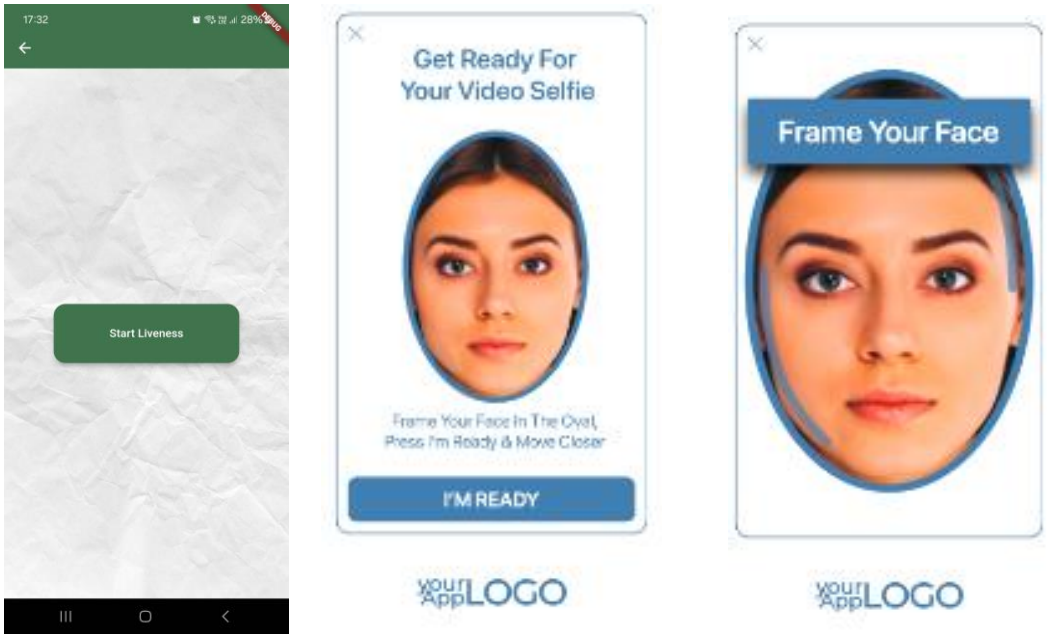
Εικόνα 17: Ροή εφαρμογής – Sign Up

Αν ο χρήστης κάνει κάποιο λάθος κατά τη διάρκεια της εγγραφής, εμφανίζονται κάποια μηνύματα έτσι ώστε να μπορέσει να συνεχίσει. (Εικόνα 17)



Εικόνα 18: Ροή εφαρμογής – Sign Up – Μηνύματα εφαρμογής

Μετά την επιτυχή εγγραφή του χρήστη στην εφαρμογή, ο χρήστης οδηγείτε στην οθόνη που εμφανίζει το button «Photo ID Match». Μόλις το επιλέξει, ξεκινά η διαδικασία ταυτοποίησης (3D FaceScan και αντιστοίχιση διπλώματος). Κατά τη διαδικασία δίνονται οδηγίες ώστε να ολοκληρωθεί επιτυχώς η διαδικασία «Video Selfie» που αποεικνύει το 3D Liveness.



Εικόνα 19: Ροή εφαρμογής – Διαδικασία 3D Liveness

Αν η «Video Selfie» δεν έχει ευκρίνεια, εμφανίζεται σχετική ενημέρωση προς το χρήστη να δοκιμάζει εκ νέου.

Εικόνα 20: Ροή εφαρμογής – Μήνυμα για νέα προσπάθεια 3D Fase Scan

Μόλις ολοκληρωθεί επιτυχώς η λήψη της «Video Selfie» τότε αποστέλεται το 3D Face Scan στο server της FaceTec. Στη συνέχεια ο χρήστης ενημερώνεται να έχει διαθέσιμο προς σάρωση το μπροστινό μέρος του διπλώματος.

Εικόνα 21: Ροή εφαρμογής – Αποατολή 3D Face Scan και προετοιμασία ταυτότητας

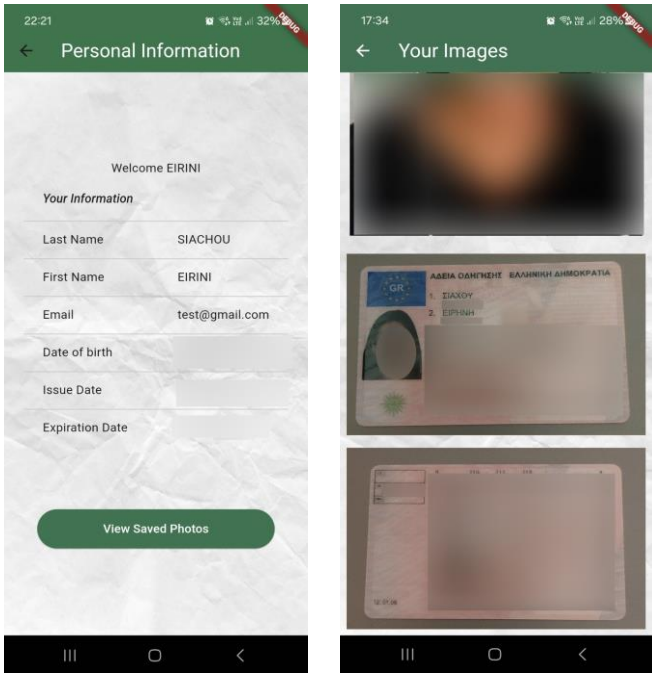
Εφόσον ολοκληρωθεί η διαδικασία, δηλαδή ανέβει το μπροστινό μέρος του διπλώματος στο server της FaceTec και επιβεβαιωθεί ότι ταιριάζει η «Video Selfie» με τη φωτογραφία προσώπου στο δίπλωμα τότε εμφανίζει μήνυμα και συνεχίζεται η διαδικασία σχετικά με τη σάρωση του πίσω μέρους του διπλώματος.

Εικόνα 22: Ροή εφαρμογής – Σκανάρισμα μπροστινού μέρους ταυτότητας

Μόλις ολοκληρωθεί η διαδικασία που αφορά τη σάρωση του πίσω μέρους του διπλώματος, εμφανίζονται τα στοιχεία χρήστη. Αν για οποιοδήποτε λόγο η διαδικασία έχει φέρει κάτι λάθος, ο χρήστης μπορεί να το αλλάξει και να επιλέξει επιβεβαίωση πληροφοριών. Έπειτα ανεβαίνουν τα στοιχεία τόσο στο server της FaceTec όσο και στη Firebase Realtime. Επίσης οι φωτογραφίες του χρήστη αποθηκεύονται στο Storage. Τέλος, εμφανίζεται μήνυμα ότι ολοκληρώθηκε η επιβεβαίωση «ταυτότητας».

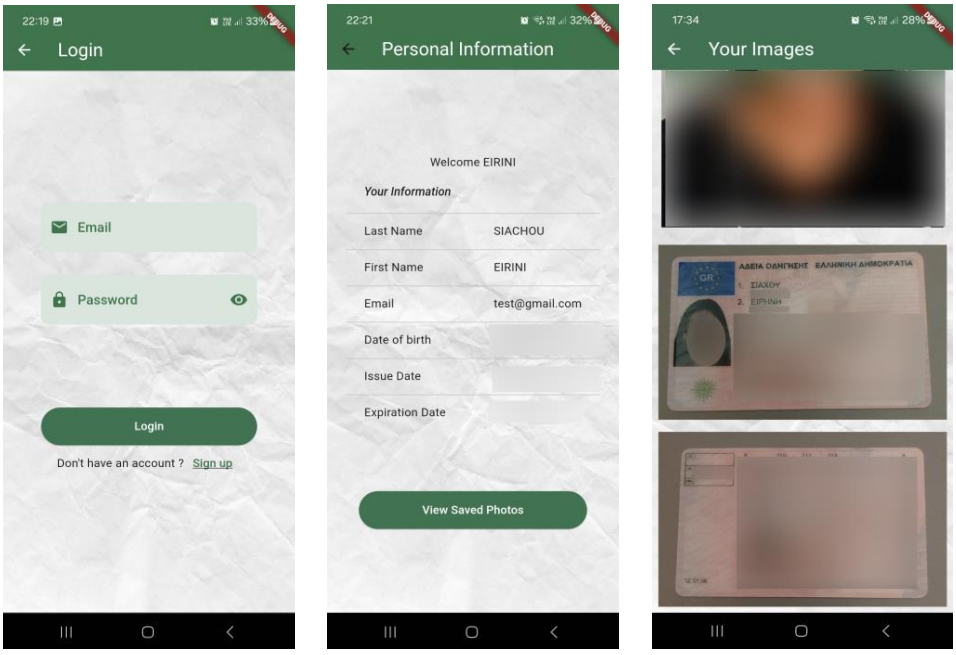
Εικόνα 23: Ροή εφαρμογής – Σκανάρισμα του πίσω μέρους ταυτότητας

Ο χρήστης μεταφέρεται στην οθόνη όπου εμφανίζονται οι πληροφορίες που αποθηκεύτηκαν. Στη συνέχεια, για να δει τις φωτογραφίες του μπορεί να επιλέξει το button «View Saved Photos».



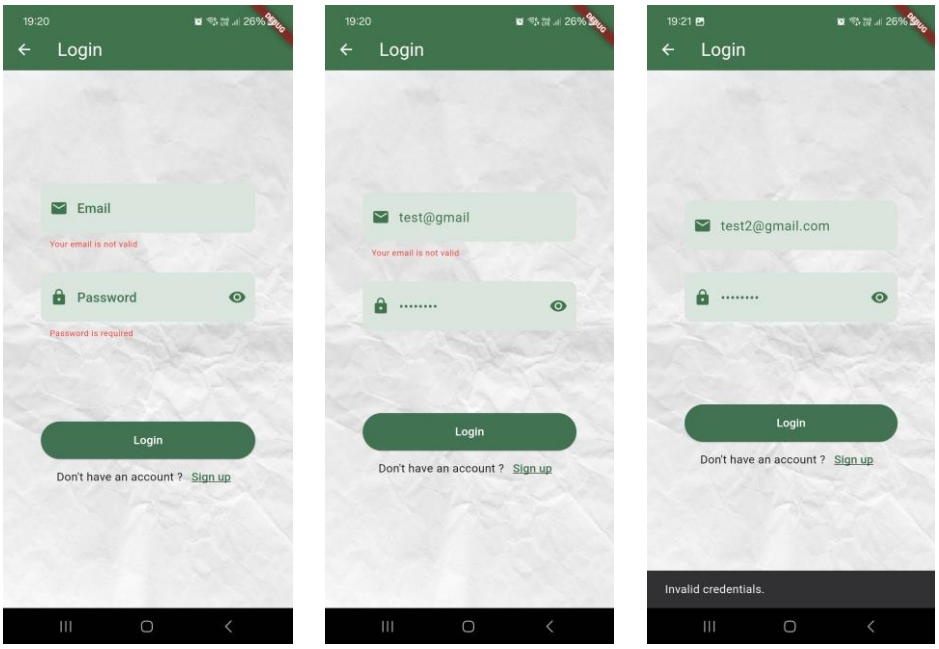
Εικόνα 24: Ροή εφαρμογής – Αποθηκευμένες πληροφορίες και φωτογραφίες του χρήστη

Σε εκ νέου άνοιγμα της εφαρμογής, ο χρήστης μπορεί να πραγματοποιήσει είσοδο στην εφαρμογή με τη διαδικασία Login, εισάγοντας το Email και το Password που είχε δηλώσει κατά την αρχική εγγραφή με αποτέλεσμα να μπορεί να δει τα στοιχεία του διπλώματος και τις φωτογραφίες του.



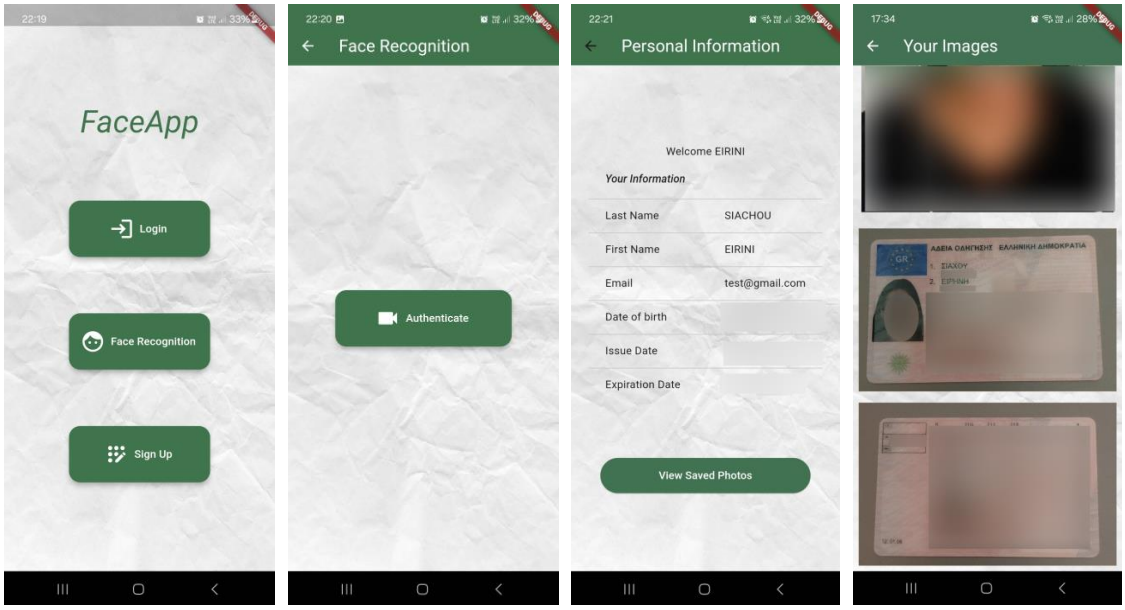
Εικόνα 25: Ροή εφαρμογής – Διαδικασία επιτυχημένου Login στην εφαρμογή

Σε περίπτωση που ο χρήστης προσπαθεί να συνδεθεί στην εφαρμογή και αποτύχει για κάποιους λόγους (λάθος email, password) τότε εμφανίζονται τα αντίστοιχα μηνύματα στην οθόνη.



Εικόνα 26: Ροή εφαρμογής – Παραδείγματα αποτυχημένου Login στην εφαρμογή

Υπάρχει και η δυνατότητα ο χρήστης να κάνει login στην εφαρμογή με Face Authentication. Μόλις ο χρήστης επιλέξει από το βασικό μενού της εφαρμογής το button «Face Recognition» μεταφέρεται στην αντίστοιχη οθόνη για να πραγματοποιήσει σύνδεση στην εφαρμογή πατώντας το button «Authenticate».Στο σημείο αυτό ξεκινά έλεγχος, για το να υπάρχει αποθηκευμένο στο Storage της εφαρμογής latestExternalRefId το οποίο αντιστοιχεί με το FaceMap του χρήστη. Εάν υπάρχει μπορεί να δει τα στοιχεία του διπλώματος και τις φωτογραφίες του.



Εικόνα 27: Ροή εφαρμογής – Διαδικασία εισόδου στην εφαρμογή με Face Authentication

Κεφάλαιο 6ο

1. ΣΥΜΠΕΡΑΣΜΑΤΑ

Συμπερασματικά, η ανάπτυξη της εφαρμογής FaceApp με τη χρήση του SDK της FaceTec για αναγνώριση προσώπου και ταυτοποίηση μέσω ταυτότητας ανέδειξε τη δύναμη και την ακρίβεια της τεχνολογίας βιομετρικών δεδομένων. Η ενσωμάτωση του SDK αποδείχθηκε αποτελεσματική, καθώς προσφέρει υψηλά επίπεδα ασφάλειας και αξιοπιστίας. Καθιστά με αυτόν τον τρόπο την εφαρμογή μια βάση ώστε με μελλοντικές βελτιώσεις να αποτελέσει μια κατάλληλη και αξιόπιστη εφαρμογή για διαδικασίες που απαιτούν ασφαλή ταυτοποίηση χρηστών.

Παρά τις προκλήσεις που αφορούν την εξασφάλιση της συμβατότητας με διάφορες συσκευές και τη διαχείριση θεμάτων απορρήτου, η τεχνολογία αυτή αποδεικνύεται ικανή να ενισχύσει την εμπιστοσύνη των χρηστών, προσφέροντας ακριβή και γρήγορη επαλήθευση ταυτότητας. Στο μέλλον, περαιτέρω βελτιώσεις και αναβαθμίσεις του συστήματος θα μπορούσαν να διευρύνουν τη χρήση της αναγνώρισης προσώπου σε διάφορους τομείς, όπως οι διαδικτυακές συναλλαγές και οι υπηρεσίες ηλεκτρονικής διακυβέρνησης, προσφέροντας μια ολοκληρωμένη και ασφαλή εμπειρία χρήστη.

2. ΜΕΛΛΟΝΤΙΚΕΣ ΕΠΕΚΤΑΣΕΙΣ

Η ανάπτυξη της εφαρμογής FaceApp έγινε με τη χρήση του SDK της FaceTec που παρέχεται για test περιβάλλον. Αυτό σημαίνει ότι υπάρχουν κάποιοι περιορισμοί στη χρήση του SDK, στην υποστήριξη από την ίδια την εταιρεία αλλά και στις δυνατότητες της εφαρμογής. Οπότε αν υπάρξει συνεργασία με την εταιρία, παρέχεται πλατφόρμα όπου μπορούν να δημιουργηθούν custom πρότυπα σε σχέση με τις ταυτότητες που γίνονται αποδεκτές. Αυτό θα έχει ως συνέπεια η εφαρμογή να μπορεί να κάνει χάριν παραδείγματος, έλεγχο φοιτητικής ή όποιου άλλου είδους ταυτότητας επιθυμεί.

Μια επέκταση που μπορεί να γίνει είναι η αποθήκευση των δεδομένων σε δικό μας server και όχι στον server της FaceTec. Αυτό δίνει τη δυνατότητα να αποθηκεύονται επιπλέον στοιχεία από τις ταυτότητες, για να μπορούν να ικανοποιούνται κάθε φορά οι ανάγκες της εφαρμογής.

Ακόμη θα μπορούσε στην υλοποίηση τη εφαρμογής να γίνουν κάποιες μικρές αλλαγές και βελτιώσεις , ώστε μελλοντικά να μπορεί να εγκατασταθεί και να χρησιμοποιηθεί και σε συσκευές ios, αλλά και ως web εφαρμογή χρησιμοποιώντας την κάμερα του υπολογιστή. Αυτή η διαδικασία θα έφερνε σημαντικές αλλαγές και στο ui/ux της εφαρμογής ώστε να γίνει και πιο φιλικό προς τους χρήστες.

Τέλος, μια πολύ σημαντική επέκταση της εφαρμογής θα ήταν η δυνατότητα συγχρονισμού των δεδομένων της όταν γίνει αποσύνδεση από το διαδίκτυο. Αυτό μπορεί να υλοποιηθεί με caching (τοπική αποθήκευση δεδομένων δηλαδή στη συσκευή) με τη χρήση βάσης δεδομένων (όπως SQLite), με αρχεία cache, ή με τη χρήση για παράδειγμα της Firebase που παρέχει μηχανισμούς για offline αποθήκευση και αυτόματη ενημέρωση των δεδομένων μόλις αποκατασταθεί η σύνδεση.

Βιβλιογραφία

[1] Michael Fairhurst, 2019, Τίτλος Biometrics: A Very Short Introduction (Very Short Introductions), Oxford University Press.

[2] Biometrics, URL: https://www.britannica.com/science/biometrics

[3] Biometrics Liveness Detection: Framework and Metrics, URL: https://www.nist.gov/system/files/documents/2021/01/26/403_schuckers.pdf

[4] Face Liveness Detection Using Artificial Intelligence Techniques: A Systematic Literature Review and Future Directions, URL: https://www.mdpi.com/2504-2289/7/1/37

[5] Innovatics, URL: https://www.innovatrics.com/innovatrics-abis/

[6] IDEMIA, URL: https://www.idemia.com/technology/our-expertise-biometrics

[7] FaceTec Competitors and Similar Companies, URL: https://craft.co/facetec/competitors

[8] FaceTec Developer Documentation, URL: https://dev.facetec.com/

[9] How to Create Use Case Description for Your Business Analysis Report, URL: https://www.dummies.com/article/business-careers-money/business/general-business/how-to-create-use-case-description-for-your-business-analysis-report-162468/

[10] Flutter Docs, URL: https://docs.flutter.dev/

[11] FaceTec partners, URL: https://www.biometricupdate.com/202105/facetec-selfie-biometrics-integrated-for-enterprises-by-veritran-as-market-stays-hot