Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
Στην Ασφάλεια Υπολογιστών και Δικτύων

Σύστημα Εξακρίβωσης Ταυτότητας Για Πλατφόρμες Εξ΄ Αποστάσεως Εκπαίδευσης Με Χρήση Βιομετρικών Τεχνολογιών

Κωνσταντίνος Ι. Ανδρουλάκης

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Μάιος 2019

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Σύστημα Εξακρίβωσης Ταυτότητας Για Πλατφόρμες Εξ΄ Αποστάσεως Εκπαίδευσης Με Χρήση Βιομετρικών Τεχνολογιών

Κωνσταντίνος Ι. Ανδρουλάκης

Επιβλέπουσα Καθηγήτρια
Αδαμαντίνη Περατικού

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στην Ασφάλεια Υπολογιστών και Δικτύων

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Μάιος 2019

Περίληψη

Η διατριβή επικεντρώνεται κυρίως στην μελέτη και έπειτα στην υλοποίηση ενός συστήματος πιστοποίησης/εξακρίβωσης ταυτότητας για πλατφόρμες εξ΄ αποστάσεως εκπαίδευσης με χρήση βιομετρικών τεχνολογιών. Τα θεματικά πεδία που καλύπτει είναι αυτά των διαδικτυακών εφαρμογών, ασφάλειας και βιομετρικών δεδομένων. Κύριοι άξονες της διατριβής είναι αφενός η μελέτη των υφιστάμενων βιομετρικών συστημάτων πιστοποίησης και αφενός η παρουσίαση και υλοποίηση ενός νέου απλού, ασφαλούς και ταυτόχρονα εύκολου στη χρήση αντίστοιχου συστήματος που θα μπορεί να χρησιμοποιηθεί από σύγχρονες πλατφόρμες εξ αποστάσεως εκπαίδευσης.

Οι διαφορετικές τεχνολογίες και προδιαγραφές ασφάλειας που χρησιμοποιεί η κάθε υπηρεσία έχει σαν αποτέλεσμα την δραματική αύξηση των λογαριασμών που διαχειρίζεται ο κάθε χρήστης στην καθημερινότητα του, καθιστώντας όλο και πιο δύσκολη την απομνημόνευσή τους. Το γεγονός αυτό σε συνδυασμό με τη ραγδαία αύξηση κακόβουλων χρηστών και διαδικτυακών επιθέσεων, την εμφάνιση όλο και περισσότερων κενών ασφάλειας στο διαδίκτυο καθώς επίσης και τη όλο και πιο συχνή καταγραφή περιπτώσεων υποκλοπής πνευματικής ιδιοκτησίας, πλαστογράφησης, λογοκλοπής και συμπαιγνίας που σχετίζονται με εξετάσεις ή γραπτές εργασίες στον τομέα της εξ αποστάσεως εκπαίδευσης, μας οδήγησαν στην αναζήτηση νέων τρόπων ταυτοποίησης των ηλεκτρονικών υπηρεσιών.

Για την επίλυση αυτού του προβλήματος σε πλατφόρμες εξ αποστάσεως εκπαίδευσης υλοποιήθηκε ένα σύστημα βιομετρικής αναγνώρισης. Το σύστημα είναι σχεδιασμένος έτσι ώστε να συλλέγει βιομετρικά δεδομένα (στην περίπτωσή μας φωτογραφίες των χρηστών) κατά τη διαδικασία της εγγραφής του εκάστοτε χρήστη στην πλατφόρμα εξ αποστάσεως εκπαίδευσης. Ένας αισθητήρας (συνήθως κάμερα) μετατρέπει το συγκεκριμένο βιομετρικό χαρακτηριστικό (φωτογραφία προσώπου) σε ηλεκτρονικό κώδικα τον οποίο αποθηκεύει και τον αντιστοιχίζει με το συγκεκριμένο χρήστη. Κάθε φορά που χρήστης προσπαθεί να αποκτήσει πρόσβαση μέσα από το συγκεκριμένο σύστημα, γίνεται έλεγχος της ταυτότητάς του, ο οποίος επιτυγχάνεται με την λήψη νέας φωτογραφικής απεικόνισής του, και τη σύγκρισή της με το αποθηκευμένο πρότυπο. Σε εξαιρετικές περιπτώσεις θα χρησιμοποιείται και ένα υποσύστημα two-factor authentication password.

Για την υλοποίηση χρησιμοποιήθηκαν τεχνολογίες και αλγόριθμοι που καλύπτονται από άδειες ελεύθερου λογισμικού ενώ το τελικό παραδοτέο είναι ένα διαδικτυακό εργαλείο αναγνώρισης

προσώπου που μπορεί να λειτουργεί είτε αυτόνομα είτε σε συνεργασία με αντίστοιχες πλατφόρμες εξ αποστάσεως εκπαίδευσης.

Μελετήθηκε η απόδοσή του εργαλείου μας και παραθέτονται αντίστοιχα μετρήσεις της απόδοσής του. Το εργαλείο αποδεικνύεται ότι είναι βοηθητικό και δεν προσθέτει περισσότερο φόρτο εργασίας στον χρήστη ενώ παράλληλα διευκολύνει και καθιστά πιο γρήγορη την σύνδεση των χρηστών.

Ειδική μνεία γίνεται στη διαχείριση των προσωπικών δεδομένων, στους κανονισμούς και νόμους που έχουν θεσπιστεί και οφείλει να ακολουθεί το εργαλείο ενώ και παρουσιάζεται και η αντιμετώπιση των προσωπικών δεδομένων των χρηστών από εμάς.

Summary

The dissertation focuses mainly on the study and then on the implementation of a certification / authentication system for biometrics-based education distance learning platforms. The thematic areas covered are those of web applications, security and biometric data. The main axes of the dissertation are the study of the existing biometric certification systems and the presentation and implementation of a new simple, safe and at the same time easy to use equivalent system that can used by modern distance education platforms.

The different security technologies and specifications used by each service result in a dramatic increase in the accounts that each user manages in his everyday life, making it increasingly difficult to memorize. This, combined with the rapid increase in malicious users and online attacks, the emergence of more and more online security gaps as well as the increasingly frequent recording of cases of intellectual property, forgery, plagiarism and collusion related to examinations or written work in the field of distance learning, led us to find new ways of identifying e-services.

To solve this problem on distance learning platforms a biometric recognition system implemented. The system designed to collect biometric data (in our case user images) during the user's registration process on the distance-learning platform. A sensor (usually a camera) converts this biometric feature (face photo) into an electronic code that it stores and assigns to that particular user. Every time a user attempts to gain access through this system, his / her identity is checked, which is obtained by taking a new photographic image and comparing it to the saved template. In exceptional cases, a two-factor authentication password subsystem can also used.

Technology and algorithms covered by free software licenses used either for the implementation, while the final delivery is an online face recognition tool that can run independently or in collaboration with corresponding distance education platforms.

The performance of our tool has studied and corresponding performance measurements are listed. The tool proves to be ancillary and does not add more workload to the user while also facilitating and quicker connecting users.

Special mention is made in the management of personal data, in the regulations and laws that have been adopted and must follow the tool and the presentation of the personal data of the users from us.

Implementation uses technologies and algorithms covered by free software, while the final delivery is an online face recognition tool.

Ευχαριστίες

Η παρούσα μεταπτυχιακή διατριβή εκπονήθηκε κατά το ακαδημαϊκό έτος 2018-2019 στον τομέα "Ασφάλεια Υπολογιστών και Δικτύων" της Σχολής Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου της Κύπρου. Στο σημείο αυτό θα ήθελα να ευχαριστήσω όλους όσους συνέβαλαν στην ολοκλήρωση αυτής της προσπάθειας.

Πρώτα απ'όλα θα ήθελα να ευχαριστήσω την επιβλέπουσα καθηγήτρια κα Αδαμαντίνη Περατικού για την εμπιστοσύνη που μου έδειξε στην ανάθεση της παραπάνω μεταπτυχιακής εργασίας και για τη πολύτιμη βοήθεια, καθοδήγηση αλλά και για τις παρατηρήσεις της σχετικά με την οργάνωση, τη δομή και το περιεχόμενο της διατριβής.

Θα ήθελα να ευχαριστήσω τον φίλο μου Βασίλη Τζικούλη για τη πολύτιμη επιστημονική βοήθεια που μου προσέφερε, για τις φιλικές του συμβουλές αλλά και για την υπομονή του σε ημέρες πίεσης.

Πάνω απ'όλα είμαι ευγνώμων στους γονείς μου Γιάννη και Μαρία αλλά και στον αδερφό μου Φοίβο, γιατί πάντα ήταν δίπλα μου όποτε τους χρειαζόμουν στη ζωή μου. Για την ηθική και υλική στήριξη που μου παρείχαν αλλά και τη συμπαράσταση καθ'όλη τη διάρκεια των σπουδών μου.

Επίσης, ευχαριστώ τη σύζυγό μου Αριάδνη η οποία μου έδωσε την ευκαιρία να αρχίσω, να συνεχίσω και να ολοκληρώσω τη παρούσα μεταπτυχιακή διατριβή και μου παρείχε πλήρη υποστήριξη κατά τη διάρκεια δύσκολων στιγμών.

Αφιερώνω αυτή την εργασία στον γιό μου Γιάννη.

Περιεχόμενα

Περίληψη 3

Summary 5

Ευχαριστίες 7

Περιεχόμενα 8

Πίνακας εικόνων/γραφημάτων 9

Εισαγωγή 10

1.1 Κίνητρο για την εργασία 11

1.2 Σκοπός και στόχοι της εργασίας 12

1.3 Προσδοκόμενα παραδοτέα 14

Βιβλιογραφική ανασκόπηση 15

2.1 Εξ αποστάσεως εκπαίδευση 15

2.2 Πληροφοριακά συστήματα 19

2.2.1 Πληροφοριακά συστήματα στην εξ αποστάσεως εκπαίδευση 20

2.2.2 Ασφάλεια Πληροφοριακών Συστημάτων 24

2.3 Βιομετρικές τεχνολογίες 25

2.3.1 Ορισμός 25

2.3.2 Κυρίαρχες βιομετρικές τεχνολογίες (δακτυλικά, πρόσωπο κλπ) 25

2.3.3 Εφαρμογές των βιομετρικών συστημάτων 27

2.3.4 Βιομετρικά συστήματα σε σχέση με τα παραδοσιακά συστήματα αναγνώρισης 28

2.3.5 Πλεονεκτήματα συστημάτων βιομετρικής πιστοποίησης χρηστών 29

2.3.6 Προβλήματα στατικής ταύτισης / μειονεκτήματα 30

Σχεδιασμός / υλοποίηση του συστήματος αναγνώρισης προσώπου 32

3.1 Εισαγωγή 32

3.2 Μεθοδολογία 34

3.3 Σχετικές υλοποιήσεις 35

3.4 Αναγνώριση προσώπου 35

3.5 Αναγνώριση χαρακτηριστικών προσώπου 36

3.6 Προσέγγιση προβλήματος 38

3.7 Υλοποίηση 39

3.7.1 Μοντέλο χρήσης συστήματος 40

3.7.2 Παρουσίαση αλγορίθμου αναγνώρισης προσώπου 41

3.7.3 Παρουσίαση αλγορίθμου ταυτοποίησης χαρακτηριστικών προσώπου 44

3.7.4 Παραμετροποίηση εργαλείων αναγνώρισης προσώπου 45

3.7.5 Παραμετροποίηση εργαλείων ταυτοποίησης προσώπου 48

3.7.6 Διασύνδεση ηλεκτρονικής πλατφόρμας με το σύστημά μας 49

3.8 Δοκιμές - Πειραματικές αξιολογήσεις 52
3.9 Απόδοση συστήματος (Σε επίπεδο διακομιστή) 53
3.10 Κόστος και εκπαίδευση 54
3.11 Περιορισμοί 54
Προσωπικά δεδομένα 56
4.1 Ορισμοί 58
4.2 Παράγοντες για τη αποδοχή των χρηστών 64
4.3 Αποδοχή των βιομετρικών συστημάτων 64
4.4 Κατευθύνσεις για τη χρήση Βιομετρικών μεθόδων 66
4.5 Βασικές αρχές που διέπουν το σύστημά μας 70
Σύνοψη 73
5.1 Σύνοψη 73
5.2 Μελλοντική έρευνα 74
Βιβλιογραφία 76
Παράρτημα 82
Index.php 82
Login.php 86
Register.php 89
TμFace.js 90
CCV.js 91
Στιγμιότυπα εφαρμογής 101

Πίνακας εικόνων/γραφημάτων

Εικόνα 1: Παράδειγμα πλαισίων οριοθέτησης κάθε προσώπου, με τις αντίστοιχες βαθμολογίες 42
Εικόνα 2: Παράδειγμα σήμανσης 68 ορόσημων σημείων προσώπου 42
Εικόνα 3: Παράδειγμα απομόνωσης και κεντραρίσματος προσώπων προς έλεγχο 43
Εικόνα 4: Παράδειγμα οριοθέτησης πολλαπλών προσώπων και τα σκορ της πιθανότητας οι οριοθετήσεις να είναι ορθά πρόσωπα 48
Εικόνα 5: Παράδειγμα οριοθέτησης πολλαπλών προσώπων και τα σκορ της πιθανότητας αναγνώρισής τους 49

Κεφάλαιο 1
Εισαγωγή

Πολλοί άνθρωποι ζητούν μια νέα προσέγγιση της εκπαίδευσης που να ανταποκρίνεται στις ανάγκες της μάθησης στη σύγχρονη εποχή. Η εξ' αποστάσεως εκπαίδευση είναι μία ευκαιρία για τους εκπαιδευόμενους για επιπλέον μάθηση και επιδιώκει τη παροχή εκπαίδευσης χωρίς την ανάγκη φυσικής παρουσίας στο χώρο που αυτή πραγματοποιείται. Ο όρος εξ αποστάσεως εκπαίδευση (distance learning / education) ή αλλιώς τηλεκπαίδευση αναφέρεται στον τρόπο διδασκαλίας/εκμάθησης, κατά τον οποίο ο εκπαιδευτής και ο εκπαιδευόμενος βρίσκονται σε απόσταση και χρησιμοποιούν ειδικά διδακτικά υλικά. Στο πέρασμα όμως του χρόνου και παράλληλα με νέες τεχνολογίες γεννήθηκαν νέες ανάγκες για την ασφάλεια των δεδομένων και την εύκολη χρήση τους. Παράλληλα η διασφάλιση των προσωπικών δεδομένων και της πνευματικής ιδιοκτησίας μας έχει οδηγήσει σε σημείο να κάνουμε πολλά πληροφοριακά συστήματα όλο και πιο δύσκολα προσβάσιμα. Για να το επιτύχουμε αυτό, έχουμε αρχίσει και αναζητούμε αδιάβλητους τρόπους πιστοποίησης. Αναζητούμε λοιπόν χαρακτηριστικά τα οποία είναι μοναδικά και σε συνδυασμό με άλλες παραμέτρους, μας προκύπτει η εκπλήρωση συνθηκών εισόδου ή μη. Τα προβλήματα αυτά προτείνεται να λύσουν οι βιομετρικές τεχνολογίες

αναγνώρισης χρηστών. Οι Βιομετρικές Τεχνολογίες είναι η επιστήμη της ανίχνευσης και της αναγνώρισης των ανθρωπίνων χαρακτηριστικών, με τη μέτρηση και την ανάλυση βιολογικών δεδομένων χρησιμοποιώντας ηλεκτρονικές τεχνολογίες. Η χρήση Βιομετρικών Τεχνολογιών είναι ένας γρήγορος και αποτελεσματικός τρόπος για να συνδεθούμε σε ένα πληροφοριακό σύστημα χωρίς να πρέπει να θυμόμαστε ένα κωδικό πρόσβασης, παρέχουν προστασία της ταυτότητας ενός ατόμου και ενισχύουν την ασφάλεια σχετικά με τη κλοπή της. Στην παρούσα εργασία επιδιώκουμε να καλύψουμε τις ανάγκες αυτές υλοποιώντας ένα τέτοιο σύστημα ταυτοποίησης προσώπου για μία πλατφόρμα εξ αποστάσεως εκπαίδευσης το οποίο επιδιώκει να αντικαταστήσει τον παραδοσιακό τρόπο σύνδεσης των χρηστών (μοντέλο ονόματος χρήστη - κωδικού) με ένα νέο που θα βασίζεται στην οπτική αναγνώριση των προσώπων των χρηστών. Πρόκειται ουσιαστικά για μια εφαρμογή που βασίζεται στον υπολογιστή ή άλλη κινητή συσκευή για την αυτόματη αναγνώριση ή επαλήθευση ενός ατόμου από ψηφιακές εικόνες, συγκρίνοντας επιλεγμένα χαρακτηριστικά του προσώπου του, μέσω της ζωντανής εικόνας που λαμβάνεται εκείνη τη στιγμή και χαρακτηριστικών προσώπου μίας βάσης δεδομένων που περιλαμβάνει τα βιομετρικά δεδομένα του συνόλου των έγκυρων χρηστών της πλατφόρμας. Με την υλοποίησή του θα δίνεται η δυνατότητα στους χρήστες να συνδέονται απλά σαρώνοντας το πρόσωπό τους. Η σάρωση αυτή μπορεί να πραγματοποιείται με τη λήψη μίας φωτογραφίας του προσώπου του υποκείμενου χρήστη με τη χρήση της κάμερας ενός ηλεκτρονικού υπολογιστή τους είτε μίας κινητής συσκευής. Στα πλαίσια της εργασίας θα επικεντρωθούμε στην υλοποίηση του συστήματος για την πλατφόρμα εξ αποστάσεως εκπαίδευσης Moodle.

1.1 Κίνητρο για την εργασία

Βασικό κίνητρο για την υλοποίηση της εργασίας αποτελεί ανάγκη απλοποίησης των τεχνικών πιστοποίησης χρηστών που γεννήθηκε από τη συνεχή και αυξανόμενη χρήση πολλαπλών και διαφορετικών ηλεκτρονικών υπηρεσιών σε καθημερινή βάση από όλο και περισσότερους χρήστες. Οι διαφορετικές τεχνολογίες και προδιαγραφές ασφάλειας που χρησιμοποιεί η κάθε υπηρεσία έχει σαν αποτέλεσμα την δραματική αύξηση των λογαριασμών που διαχειρίζεται ο κάθε χρήστης στην καθημερινότητα του, καθιστώντας όλο και πιο δύσκολη την απομνημόνευσή τους. Το γεγονός αυτό σε συνδυασμό με τη ραγδαία αύξηση κακόβουλων χρηστών και διαδικτυακών επιθέσεων, την εμφάνιση όλο και περισσότερων κενών ασφάλειας στο διαδίκτυο καθώς επίσης και τη όλο και πιο συχνή καταγραφή περιπτώσεων υποκλοπής πνευματικής ιδιοκτησίας, πλαστογράφησης, λογοκλοπής και συμπαιγνίας που σχετίζονται με εξετάσεις ή γραπτές εργασίες στον τομέα της εξ αποστάσεως εκπαίδευσης, μας οδήγησαν στην αναζήτηση

νέων τρόπων ταυτοποίησης των ηλεκτρονικών υπηρεσιών. Η αναγνώριση ενός ατόμου και ο έλεγχος πρόσβασης είναι αναμφισβήτητα δύο τομείς οι οποίοι απαιτούν τη μέγιστη ασφάλεια. Οι κωδικοί PINs, οι έξυπνες κάρτες αλλά και ο συνδυασμός τους, συνέβαλαν, αλλά και προσφέρουν ακόμη τα μέγιστα σε συστήματα ελέγχου πρόσβασης, ηλεκτρονικών συναλλαγών ή και σε συστήματα εξ αποστάσεως εκπαίδευσης. Με την πάροδο όμως των χρόνων, η τεχνολογία τους σταδιακά άρχισε να γίνεται προσιτή στον καθένα με αποτέλεσμα να αρχίζουν να εμφανίζονται κρούσματα παραβίασης ή πλαστογράφησής τους. Παράλληλα, η χρήση πολλών και διαφορετικών καρτών που απαιτούσε η κάθε εφαρμογή αλλά και η αποστήθιση πληθώρας κωδικών PINs, δεν έγιναν αποδεκτές από το ευρύ κοινό, με αποτέλεσμα να δημιουργηθεί η ανάγκη για κάποια νέα συστήματα, τα οποία θα έπρεπε αφενός να είναι εύχρηστα και αφετέρου να είναι πιο ασφαλή. Το πρόβλημα αυτών των νέων τεχνολογιών έρχονται να επιλύσουν οι βιομετρικές τεχνολογίες ταυτοποίησης. Η χρήση Βιομετρικών Τεχνολογιών είναι ένας γρήγορος και αποτελεσματικός τρόπος για την πιστοποίηση, αυθεντικοποίηση και σύνδεση των χρηστών σε μία ηλεκτρονική υπηρεσία χωρίς την ανάγκη χρήσης ζευγών ονόματος χρήστη και κωδικού που έχει σαν αποτέλεσμα την απομνημόνευση όλο και λιγότερης πληροφορίας από μέρους τους. Οι Βιομετρικές Τεχνολογίες παρέχουν προστασία της ταυτότητας του ατόμου, ενισχύουν την ασφάλεια σχετικά με τη κλοπή της αλλά ταυτόχρονα επιταχύνουν και τη διαδικασία πιστοποίησης.

1.2 Σκοπός και στόχοι της εργασίας

Σκοπός της διατριβής είναι η παρουσίαση βιομετρικών τεχνολογιών και ποιο συγκεκριμένα της μεθόδου αναγνώρισης προσώπου και των χαρακτηριστικών της που μπορούμε να χρησιμοποιήσουμε για να διευκολύνουμε τη διαδικασία σύνδεσης ενός χρήστη σε μία ηλεκτρονική υπηρεσία (στην περίπτωσή μας ηλεκτρονική πλατφόρμα εξ αποστάσεως εκπαίδευσης) ενώ ταυτόχρονα προστατεύουμε την ατομική ταυτότητα των χρηστών.

Στόχος μας είναι η είναι η υλοποίηση ενός Βιομετρικού Συστήματος ταυτοποίησης χρηστών για Πλατφόρμες εξ αποστάσεως εκπαίδευσης. Το σύστημα είναι σχεδιασμένος έτσι ώστε να συλλέγει βιομετρικά δεδομένα (στην περίπτωσή μας φωτογραφίες των χρηστών) κατά τη διαδικασία της εγγραφής του εκάστοτε χρήστη στην πλατφόρμα εξ αποστάσεως εκπαίδευσης. Ένας αισθητήρας (συνήθως κάμερα) μετατρέπει το συγκεκριμένο βιομετρικό χαρακτηριστικό (φωτογραφία προσώπου) σε ηλεκτρονικό κώδικα τον οποίο αποθηκεύει και τον αντιστοιχίζει με το συγκεκριμένο χρήστη. Κάθε φορά που χρήστης προσπαθεί να αποκτήσει πρόσβαση μέσα

από το συγκεκριμένο σύστημα, γίνεται έλεγχος της ταυτότητάς του, ο οποίος επιτυγχάνεται με την λήψη νέας φωτογραφικής απεικόνισής του, και τη σύγκρισή της με το αποθηκευμένο πρότυπο. Σε εξαιρετικές περιπτώσεις θα χρησιμοποιείται και ένα υποσύστημα two-factor authentication password.

Κατά την υλοποίηση του συστήματος μας θα πρέπει να καλύπτονται κάποιες συγκεκριμένες προδιαγραφές όπως αυτές αναλύονται παρακάτω.

1. Αρχικά ο εκπαιδευόμενος/εκπαιδευτικός κατά την εγγραφή του θα παρέχει μία καθαρή φωτογραφία ταυτότητας την οποία το σύστημα θα χρησιμοποιεί ως σημείο 0.

2. Ο διαχειριστής του συστήματος όταν θα δημιουργεί ένα νέο λογαριασμό για ένα εκπαιδευόμενο/εκπαιδευτικό θα αντιστοιχίζει την φωτογραφία ταυτότητάς του στο σύστημα.

3. Ο εκπαιδευόμενος/εκπαιδευτικός κατά την πρώτη προσπάθεια σύνδεσης στο σύστημα και αφού καταχωρήσει τα στοιχεία ορθά και συνδεθεί θα πρέπει να παρέχει μία «ζωντανή» φωτογραφία εκείνης της στιγμής μέσω της κάμερας της ηλεκτρονικής συσκευής που χρησιμοποιεί. Η είσοδός του στο σύστημα δεν θα επιτρέπεται μέχρι την υποβολή της φωτογραφίας. Αυτή η φωτογραφία αρχικά θα συγκρίνεται με την υπάρχουσα αποθηκευμένη και έπειτα θα αποθηκεύεται στο σύστημα ως δεύτερος οδηγός.

4. Έπειτα, και για κάθε άλλη προσπάθεια σύνδεσης, ο εκπαιδευόμενος/εκπαιδευτικός θα έχει τη δυνατότητα να συνδεθεί είτε χρησιμοποιώντας το σύστημα αναγνώρισης προσώπου είτε το κλασσικό σύστημα του ζεύγους email/password.

5. Κάθε προσπάθεια ταυτοποίησης του εκπαιδευόμενου/εκπαιδευτικού θα έχει ως αποτέλεσμα ένα αριθμό ακρίβειας. Όταν αυτός ο αριθμός θα είναι κάτω από ένα ορισμένο threshold για ορισμένο αριθμό προσπαθειών το σύστημα αναγνώρισης προσώπου θα απενεργοποιείται. Ο εκπαιδευόμενος/εκπαιδευτικός θα μπορεί να συνδεθεί μονάχα με τον κωδικό του ενώ μετά από επιτυχή σύνδεση θα του παρουσιάζονται και οι αντίστοιχες φωτογραφίες των εσφαλμένων προσπαθειών προς ενημέρωσή του με στόχο την αναγνώριση πιθανών κακόβουλων προσπαθειών σύνδεσης από τρίτους.

1.3 Προσδοκόμενα παραδοτέα

Το αποτέλεσμα της εργασίας που θα αποτελέσει και το παραδοτέο υλικό είναι ένα σύστημα αναγνώρισης προσώπου με τη μορφή εργαλείου (plugin). Οδηγίες χρήσης καθώς και ένα πρότυπο παράδειγμα μίας πλατφόρμας εξ αποστάσεως εκπαίδευσης την οποία θα συνδεθεί το εργαλείο.

Το παραδοτέο εργαλείο θα είναι σε θέση να λειτουργεί είτε αυτόνομα είτε ως μέρος ενός μεγαλύτερου πληροφοριακού συστήματος στο οποίο θα έχει τη δυνατότητα να διασυνδεθεί.

Κεφάλαιο 2
Βιβλιογραφική ανασκόπηση

2.1 Εξ αποστάσεως εκπαίδευση

Οι περισσότεροι άνθρωποι βλέπουν την εξ' αποστάσεως εκπαίδευση ως πολύπλοκη δια-δραστική διδασκαλία. Στη πραγματικότητα η εξ' αποστάσεως εκπαίδευση είναι μια αρκετά εύκολη χρήση ηλεκτρονικών τεχνολογιών για τη δημιουργία μαθησιακών εμπειριών. Η εξ' αποστάσεως εκπαίδευση προσφέρει μια εναλλακτική λύση στις παραδοσιακές μεθόδους μάθησης. Οι εφαρμογές που χρησιμοποιούνται μπορεί να παρέχουν βίντεο, δια-δραστικά παιχνίδια, έτσι ώστε να παρακινεί τους εκπαιδευόμενους και να τους κινεί το ενδιαφέρον. Τα τελευταία χρόνια η δημοτικότητα των μαθημάτων της εξ' αποστάσεως εκπαίδευσης έχει αυξηθεί σημαντικά και αυτό έχει σαν αποτέλεσμα τη διεύρυνση των διαδικτυακών μαθημάτων.

Η εξ' αποστάσεως εκπαίδευση επιτρέπει την αλληλεπίδραση προσφέροντας ταυτόχρονα δυνατότητες βίντεο και ήχου και μπορεί να συνδέσει τους μαθητές από απόσταση με άλλες τάξεις που διδάσκονται σε ένα διαδικτυακό φόρουμ.

Όταν οι εκπαιδευτικοί εξετάζουν το μέλλον της εκπαίδευσης, μία από τις λέξεις κλειδιά που θα χρησιμοποιηθούν είναι η καινοτομία.

Τα εξ' αποστάσεως μαθήματα είναι χρήσιμα, προσπελάσιμα και αξιοποιήσιμα για την απόκτηση αναγνωρισμένων και σεβαστών προσόντων σε παγκόσμιο επίπεδο. Υπάρχει ένα ευρύ φάσμα πλεονεκτημάτων της εξ' αποστάσεως εκπαίδευσης που το πιο σημαντικό είναι η ευελιξία. Οι εκπαιδευόμενοι μπορούν να ολοκληρώσουν οποιαδήποτε σειρά μαθημάτων επιθυμούν οπουδήποτε και οποτεδήποτε, καθιστώντας τα βολικά για όλους εκείνους που είναι πολυάσχολοι. Είναι λιγότερο δαπανηρά από τα παραδοσιακά μαθήματα και αυτό έχει σαν αποτέλεσμα η μάθηση να είναι προσιτή σε περισσότερο κόσμο.

Μπορούμε να χωρίσουμε την εξ' αποστάσεως εκπαίδευση σε δύο βασικούς τύπους: Τη Σύγχρονη και την Ασύγχρονη.

Σύγχρονη: Εκπαιδευτής και εκπαιδευόμενοι αλληλοεπιδρούν σε διαφορετικό χώρο αλλά στον ίδιο χρόνο. Η σύγχρονη εκπαίδευση μπορεί να περιλαμβάνει πολυμεσικές εφαρμογές όπως ομάδες συζητήσεων ομάδων (group chats), διαδικτυακά σεμινάρια και τηλεδιάσκεψη με ήχο και/ή βίντεο. Προτιμάται σε περιπτώσεις όπου είναι επιθυμητή η άμεση επικοινωνία και αλληλεπίδραση.

Ασύγχρονη: Εκπαιδευτής και εκπαιδευόμενοι αλληλοεπιδρούν σε διαφορετικό χώρο και χρόνο. Η ασύγχρονη εκπαίδευση μπορεί να περιλαμβάνει επικοινωνία μέσω (ηλεκτρονικής) αλληλογραφίας, πίνακες ανακοινώσεων και μαγνητοσκοπημένα ή ηχογραφημένα μηνύματα. Προτιμάται σε περιπτώσεις εκπαιδευόμενων που έχουν πολλές υποχρεώσεις και θέλουν να ορίσουν οι ίδιοι τον χρόνο εκπαίδευσης.

Η εξ αποστάσεως εκπαίδευση παρουσιάζει ορισμένα πλεονεκτήματα αλλά και μειονεκτήματα σε σχέση με τις παραδοσιακές μεθόδους διδασκαλίας. Πιο συγκεκριμένα, τα πλεονεκτήματα της εκπαίδευσης από απόσταση όπως αναλύουν και οι κκ (Τζιμόπουλος, et al , 2009) είναι τα εξής:

- Ευελιξία: Ο εκπαιδευόμενος έχει τη δυνατότητα να πραγματοποιήσει ένα μεγάλο μέρος ή ακόμα και το σύνολο της εκπαιδευτικής διαδικασίας στον χρόνο που θα επιλέξει.

- Ανεξαρτησία θέσης: Οι εκπαιδευόμενοι μπορούν να παρακολουθήσουν ένα μάθημα στο δικό τους περιβάλλον.

- Ίσες ευκαιρίες: Ακόμα και άτομα με αναπηρία ή κινητικά προβλήματα έχουν ίσες ευκαιρίες στην εξ αποστάσεως εκπαίδευση.

- Εξατομικευμένη μάθηση: Οι εκπαιδευόμενοι μπορούν, ως ένα βαθμό, να μάθουν με τον δικό τους ρυθμό με τα δικά τους μέσα (υπολογιστή, σύνδεση στο διαδίκτυο) και με υλικό που απευθύνεται αποκλειστικά σε αυτούς.

- Περισσότερες επιλογές: Οι εκπαιδευόμενοι μπορούν να παρακολουθήσουν περισσότερα μαθήματα χωρίς να φοβούνται ότι οι ώρες παρακολούθησης θα συμπίπτουν.

- Λιγότερα λειτουργικά έξοδα: για μετακινήσεις μαθητών και εκπαιδευτικών, αγορά επιπλέον εξοπλισμού, δημιουργία λιγότερων αιθουσών μια και αυτές αντικαθίστανται πλέον από τις εικονικές τάξεις.

Ωστόσο, η εξ αποστάσεως εκπαίδευση έχει και ορισμένα μειονεκτήματα:

- Απαιτεί αυτοπειθαρχία και σωστή διαχείριση χρόνου: Σε μικρές ηλικίες αυτό είναι πιο δύσκολο να επιτευχθεί σε αντίθεση με την εκπαίδευση ενηλίκων.

- Ατομικό κόστος: Η αγορά του κατάλληλου εξοπλισμού είναι πιο ακριβή από το να παρακολουθήσει κανείς ένα μάθημα με την παραδοσιακή μέθοδο διδασκαλίας.

- Ικανότητα χρήσης Η/Υ και εξοικείωση με το Διαδίκτυο: θα πρέπει να αποτελούν προαπαιτούμενο ώστε να είναι αποτελεσματική η εξ αποστάσεως εκπαίδευση.

- Προβλήματα σύνδεσης ή εξοπλισμού: Μπορούν να αποτελέσουν σημαντικό εμπόδιο στην ομαλή διεξαγωγή του μαθήματος.

Παρόλα αυτά η εξ αποστάσεως εκπαίδευση, όπως αναφέραμε, αποτελεί ένα νέο μοντέλο επιμόρφωσης που συνεχώς κερδίζει όλο και περισσότερους υποστηρικτές και ανάμεσά τους:

1. Εκπαιδευτικά κέντρα που οργανώνουν σεμινάρια (για επιχειρήσεις, ιδιώτες)

2. Εκπαιδευτές που προσφέρουν σεμινάρια

3. Επιχειρήσεις κάθε τύπου που επιθυμούν να οργανώσουν την εσωτερική τους εκπαίδευση (εκπαίδευση και κατάρτιση εργαζομένων)

4. Πανεπιστήμια.

Η σπουδαιότητα της έννοιας της Πληροφορίας αλλά και των ενεργειών που την συνοδεύουν γίνεται ξεκάθαρη από το Σύνταγμα της Ελλάδας (Σύνταγμα της Ελλάδας, 2008) στο άρθρο 5Α, παράγραφος 2 όπου αναφέρεται:

«Καθένας έχει δικαίωμα συμμετοχής στην Κοινωνία της Πληροφορίας. Η διευκόλυνση της πρόσβασης στις πληροφορίες που διακινούνται ηλεκτρονικά , καθώς και της παραγωγής, ανταλλαγής και διάδοσης τους αποτελεί υποχρέωση του Κράτους , τηρουμένων πάντοτε των εγγυήσεων των άρθρων 9 , 9Α και 19.»

Η πολιτεία ήδη έχει υλοποιήσει και συνεχίζει να υλοποιεί δράσεις που σχετίζονται με Ηλεκτρονική Τηλεκπαίδευση σε διάφορες βαθμίδες με επίκεντρο την ακαδημαϊκή κοινότητα όπου σε όλα τα ακαδημαϊκά ιδρύματα έχει υλοποιηθεί ένα σύστημα Ηλεκτρονικής Τηλεκπαίδευσης, πχ. Στο Πανεπιστήμιο Κρήτης υπάρχει το σύστημα MOODLE όπου προσφέρεται κατ' ελάχιστο το υλικό των μαθημάτων.

Στη Πρωτοβάθμια και Δευτεροβάθμια εκπαίδευση γίνονται διάφορες προσπάθειες επιμόρφωσης οι οποίες αφορούν κατά κύριο λόγο τους εκπαιδευτικούς και όχι τους μαθητές (Γώγουλος, Γ. et al , 2001)

2.2 Πληροφοριακά συστήματα

Για την ορθή ωστόσο παρουσίαση όλης της πληροφορίας που χρησιμοποιείται στην περίπτωση της εξ αποστάσεως εκπαίδευσης είναι απαραίτητη η ύπαρξη και σωστή χρήση πληροφοριακών συστημάτων.

Πληροφοριακό σύστημα είναι σύνολο από συνιστώντα στοιχεία που αλληλοεπιδρούν για να παράγουν πληροφορία. Η τεχνολογία των πληροφοριών αναφέρεται στις διαδικασίες, τις πρακτικές ή τα συστήματα που διευκολύνουν την επεξεργασία και τη μεταφορά πληροφοριών (Ken Kennedy, 1997). Αναμφίβολα, σήμερα οι περισσότεροι είναι πολύ εξοικειωμένοι με τα σύγχρονα συστατικά της τεχνολογίας των πληροφοριών. Ένα πληροφοριακό σύστημα μπορεί να οριστεί ως ένα σύνολο ανθρώπων, δεδομένων, τεχνολογίας και οργανωτικών μεθόδων που δουλεύουν μαζί για να συλλέξουν. να επεξεργαστούν. να αποθηκεύουν και να μεταβιβάσουν πληροφορίες για να στηρίξουν τη λήψη αποφάσεων και τον έλεγχο.

Οι κατηγορίες των συνιστώντων στοιχείων ενός πληροφοριακού συστήματος είναι πέντε:

1. Υλικό ηλεκτρονικών υπολογιστών - hardware
2. Λογισμικό - software
3. Δεδομένα - data
4. Διαδικασίες - procedures (π.χ. για την χρήση αλλά και τη διαχείριση του πληροφοριακού συστήματος)
5. Άνθρωποι - people

Η ιστορία των πληροφοριακών συστημάτων συμπίπτει με την ιστορία της επιστήμης των υπολογιστών, που άρχισε πολύ πριν από τη σύγχρονη επιστήμη της επιστήμης των υπολογιστών που εμφανίστηκε στον εικοστό αιώνα. . Όσον αφορά την κυκλοφορία των πληροφοριών και των ιδεών, πολλά κληροδοτούμενα πληροφοριακά συστήματα εξακολουθούν να υπάρχουν ακόμη και σήμερα, ενώ ανανεώνονται συνεχώς για να προωθήσουν εθνογραφικές προσεγγίσεις, να εξασφαλίσουν την ακεραιότητα των δεδομένων και να βελτιώσουν την κοινωνική αποτελεσματικότητα και αποδοτικότητα της όλης διαδικασίας. Σε γενικές γραμμές, τα

πληροφοριακά συστήματα επικεντρώθηκαν στην επεξεργασία των πληροφοριών εντός των οργανισμών, ιδίως στο πλαίσιο των επιχειρήσεων, και στο διαμοιρασμό των οφελών με την κοινωνία. (Wikipedia, 2018)

Κάθε πληροφοριακό σύστημα επιβάλλεται να προσδιορίζει, αποδοτικά και αποτελεσματικά, τις ανθρώπινες ανάγκες αυτών που το χρησιμοποιούν καθώς και να επεξεργάζεται όλες τις πληροφορίες έχοντας ως αποτέλεσμα την ικανοποίηση αυτών των αναγκών.

Είναι σημαντικό να γίνει αντιληπτό ότι τα πληροφοριακά συστήματα αναπτύσσονται για να βοηθήσουν τους χρήστες του στην επίτευξη των στόχων τους. Ενώ ίσως φαίνεται προφανές δεν γίνεται πάντοτε έτσι καθώς η πρόκληση να εφαρμοσθεί η νέα τεχνολογία γίνεται συχνά ως αυτοσκοπός ή για να παρουσιάσει η επιχείρηση/ οργανισμό/ εκπαιδευτικό ίδρυμα ένα νεωτερικό χαρακτήρα ή για να αντιγράψει άλλες ιδέες. Αντίθετα θα πρέπει να διερευνά τον στόχο του πληροφοριακού συστήματος, την χρησιμότητά του, τη σχέση κόστους/οφέλους που θα έχει. Δηλαδή, θα πρέπει το κάθε πληροφοριακό σύστημα να εξετάζεται μέσα από την οπτική της κάλυψης των εκπαιδευτικών αναγκών.

Η σημασία των πληροφοριακών συστημάτων σήμερα στους οργανισμούς αυξάνεται. Το γεγονός αυτό δημιουργεί την ανάγκη να υπάρχει η γνώση έτσι ώστε να μπορεί κανείς να είναι ενημερωμένος και αποτελεσματικός χρήστης προϊόντων και υπηρεσιών πληροφορικής τεχνολογίας. Δηλαδή, να μπορεί να διατυπώνει τις σχετικές ερωτήσεις, να αντιλαμβάνεται τις απαντήσεις και να λαμβάνει στη συνέχεια τις σωστές αποφάσεις σχετικά με τα πληροφοριακά συστήματα.

2.2.1 Πληροφοριακά συστήματα στην εξ αποστάσεως εκπαίδευση

Ειδικότερα, η Ασύγχρονη εξ αποστάσεως εκπαίδευση αποτελεί το βασικό ενισχυτικό παράγοντα μίας αποτελεσματικής και εκσυγχρονισμένης οργανωτικής δομής, συνιστούμενης από δρώσες οντότητες (φυσικά πρόσωπα, διαδικασίες, πληροφοριακά συστήματα κλπ), και από τις λειτουργικές τους αλληλεπιδράσεις. Οι πλατφόρμες είναι ολοκληρωμένα Σύστηματα Διαχείρισης Ηλεκτρονικών Μαθημάτων και αποτελούν προτάσεις του Ακαδημαϊκού Διαδικτύου για την υποστήριξη της Υπηρεσίας Ασύγχρονης εξ αποστάσεως εκπαίδευσης. Έχουν σχεδιαστεί με προσανατολισμό την ενίσχυση της συμβατικής Εκπαιδευτικής Διαδικασίας.

Οι πλατφόρμες ασύγχρονης εκπαίδευσης ή πλατφόρμες εικονικής εκμάθησης (Virtual Learning Environments) αποτελούν συστήματα λογισμικού που δίνουν τη δυνατότητα στον εκπαιδευτικό να επικοινωνεί με τους μαθητές του από απόσταση και σε μη πραγματικό χρόνο για την παροχή του εκπαιδευτικού υλικού που απαιτείται για τη διεξαγωγή του μαθήματος. Οι περισσότερες από τις πλατφόρμες αυτές έχουν σαν στόχο, όχι απλώς την αναπαραγωγή της κλασσικής εκπαιδευτικής διαδικασίας σε περιβάλλον υπολογιστή, αλλά και την εκμετάλλευση της τεχνολογίας των υπολογιστών για την παροχή εξελιγμένων εργαλείων εκπαίδευσης σε μαθητές και καθηγητές, κάτι που συνεπάγεται συνολικά την αναβάθμιση της παρεχόμενης εκπαίδευσης.

Σήμερα, υπάρχουν πλήθος εμπορικά προγράμματα και εφαρμογές για την παροχή υπηρεσιών ασύγχρονης εξ αποστάσεως εκπαίδευσης. Επίσης, υπάρχει πολύ μμεγάλος αριθμός συστημάτων που έχουν σχεδιαστεί στη μμεγάλη τους πλειοψηφία από εκπαιδευτικά ιδρύματα και διατίθενται ελεύθερα (open –source) όπως οι δημοφιλείς πλατφόρμες ανοιχτού λογισμικού Moodle, Chamilo, Sakai 11 και Dokeos.

Σχεδόν το σύνολο των συστημάτων ασύγχρονης εξ αποστάσεως εκπαίδευσης που είναι σήμερα διαθέσιμα, βασίζονται στην αρχιτεκτονική πελάτη-εξυπηρετητή (client-server). Αυτό σημαίνει ότι ένας τερματικός υπολογιστής (client) χρησιμοποιεί έναν web browser για να έχει πρόσβαση σε ιστοσελίδες που είναι αποθηκευμένες σε έναν κεντρικό server.

Πιο αναλυτικά το Moodle (Modular Object Oriented Developmental Learning Environment) είναι ελεύθερο λογισμικό διαχείρισης μαθημάτων (Course Management System), ένα σύστημα διαχείρισης μάθησης Learning Management System (LMS) ή ένα σύστημα εικονικής μάθησης (Virtual Learning Environment – VLE), ή πιο απλά ένα πακέτο λογισμικού για τη διεξαγωγή ηλεκτρονικών μαθημάτων μέσω Διαδικτύου, που προσφέρει ολοκληρωμένες υπηρεσίες ασύγχρονης εξ αποστάσεως εκπαίδευσης. Δημιουργήθηκε το 1999 από τον Αυστραλό Martin Dougiamas ως τμήμα του PhD του και σύμφωνα με αυτόν, έχει δημιουργηθεί πάνω στη φιλοσοφία του κοινωνικού δομητισμού. Το Moodle παρέχεται δωρεάν ως ελεύθερο λογισμικό-λογισμικό ανοικτού κώδικα (κάτω από την GNU Public License) και μπορεί να τρέξει σε οποιοδήποτε σύστημα που υποστηρίζει PHP, ενώ έχει τη δυνατότητα να συνδυάζεται με πολλούς τύπους βάσεων δεδομένων (ιδιαίτερα MySQL). Χρησιμοποιείται κυρίως για τις ανάγκες της ασύγχρονης εξ αποστάσεως εκπαίδευσης. Μέχρι στιγμής έχει περισσότερους από 200.000 εγγεγραμμένους οργανισμούς και χρήστες ενώ διατίθεται μεταφρασμένο σε περισσότερες από 75 γλώσσες. (Wikipedia, 2019) (Moodle, 2019)

Το Chamilo είναι και αυτό ένα Learning Management System (LMS) το οποίο είναι ένα λογισμικό ανοιχτού κώδικά.

Το Chamilo μπορεί να εγκατασταθεί σε οποιοδήποτε server που υποστηρίζει PHP και SQL database. Το περιβάλλον χρήστη είναι προσβάσιμο από οποιοδήποτε browser (Internet explorer, Chrome, Mozilla, Safari, κ.ά.) και έτσι δεν απαιτεί την εγκατάσταση και άλλων προγραμμάτων. Τέλος, είναι συμβατό με όλους τους τύπους λειτουργικών συστημάτων (Windows, Linux, MacOS).

Το Chamilo χρησιμοποιείται από Κυβερνήσεις, ιδιωτικές εταιρείες, δημόσια και ιδιωτικά Πανεπιστήμια, Μη-κυβερνητικές οργανώσεις και από άλλους τύπους οργανισμών για απλή ζωντανή εκπαίδευση μέχρι πλήρως αναγνωρισμένη εξ αποστάσεως εκπαίδευσης επίσης και ως ηλεκτρονικό κατάστημα μαθημάτων αλλά και ως εργαλείο διαχείρισης ανθρώπινου δυναμικού από εταιρείες. Αυτή τη στιγμή υπάρχουν πάνω από 3.500.000 ενεργοί χρήστες παγκοσμίως.

Μπορεί επίσης να χρησιμοποιηθεί και για mobile learning, καθώς είναι συμβατό με όλες τις συσκευές τηλεφώνου. (Medion7, 2019)

Το Sakai (https://sakaiproject.org/) είναι μια ομάδα εργαλείων ανοικτού κώδικα που χρησιμοποιούνται σε online μαθησιακά περιβάλλοντα. Διατίθεται δωρεάν, βασίζεται σε λογισμικό ανοικτού και ελεύθερου κώδικα και αναπτύχθηκε από την κοινότητα Sakai. Το κάθε εκπαιδευτικό ίδρυμα μπορεί να επιλέξει, από το σύνολο των προσφερόμενων εργαλείων, εκείνα που ανταποκρίνονται στις απαιτήσεις που θέλει να ικανοποιήσει.

Εργαλεία επικοινωνίας που υποστηρίζονται είναι τα chat room, το email, το dropbox, οι ανοιχτές συζητήσεις, πεδία ανακοινώσεων που χρησιμοποιούνται για την εισαγωγή νέων και χρήσιμων αρχείων και ομαδικές συζητήσεις.

Ο εκπαιδευτικός μπορεί να διατηρεί βαθμολόγιο (gradebook) με τη βαθμολογία όλων των εκπαιδευομένων και παρατηρήσεις που αφορούν την πρόοδό τους. Επιπλέον, χρησιμοποιώντας τα ενσωματωμένα στατιστικά εργαλεία μπορεί να εξάγει συμπεράσματα για την εκπαιδευτική διαδικασία γενικά ή και για κάθε μαθητή ξεχωριστά. Οι καθηγητές και οι εκπαιδευόμενοι έχουν πρόσβαση σε διαμοιραζόμενο ημερολόγιο, ενώ ο κάθε χρήστης διαθέτει και προσωπική σελίδα με τα μαθήματα στα οποία συμμετέχει και με την ηλεκτρονική αλληλογραφία που έχει λάβει.

Όσον αφορά τα εργαλεία μάθησης ο εκπαιδευόμενος έχει στη διάθεσή του τεστ αξιολόγησης, γλωσσάρι, πίνακες και σχεδιαγράμματα. Επίσης, προσφέρονται εξειδικευμένα εγχειρίδια χρήσης που επεξηγούν τη λειτουργικότητα του συστήματος.

Τέλος, υπό ανάπτυξη βρίσκονται νέα εκπαιδευτικά εργαλεία ή αυτά προσφέρονται από τρίτους οργανισμούς (third part modules) όπως το SCORM, το blog tool, υπηρεσίες multipoint audio και διαμοιραζόμενου ασπροπίνακα.

Το Sakai μπορεί να υποστηρίξει επιτυχώς κάθε δραστηριότητα που μπορεί να χρειαστεί επικοινωνία, συνεργασία και διαμοίραση της γνώσης μεταξύ των χρηστών της πλατφόρμας. Τέλος, να σημειωθεί ότι έχει δοθεί βαρύτητα ώστε να είναι εύχρηστο και προσβάσιμο και από άτομα με κάποια αναπηρία. (Τεχνολογίες και Πρότυπα για την Υποστήριξη Εκπαιδευτικών Περιβαλλόντων Διαδικτύου, 2019)

Το Dokeos (http://www.dokeos.com/) είναι ένα περιβάλλον ηλεκτρονικής μάθησης, διαδικτυακής διαχείρισης μαθημάτων και εργαλείο συνεργασίας. Διατίθεται δωρεάν και είναι λογισμικό ανοιχτού κώδικα. Είναι γραμμένο στη γλώσσα προγραμματισμού PHP και χρησιμοποιεί την MySQL για τη διαχείριση των βάσεων δεδομένων του. Είναι βασισμένο στο cloud και χαρακτηρίζεται ως Software as a Service (SaaS).

Οι δυνατότητες του Dokeos περιλαμβάνουν τη διαμοίραση εκπαιδευτικού υλικού, τη διατήρηση χρονοδιαγράμματος του μαθήματος, παρακολούθηση της προόδου των μαθητών, τη συμμετοχή σε συνεδρίες chat με κείμενο, ήχο και βίντεο και την πραγματοποίηση διαγωνισμάτων και τεστ. Επιπλέον, ο καθηγητής μπορεί να καθορίσει ένα γνωστικό μονοπάτι μέσα στο υλικό, το οποίο μπορούν να ακολουθήσουν οι μαθητές ώστε να φθάσουν ταχύτερα και περισσότερο αποδοτικά στον εκπαιδευτικό στόχο. Ακόμη, υποστηρίζονται όλων των ειδών τα έγγραφα και το κάθε μάθημα διαθέτει μια ψηφιακή θυρίδα στην οποία μπορεί ο μαθητής να αποστείλει την εργασία του. Η εφαρμογή Dokeos διαθέτει χώρους συζήτησης, πίνακες ανακοινώσεων, υπερσυνδέσεις προς άλλες ιστοσελίδες και δυνατότητες συνεργασίας των εκπαιδευομένων σε ομάδες.

Τέλος, το Dokeos προσφέρει δυνατότητες τηλεδιάσκεψης, αυτόματης αξιολόγησης μέσω Η/Υ, συγγραφής εκπαιδευτικού blog, αλλά και δημιουργία εκπαιδευτικών παιχνιδιών. Οι καθηγητές μπορούν να οργανώσουν τα μαθήματά τους με βάση κάποια παιδαγωγικά προσχέδια.

Πρέπει, ωστόσο, να σημειωθεί ότι οι υπηρεσίες τηλεδιάσκεψης προσφέρονται με χρέωση. (Τεχνολογίες και Πρότυπα για την Υποστήριξη Εκπαιδευτικών Περιβαλλόντων Διαδικτύου, 2019)

2.2.2 Ασφάλεια Πληροφοριακών Συστημάτων

Ασφάλεια Πληροφοριακού Συστήματος είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του ΠΣ αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή.

Ότι αξίζει να προστατευθεί ονομάζεται αγαθό. Τα αγαθά αξίζει να προστατευθούν επειδή έχουν αξία. Η αξία τους μπορεί να μειωθεί αν υποστούν ζημιά. Τα αγαθά είναι δύο ειδών. Η Πληροφορία ή τα Δεδομένα και οι υπολογιστικοί πόροι που χρησιμοποιούμε για να τα επεξεργαστούμε. Σύστημα είναι ένας αριθμός αλληλοεπιδρώντων στοιχείων, που οργανικά συναρμολογημένα σε μία ολότητα μπορούν να εκτελούν μία ορισμένη λειτουργία. Πληροφοριακό Σύστημα (Π.Σ) είναι ένα οργανωμένο σύνολο από πέντε στοιχεία (άνθρωποι, λογισμικό, υλικό, διαδικασίες και δεδομένα), τα οποία αλληλοεπιδρούν μεταξύ τους και με το περιβάλλον, με σκοπό την παραγωγή και διαχείρισης πληροφορίας, για την υποστήριξη των ανθρωπίνων δραστηριοτήτων, στα πλαίσια του οργανισμού. Ασφάλεια Π.Σ είναι το οργανωμένο πλαίσιο από έννοιες, αντιλήψεις, αρχές, πολιτικές, διαδικασίες, τεχνικές και μέτρα που απαιτούνται για να προστατευθούν τα στοιχεία του ΠΣ αλλά και το σύστημα ολόκληρο, από κάθε σκόπιμη ή τυχαία απειλή. Στο επόμενο κεφάλαιο θα αναλύσουμε πως θα πρέπει να ασφαλίσουμε ένα Π.Σ με τις τεχνικές της Ταυτοποίησης Αυθεντικοποίησης.

Σχολεία, κολλέγια και Πανεπιστήμια εισέρχονται σιγά σιγά στην επανάσταση των βιομετρικών στοιχείων. Για να εξασφαλιστεί ότι μόνο οι εγκεκριμένοι μαθητές αποκτούν πρόσβαση σε δραστηριότητες όπως η εγγραφή, η παρακολούθηση βιβλίων, Online πρόσβαση στη βιβλιοθήκη κτλ, τα βιομετρικά συστήματα χρησιμοποιούν μια ποικιλία φυσικών και συμπεριφορικών χαρακτηριστικών που λαμβάνονται από ένα άτομο. Αυτά μπορεί να περιλαμβάνουν: δακτυλικό αποτύπωμα, πρόσωπο, ίριδα, υπογραφή, μοτίβο φωνής, φλέβα, ακόμα και το DNA για να καθοριστεί η ταυτότητα. Χρησιμοποιώντας περισσότερο από ένα βιομετρικό σύστημα μπορεί να βελτιώσει την ακρίβειά του. Δεν υπάρχει ένα μοναδικό βιομετρικό σύστημα που να είναι ιδανικό.

Ένα είναι σίγουρο, το μέλλον της ασφάλειας των πληροφοριακών συστημάτων ξεκινά από τα συστήματα βιομετρικής αναγνώρισης.

2.3 Βιομετρικές τεχνολογίες

2.3.1 Ορισμός

Σύμφωνα με τον Wayman Jame οι "βιομετρικές τεχνολογίες" είναι αυτοματοποιημένες μέθοδοι επαλήθευσης ή αναγνώρισης την ταυτότητα ενός ζωντανού ατόμου που βασίζεται σε ένα φυσιολογικό ή συμπεριφορικό χαρακτηριστικό. (Wayman et al, 2005)

Οι Βιομετρικές Τεχνολογίες είναι η επιστήμη της ανίχνευσης και της αναγνώρισης των ανθρωπίνων χαρακτηριστικών, με τη μέτρηση και την ανάλυση βιολογικών δεδομένων με τη χρήση ηλεκτρονικών τεχνολογιών. Η χρήση Βιομετρικών Τεχνολογιών είναι ένας γρήγορος και αποτελεσματικός τρόπος για να συνδεθούμε χωρίς να πρέπει να θυμόμαστε ένα κωδικό πρόσβασης. Οι Βιομετρικές Τεχνολογίες παρέχουν προστασία της ταυτότητας ενός ατόμου και ενισχύουν την ασφάλεια σχετικά με τη κλοπή της.

2.3.2 Κυρίαρχες βιομετρικές τεχνολογίες (δακτυλικά, πρόσωπο κλπ)

- Πρόσωπο: Βασίζεται στον υπολογιστή για την αυτόματη αναγνώριση ή επαλήθευση ενός ατόμου από ψηφιακές εικόνες ή εικόνες βίντεο, συγκρίνοντας τις επιλεγμένες λειτουργίες προσώπου στην ζωντανή εικόνα και τη βάση δεδομένων προσώπου.

- Δακτυλικό αποτύπωμα: Το βιομετρικό σύστημα παίρνει μια εικόνα των δακτύλων ενός ατόμου και καταγράφει τα χαρακτηριστικά του. Αυτές οι πληροφορίες μπορεί στη συνέχεια να επεξεργαστούν ή να αποθηκευτούν ως εικόνα ή ως κωδικοποιημένος αλγόριθμος υπολογιστή για σύγκριση με άλλα αρχεία δακτυλικών αποτυπωμάτων. Αυτή η τεχνική βρίσκει εφαρμογές στην επιβολή του νόμου, την πρόληψη της απάτης και την πρόσβαση στον υπολογιστή.

- Φωνή: Είναι η διαδικασία καθορισμού του καταχωρημένου ομιλητή που παρέχει μια συγκεκριμένη φράση ή "φωνητικό αποτύπωμα". Η αναγνώριση φωνής ή ομιλητών χρησιμοποιεί φωνητικά χαρακτηριστικά για την ταυτοποίηση ατόμων με τη χρήση φράσης πρόσβασης (κωδικός πρόσβασης)

- Παλάμη: Η φλεβική φλέβα είναι ένα από τα πιο ασφαλή βιομετρικά στοιχεία και είναι το πρώτο σύστημα επαφής προσωπικού επαφής στον κόσμο. Λειτουργεί καταγράφοντας την εικόνα του μοτίβου της φλέβας ενός ατόμου ενώ ακτινοβολεί με ακτίνες κοντά στην υπέρυθρη ακτινοβολία. Η ειδικότητά του είναι ότι μπορεί να ανιχνεύσει το μοτίβο της φλέβας στην ανθρώπινη παλάμη με μεγάλη ακρίβεια. Όταν ο αισθητήρας εκπέμπει ακτίνες υπέρυθρης ακτινοβολίας προς την παλάμη του χεριού, το αίμα που ρέει μέσω αυτών πίσω στην καρδιά με μειωμένο οξυγόνο απορροφά την ακτινοβολία και προκαλεί την εμφάνιση των φλεβών ως ένα μαύρο μοτίβο. Αυτό το πρότυπο καταγράφεται και αποθηκεύεται σε κρυπτογραφημένη μορφή σε μια βάση δεδομένων, ένα διακριτικό ή μια έξυπνη κάρτα ως αναφορά για μελλοντική σύγκριση

- Γεωμετρία χεριών: Περιλαμβάνει τη μέτρηση και την ανάλυση του σχήματος του χεριού. Είναι μια αρκετά απλή διαδικασία και είναι εκπληκτικά ακριβής. Αν και απαιτεί ειδικό υλικό για χρήση, μπορεί εύκολα να ενσωματωθεί σε άλλες συσκευές ή συστήματα. Σε αντίθεση με τα δακτυλικά αποτυπώματα, το ανθρώπινο χέρι δεν είναι μοναδικό. Τα μεμονωμένα χαρακτηριστικά χεριού δεν είναι αρκετά περιγραφικά για την αναγνώριση. Ωστόσο, είναι δυνατόν να σχεδιαστεί μια μέθοδος συνδυάζοντας διάφορα μεμονωμένα χαρακτηριστικά και μετρήσεις των δακτύλων και των χεριών για λόγους επαλήθευσης.

- Ίρις: Συνδυάζει την όραση του υπολογιστή, την αναγνώριση προτύπων, το στατιστικό συμπέρασμα και την οπτική. Σκοπός του είναι η αναγνώριση σε πραγματικό χρόνο της υψηλής ταυτότητας ενός ατόμου με μαθηματική ανάλυση των τυχαίων μοτίβων που είναι ορατά μέσα στην ίριδα του οφθαλμού από κάποια απόσταση. Οι σκάνες Iris είναι εξαιρετικά ακριβείς.

- Σάρωση αμφιβληστροειδούς: Η σάρωση αναλύει το στρώμα των αιμοφόρων αγγείων στο πίσω μέρος του ματιού. Περιλαμβάνει τη χρήση πηγής φωτός χαμηλής έντασης και οπτικού συζευκτήρα και μπορεί να διαβάσει τα σχέδια με μεγάλη ακρίβεια. Απαιτεί από τον χρήστη να αφαιρέσει γυαλιά, να τοποθετήσει το μάτι κοντά στη συσκευή και να

εστιάσει σε ένα συγκεκριμένο σημείο. Οι συσκευές σάρωσης αμφιβληστροειδούς είναι μεγάλες επιλογές μακροπρόθεσμης και υψηλής ασφάλειας.

- DNA: Ανεξάρτητα από αυτές τις βασικές διαφορές, το DNA είναι ένας τύπος βιομετρικού δεδομένου ότι είναι η χρήση ενός φυσιολογικού χαρακτηριστικού για την επαλήθευση ή τον προσδιορισμό της ταυτότητας. Ο έλεγχος DNA είναι μια τεχνολογία με υψηλό βαθμό ακρίβειας, ωστόσο, η πιθανότητα δειγματοληψίας μόλυνσης και υποβάθμισης θα επηρεάσει την ακρίβεια της μεθόδου

- Υπογραφή: είναι η διαδικασία που χρησιμοποιείται για την αναγνώριση της χειρόγραφης υπογραφής ενός ατόμου. Χρησιμοποιεί τη βιομετρική συμπεριφορά μιας χειρόγραφης υπογραφής για να επιβεβαιώσει την ταυτότητα ενός χρήστη υπολογιστή. Αυτό γίνεται με την ανάλυση του σχήματος, της ταχύτητας, του εγκεφαλικού, της πίεσης και της χρονικής πληροφορίας κατά τη διάρκεια της πράξης υπογραφής.

- Βάδισμα: βασίζεται στον τρόπο με τον οποίο περπατάει ένα άτομο. Είναι ένας βιομετρικός τύπος συμπεριφοράς. Δεν επηρεάζεται από την ταχύτητα του περιπάτου του ατόμου.

- Πληκτρολόγηση: Ο τρόπος και ο ρυθμός με τον οποίο αναλύονται οι χαρακτήρες μεμονωμένων τύπων για την ανάπτυξη ενός μοναδικού βιομετρικού προτύπου του χρήστη που πληκτρολογεί πρότυπο για μελλοντική πιστοποίηση. Χρησιμοποιείται για την επαλήθευση ή ακόμα και για τον προσδιορισμό της ταυτότητας του ατόμου που παράγει αυτές τις πληκτρολογήσεις.

2.3.3 Εφαρμογές των βιομετρικών συστημάτων

Σχεδιάζοντας ένα σύστημα όπου είναι κρίσιμο το άτομο που αποκτά πρόσβαση είναι το εξουσιοδοτημένο πρόσωπο η βιομετρία είναι μια λογική επιλογή. Υπάρχουν αρκετές ιδέες/προτάσεις για το σχεδιασμό ενός τέτοιου συστήματος όπως μας περιγράφουν και οι Καμπουράκης Γεώργιος στο άρθρο του Security and Privacy in m-learning and beyond: Challenges and state of the art. το 2013, οι González-Agulla, Elisard στα άρθρα τους Development and Implementation of a Biometric Verification System for E-learning Platforms, 2004, οι Asha, S., και C. Chellappan (Asha et al , 2008) και οι Kang, Byeong Ho, and Hyejin Kim (Kang et al, 2015).

Όμως όπως χαρακτηριστικά αναφέρουν οι Castiglione, Aniello και Sayed, Mohamed, και Farid Jradi (Sayed, Mohamed et al, 2014) υπάρχουν ακόμη πολλοί τομείς και περιθώρια έρευνας και ανάπτυξης όπως η τελειοποίηση των αλγορίθμων βιομετρικών συστημάτων και όπως και στην περίπτωσή της διατριβής, η αξιοποίηση απλών και προσιτών μέσων (κάμερα Η/Υ) καθιστώντας τις βιομετρικές τεχνολογίες οικονομικά αποδοτικές, κλιμακούμενες, αξιόπιστες, ανεξάρτητες εξειδικευμένου υλικού και σε θέση να παρέχουν βελτιωμένη ασφάλεια οποιαδήποτε στιγμή και οπουδήποτε.

2.3.4 Βιομετρικά συστήματα σε σχέση με τα παραδοσιακά συστήματα αναγνώρισης

Τα πιο σημαντικά και συνηθισμένα προβλήματα που αντιμετωπίζουν οι χρήστες χρησιμοποιώντας τα κοινά συστήματα ασφαλείας έχουν ένα κοινό παρονομαστή, βασίζονται σε κωδικούς ή κάρτες.

Τόσο οι κωδικοί όσο και οι κάρτες μπορούν πολύ εύκολα είτε να ξεχαστούν είτε να χαθούν αντίστοιχα. Ακόμη, μη εξουσιοδοτημένα άτομα θα μπορούσαν παράνομα να κατέχουν τα στοιχεία εισόδου ενός χρήστη και να αποκτήσουν παράνομα πρόσβαση σε προσωπικά του δεδομένα ή υπηρεσίες.

Όμως υπάρχουν κάποια βασικά χαρακτηριστικά, πιο σημαντικά, των βιομετρικών συστημάτων που τα κάνουν να ξεχωρίζουν από τα παραδοσιακά συστήματα αναγνώρισης όπως η ακρίβεια, το ποσοστό αναγνώρισης ενός εξουσιοδοτημένου προσώπου από ένα μη εξουσιοδοτημένο, η ταχύτητα αναγνώρισης ενός ατόμου από το σύστημα και η αξιοπιστία του συστήματος αναφερόμενοι στη απρόσκοπτη και με ακρίβεια λειτουργία ενός συστήματος με πολύ μικρότερο κόστος και πόρους τόσο για τη λειτουργία όσο και για την εποπτεία του. Ακόμη ο χρόνος επεξεργασίας των δεδομένων ενός χρήστη επηρεάζεται από τις παραμέτρους της αποθήκευσης δεδομένων, της επεξεργασίας τους, της διαδικασίας καταχώρησής των δεδομένων σε ένα σύστημα βιομετρικής αναγνώρισης με πολύ θετικό ισοζύγιο απέναντι στα παραδοσιακά συστήματα αναγνώρισης.

Τέλος θα πρέπει να αναφέρουμε ότι στα βιομετρικά συστήματα παίζει σημαντικό ρόλο η μη δυνατότητα εισόδου σε μη εξουσιοδοτημένο προσωπικό. Για την επίτευξη της μη εισόδου

χρειάζεται μεγάλη ακρίβεια του βιομετρικού χαρακτηριστικού. Με αυτό τον τρόπο μειώνονται ραγδαία οι πιθανότητες παραποίησης των στοιχείων κάποιου χρήστη.

2.3.5 Πλεονεκτήματα συστημάτων βιομετρικής πιστοποίησης χρηστών

Χρησιμοποιώντας τέτοιες μεθόδους ασφαλείας, μέσω βιομετρικών συστημάτων, θα πρέπει να λάβουμε υπόψιν μας ότι διευκολύνεται η ζωή μας απαλλάσσοντάς μας από την απομνημόνευση κωδικών ή τη συνεχή σκέψη να μην ξεχάσουμε την κάρτα μας για την πρόσβαση. Μόνο με ένα σωματικό μας χαρακτηριστικό, το οποίο δεν μεταβάλλεται στο χρόνο και αποτελεί και μοναδικό στον κόσμο, έχουμε πρόσβαση στους επιτρεπόμενους χώρους. Παρόλα όμως τα θετικά υπάρχουν και αρνητικά στοιχεία όπως η απώλεια της ιδιωτικότητας. Παρακάτω θα ακολουθήσουν ενδεικτικά μειονεκτήματα και πλεονεκτήματα την βιομετρικών συστημάτων πρόσβασης.

- Δεν απαιτούν τη χρήση κάρτας, κωδικού πρόσβασης ή οποιαδήποτε άλλης συσκευής.
- Η αναγνώριση γίνεται με φυσικά χαρακτηριστικά και δεν απαιτείται η διαρκής ύπαρξη διαχειριστή για την ενημέρωση του συστήματος.
- Χαμηλό κόστος προμήθειας και συντήρησης.
- Χαμηλοί χρόνοι απόκρισης.
- Δεν απαιτούν διαρκή ανανέωση τα χαρακτηριστικά με την πάροδο του χρόνου.
- Σύντομη διαδικασία καταχώρησης.

2.3.6 Προβλήματα στατικής ταύτισης / μειονεκτήματα

Τα κυριότερα μειονεκτήματα των βιομετρικών συστημάτων αναγνώρισης παρουσιάζονται σε ηθικά θέματα που προκύπτουν εξαιτίας της άγνοιας των χρηστών. Πιο συγκεκριμένα κάποιοι από τους παράγοντες που επηρεάζουν αρνητικά τα βιομετρικά συστήματα θα μπορούσαμε να πούμε ότι είναι

- Η αντίληψη του συνόλου του κόσμου ότι η λήψη δακτυλικού αποτυπώματα συνάδει και με διάπραξη εγκληματικής ενέργειας.

- Η αντίληψη ότι η εκπεμπόμενη ακτινοβολία βλάπτει την υγεία.

- Η αντίληψη άρσης της ιδιωτικότητας

Αυτοί οι παράγοντες ωστόσο μπορούν εύκολα να αντισταθμιστούν καθώς σε περιπτώσεις ασφάλειας των προσωπικών δεδομένων των χρηστών που θα χρησιμοποιηθούν όπως αναφέρει και οι De Silva, Sam, Anthony Liu, και L. L. P. Nabarro η λειτουργία των βιομετρικών συστημάτων πρέπει να εναρμονιστεί με τις αλλαγές του νέου κανονισμού προστασίας προσωπικών δεδομένων κάνοντας έτσι τους χρήστες να νιώσουν πιο ασφαλείς και πιθανόν και πιο οικείοι απέναντι στις νέες αυτές τεχνολογίες.

Βέβαια δεν υπάρχει κάποιο συγκεκριμένο κριτήριο για την μέτρηση της απόδοσης, αφού για κάθε βιομετρικό χαρακτηριστικό υπάρχουν άλλα τόσα κριτήρια. Υπάρχουν κάποιοι δείκτες όπου γίνεται η μέτρηση όπως

1. Δείκτης Λανθασμένης Αποδοχής (False Acceptance Rate, FAR). Τα αποτελέσματα εκφράζονται σε ποσοστιαία κλίμακα και δείχνουν το ποσοστό δύο διαφορετικών ατόμων να λαμβάνονται από το σύστημα ως ένα.

2. Δείκτης Λανθασμένης Απόρριψης (False Rejection Rate, FRR). Τα αποτελέσματα εκφράζονται σε ποσοστιαία κλίμακα και δείχνουν πως δυο χαρακτηριστικά ενός ατόμου λαμβάνονται από το σύστημα ως δυο διαφορετικά άτομα.

Οι δείκτες αυτοί χρησιμοποιούνται στα συστήματα πρόσβασης έχοντας ως σκοπό την ελαχιστοποίηση της πρόσβασης στο μη αρμόδιο προσωπικό. Η σχέση αυτών των δύο δεικτών

είναι αντιστρόφως ανάλογη. Αυτό σημαίνει ότι μειώνοντας τον FAR, δεν επιτρέπεται σε ένα άτομο να εισέλθει, όμως αυξάνοντας το FRR ενδέχεται ένα άτομο που του επιτρέπεται η πρόσβαση κανονικά, να χρειαστεί να γίνει λήψη αποτυπώματος παραπάνω από δυο φορές για να δημιουργηθεί το πρότυπο προς σύγκριση.

Για να φτάσουμε σε αυτό το σημείο θα πρέπει να λάβουμε σοβαρά υπόψιν τη δοκιμή αυτών των συστημάτων χρησιμοποιώντας παραμέτρους των παραπάνω δεικτών, με τεχνικές και εργαλεία όπως προτείνουν σε άρθρο τους και οι Poh, Norman, και Samy Bengio.

Υπάρχει και ένα ακόμη σύνολο δεικτών, το οποίο αποτελείται από τα παρακάτω:

1. Δείκτης τομής λανθασμένων εκτιμήσεων (Cross-over Error Rate, CER) ή Δείκτης σου σφάλματος (Equal Error Rate, EER). Τα αποτελέσματα εκφράζονται σε ποσοστιαία κλίμακα. Υπάρχει μια σύνδεση με τους προηγούμενους δύο δείκτες. Αποτελεί το σημείο τομής τους.

2. Δείκτης αποτυχίας εγγραφής (Failure to Enroll Rate, FER ή FTR). Αυτός ο δείκτης εκφράζει το ποσοστό που προσπάθησε κάποιος να εισάγει ένα πρότυπο κατά τη διαδικασία της εγγραφής. Ένας λόγος που δημιουργείται αδυναμία είναι η λήψη κακής ποιότητας προτύπου.

3. Δείκτης αποτυχίας λήψης (Failure To Capture Rate, FTC). Μετράει την αποτυχία εντοπισμού βιομετρικού χαρακτηριστικού χωρίς να υπάρχει πρόβλημα στο εν λόγω χαρακτηριστικό.

4. Χωρητικότητα προτύπου (template capacity). Μετράει τον μέγιστο αριθμό δεδομένων που μπορούν να εισαχθούν στο σύστημα.

Κεφάλαιο 3
Σχεδιασμός / υλοποίηση του συστήματος αναγνώρισης προσώπου

3.1 Εισαγωγή

Η υλοποίηση του εργαλείου βασίστηκε στα εργαλεία ανοιχτού κώδικα face-api.js και tensorflow.js core τα οποία υλοποιούν πολλά CNN (Convolutional Neural Networks) για την επίλυση της ανίχνευσης προσώπων, της αναγνώρισης προσώπων και της ανίχνευσης ορόσημων προσώπων, βελτιστοποιημένων για τον ιστό και για κινητές συσκευές. Τα παραπάνω εργαλεία ήταν επίσης σε θέση να διασυνδεθούν με το σύστημα εξ αποστάσεως εκπαίδευσης moodle που χρησιμοποίησα για την κατασκευή του τελικού παραδοτέου πληροφοριακού συστήματος της εργασίας.

Μέχρι στιγμής, το face-api.js υλοποιούσε αποκλειστικά ένα CNN SSN Mobilenet v1 βασισμένο στο CNN για ανίχνευση προσώπου. Παρόλο που το SSD είναι αρκετά ακριβής ανιχνευτής προσώπου, δεν είναι τόσο γρήγορο (από την άποψη του χρόνου συμπερασμάτων) όσο άλλες αρχιτεκτονικές

και μπορεί να μην είναι δυνατόν να επιτευχθεί πραγματικός χρόνος με αυτόν τον ανιχνευτή προσώπου, εκτός αν εσείς / οι χρήστες του webapp έχουν μια αξιοπρεπή GPU. Όμως πολλές έρευνες δείχνουν ότι δεν χρειαζόμαστε πάντα αυτόν τον βαθμό ακρίβειας και μερικές φορές θα προτιμούσαμε να ανταλλάσσουμε την υψηλή ακρίβεια με αντάλλαγμα για έναν πολύ πιο γρήγορο ανιχνευτή προσώπου.

Εκεί μπαίνει στο παιχνίδι το MTCNN, το οποίο είναι τώρα διαθέσιμο στο face-api.js. Το MTCNN είναι ένας πολύ πιο ελαφρύς ανιχνευτής προσώπου. Στο παρακάτω θα επισημάνω, πώς συγκρίνεται με το SSD Mobilenet v1:

Πλεονεκτήματα:

- συντομότεροι χρόνοι συμπερασμάτων (ταχύτερη ταχύτητα ανίχνευσης)
- ταυτόχρονη ανίχνευση 5 σημείων ορόσημου προσώπου (παίρνουμε ευθυγράμμιση προσώπου δωρεάν)
- πολύ μικρότερο μέγεθος μοντέλου: μόνο ~ 2MB σε σύγκριση με ~ 6MB
- μπορεί να ρυθμιστεί: υπάρχουν μερικές παράμετροι που μπορείτε να συντονίσετε για να αυξήσετε την απόδοση για τις συγκεκριμένες απαιτήσεις σας

Μειονεκτήματα:

- λιγότερο ακριβή από το SSD Mobilenet v1

Η σύνοψη όλων των παραπάνω με οδήγησε στο να χρησιμοποιήσω τις παραπάνω βιβλιοθήκες στην υλοποίηση του συστήματος.

3.2 Μεθοδολογία

Η μεθοδολογία που ακολούθησα για την διεκπεραίωση της εργασίας χωρίζεται σε 7 φάσεις. Εξαιτίας της φύσης του θέματος της διατριβής θα επιλέξουμε να εργαστούμε ακολουθώντας το πλαίσιο software development lifecyle.

Το πλαίσιο αυτό καθορίζει τις εργασίες που εκτελούνται σε κάθε βήμα της διαδικασίας ανάπτυξης λογισμικού. Πιο συγκεκριμένα τα βήματα που ακολούθησα είναι τα παρακάτω:

- Σχεδίαση. Αυτή είναι η πρώτη φάση της διαδικασίας ανάπτυξης του συστήματος μας.

- Ανάλυση και απαιτήσεις συστημάτων. Στη δεύτερη φάση εργάστηκα για την πηγή του προβλήματος τους ή για την ανάγκη αλλαγής.

- Σχεδίαση συστήματος. Στην τρίτη φάση περιέγραψα λεπτομερώς τις απαραίτητες προδιαγραφές, χαρακτηριστικά και λειτουργίες που θα ικανοποιούν τις λειτουργικές απαιτήσεις του προτεινόμενου συστήματος που θα ισχύουν

- Ανάπτυξη. Η φάση ανάπτυξης σηματοδοτεί το τέλος του αρχικού τμήματος της διαδικασίας. Επιπλέον, αυτή η φάση σηματοδοτεί την έναρξη της παραγωγής.

- Ενσωμάτωση και δοκιμή. Η πέμπτη φάση περιελάβανε την ολοκλήρωση του συστήματος και τη δοκιμή του (προγραμμάτων και διαδικασιών). Έκρινα μάλιστα απαραίτητο ότι θα χρειαστούμε ποσοτική έρευνα. Ποσοτική έρευνα είναι η συστηματική εμπειρική διερεύνηση των παρατηρούμενων φαινομένων μέσω στατιστικών, μαθηματικών ή υπολογιστικών τεχνικών. Χρησιμοποιείται συνήθως αντιπροσωπευτικό δείγμα παρατηρήσεων και επιδιώκεται γενίκευση σε ένα ευρύτερο πληθυσμό.

- Υλοποίηση. Κατά την έκτη φάση της μεθοδολογίας που ακολούθησα έγραψα την πλειοψηφία του κώδικα για το πρόγραμμα. Μετά το τέλος της φάσης της υλοποίησης έγινε και αξιολόγηση του συστήματος με διάφορες τεχνικές testing (πχ χρησιμοποιώντας έτοιμα dataset βιομετρικών δεδομένων)

- Λειτουργίες και Συντήρηση. Η έβδομη και η τελική φάση περιελάβανε τη συντήρηση και τακτικές αναπροσαρμογές.

Ακολούθησα λοιπόν το μοντέλο του Καταρράκτη με Γραμμική ακολουθία φάσεων έχοντας ακολουθία σαφώς καθορισμένων βημάτων, λαμβάνοντας υπόψιν ότι κάθε βήμα καταλήγει στην δημιουργία προϊόντος (έγγραφο ή κώδικας) και κάθε προϊόν αποτελεί τη βάση για το επόμενο βήμα δίνοντας μας τη δυνατότητα του ελέγχου της ορθότητας του τελικού προϊόντος.

3.3 Σχετικές υλοποιήσεις

Αν και αυτή τη στιγμή υπάρχουν στην αγορά τόσο διάφορες υλοποιήσεις συστημάτων αναγνώρισης προσώπου όσο και ένας πολύ μεγάλος αριθμός συστημάτων εξ αποστάσεως εκπαίδευσης, λίγα συνδυάζουν τα δύο αυτά χαρακτηριστικά.

Προγράμματα εμπορικού χαρακτήρα και σκοπού ενσωματώνουν την τεχνολογία αναγνώρισης προσώπου έτσι ώστε ο εκπαιδευτικός να γνωρίζει και να ενημερώνεται για την παρακολούθηση του μαθήματος ή όχι από το μαθητή αλλά και για την αποφυγή περιπτώσεων πλαστοπροσωπίας ή ακόμη και νοθείας πιθανόν σε κάποια εξέταση.

Παράλληλα πολλές υλοποιήσεις υπάρχουν σε περιπτώσεις ερευνητικών εφαρμογών που σκοπό έχουν την μελέτη αλλά και την περεταίρω ανάπτυξη αντίστοιχων συστημάτων αναγνώρισης προσώπου.

Δυστυχώς δεν υπάρχουν υλοποιήσεις (ενεργές) σε λογισμικά ανοικτού κώδικα που θα μπορούσαν να χρησιμοποιηθούν χωρίς κόστος.

3.4 Αναγνώριση προσώπου

Ένα Σύστημα Αναγνώρισης Προσώπου είναι μια εφαρμογή των Συστημάτων Αναγνώρισης Προτύπων, που χρησιμοποιείται για αυτοματοποιημένη αναγνώριση ή επιβεβαίωση της ταυτότητας ενός ατόμου από μία ψηφιακή εικόνα ή ένα καρέ από βίντεο. Ένας τρόπος για να γίνει αυτό, είναι η σύγκριση χαρακτηριστικών προσώπου μεταξύ της εισόδου στο σύστημα (στατική εικόνα) και μιας βάσης δεδομένων χαρακτηριστικών.

Συνηθίζεται να χρησιμοποιείται σε συστήματα ασφαλείας και μπορεί να συγκριθεί με άλλες βιομετρικές μεθόδους όπως η αναγνώριση δαχτυλικών αποτυπωμάτων ή αναγνώριση αμφιβληστροειδούς χιτώνα.

Τα Συστήματα Αναγνώρισης Προτύπων, μεταξύ των οποίων και το Σύστημα Αναγνώρισης Προσώπου, ακολουθούν μια τυπική αρχιτεκτονική που περιλαμβάνει τέσσερα βασικά στάδια επεξεργασίας:

1. Λήψη μετρήσεων για κάποιες από τις ιδιότητες του αντικειμένου που μας αφορούν

2. Προ επεξεργασία των μετρήσεων για τη μείωση θορύβου και/ή κανονικοποίηση των μετρήσεων

3. Εξαγωγή χαρακτηριστικών με τα οποία γίνεται η διάκριση των προτύπων

4. Ταξινόμηση, που περιλαμβάνει τη σύγκριση των χαρακτηριστικών του αντικειμένου με κάποια χαρακτηριστικά που το σύστημα ήδη γνωρίζει που ανήκουν, ώστε να το αντιστοιχίσει σε κάποια κλάση.

Υπάρχουν δύο βασικές διαδεδομένες μέθοδοι για την αναγνώριση προσώπου, η γεωμετρική, που στηρίζεται σε χαρακτηριστικά του πρόσωπο, και η φωτομετρική που στηρίζεται στην όψη του.

Στο σχήματα παρακάτω φαίνεται η διαδικασία που ακολουθεί συγκεκριμένα ένα σύστημα αναγνώρισης προσώπου, και τα βήματα από τη στιγμή που θα δεχθεί κάποιο στιγμιότυπο - εικόνα ως είσοδο, μέχρι την απάντηση για την ταυτότητα του προσώπου.

3.5 Αναγνώριση χαρακτηριστικών προσώπου

Κάποιοι αλγόριθμοι αναγνώρισης προσώπου, αναγνωρίζουν τα πρόσωπα εξάγοντας χαρακτηριστικά από την εικόνα του προσώπου του ατόμου. Η εταιρία Identix® που εδρεύει στη Μινεσότα, είναι μια από τις πολυάριθμες εταιρίες που ασχολούνται στο χώρο και το λογισμικό της (Facelt®) μπορεί να αποτυπώσει το πρόσωπο κάποιου ατόμου από ένα πλήθος, νο το αποκόψει και στη συνέχεια να διασταυρώσει συγκεκριμένα χαρακτηριστικά που έχει στη βάση δεδομένων του. Κάθε πρόσωπο έχει πολυάριθμα ξεχωριστά διακριτικά στοιχεία από άλλα, με διαφορετικές κορυφές και κοιλάδες, που μπορούν να αποτελέσουν χαρακτηριστικά για το συγκεκριμένο πρόσωπο. Τέτοια μπορεί να είναι:

- Η απόσταση μεταξύ ματιών.

- Το πλάτος της μύτης.
- Το βάθος των ματιών.
- Το σχήμα των ζυγωματικών.
- Το μήκος του σαγονιού.

Το ανθρώπινο πρόσωπο έχει περίπου 80 τέτοια χαρακτηριστικά, που καθορίζουν τις διαφορές μεταξύ προσώπων και αποκαλούνται κομβικά σημεία (nodal points). Άλλου είδους αλγόριθμοι, κανονικοποιούν (normalize) μια σειρά δεδομένων που απαιτούν για την αναγνώριση προσώπου από ένα σύνολο προσώπων και στη συνέχεια συμπιέζουν τα χαρακτηριστικά που απαιτούν, καταλήγοντας στην πιο μικρή ικανοποιητική διάσταση διανύσματος χαρακτηριστικών. Η μέθοδος αυτή χρησιμοποιεί τον αλγόριθμο PCA (Principal Components Analysis) και πρωτοπόρος της ήταν οι Kirby και Sirivich το 1988 (η μέθοδος αυτή πολλές φορές αποκαλείται σαν χρήση eigenfaces). Μια άλλη πολύ διαδεδομένη μέθοδος, συμπεριλαμβάνει την κατηγοριοποίηση προσώπων κατά την εκπαίδευση του συστήματος και στη συνέχεια τη χρήση του αλγόριθμου LDA (Linear Discriminant Analysis), ώστε να μεγιστοποιηθεί η πυκνότητα ομοίων στοιχείων εντός της ίδιας κλάσης (ίδιο πρόσωπο) και παράλληλα να αυξηθούν οι διαφορές που έχουν οι ίδιες οι κλάσεις.

Άλλοι παρόμοιοι αλγόριθμοι είναι οι Elastic Bunch Graph Matching που χρησιμοποιεί τον αλγόριθμο Fisherface, ο Hidden Markov model και ο νευρωνικός Dynamic Link Matching.

Η τρισδιάστατη μέθοδος αναγνώρισης προσώπου αποτελεί μια παραλλαγή της κλασικής δισδιάστατης αναγνώρισης, όπου χρησιμοποιείται η τρισδιάστατη γεωμετρική αναπαράσταση του ανθρώπινου προσώπου. Είναι γνωστό ότι η τρισδιάστατη αναγνώριση προσώπου μπορεί να επιτύχει σαφέστατα καλύτερα αποτελέσματα από τη δισδιάστατη, πλησιάζοντας την ταυτοποίηση δαχτυλικού αποτυπώματος.

Στην τρισδιάστατη μέθοδο, επιτυγχάνονται καλύτερα αποτελέσματα εξετάζοντας τη γεωμετρία συμπαγών στοιχείων του προσώπου. Έτσι αποφεύγονται προβλήματα που προκύπταν με τη δισδιάστατη μελέτη και αφορούσαν αλλαγές στο φωτισμό, αλλαγές στην έκφραση των προσώπων, make up, διαφοροποίηση στον προσανατολισμό του προσώπου κατά τη λήψη του στιγμιότυπου κλπ.

Το σημαντικότερο μειονέκτημα της τρισδιάστατης αναγνώρισης προσώπων, είναι η ανάγκη για τρισδιάστατα μοντέλα, που απαιτούν τη χρήση ειδικών τύπων συστήματα λήψης. Βέβαια, εξίσου ικανοποιητικές είναι πλέον πολλαπλές λήψεις του ίδιου αντικειμένου από διαφορετικές οπτικές γωνίες, που με κατάλληλη επεξεργασία, μπορεί να αποδώσει τις μεταβλητές που ενδιαφέρουν το σύστημα.

Η έρευνα στον τομέα της τρισδιάστατης αναγνώρισης προσώπου, ενισχύεται από την ανάπτυξη αισθητήρων που μπορούν να κάνουν καλύτερη δουλειά από τις απλές 3D μηχανές λήψης. Οι αισθητήρες αυτοί λειτουργούν προβάλλοντας δομημένο φως στο υπό εξέταση πρόσωπο, ενώ μπορούν να συνδεθούν παράλληλα περίπου 12 πάνω σε ένα CMOS Chip, καθένας λαμβάνοντας διαφορετικό τμήμα του οπτικού φάσματος. Άλλες μέθοδοι, συμπεριλαμβάνουν τη χρήση αόρατων δομών φωτός για τη λήψη των δεδομένων, καθώς δεν θα απαιτούσαν την ύπαρξη (ή όχι) φωτός στο χώρο που βρίσκεται το πρόσωπο.

Για την επίτευξη ακόμα καλύτερων αποτελεσμάτων, με μεγαλύτερη εγκυρότητα, χρησιμοποιείται μια επιπλέον διαδικασία που ονομάζεται Surface Texture Analysis (ανάλυση υφής επιφάνειας). Με τη χρήση αλγορίθμων για τη μετατροπή ενός τμήματος της επιφάνειας του προσώπου, σε μαθηματικές ακολουθίες, μετρήσιμες στο χώρο, το σύστημα μπορεί να αναγνωρίσει γραμμές και πόρους στο δέρμα, που έχει στην πραγματικότητα το πρόσωπο. Η εταιρία Identix® ισχυρίζεται ότι αυτού του είδους η ανάλυση, δίνει μια ώθηση 20 έως 25% στην επιτυχή αναγνώριση προσώπου

3.6 Προσέγγιση προβλήματος

Συμπεριλαμβανομένων των προαναφερθέντων, τα συστήματα αναγνώρισης προτύπων είναι ακόμα σε πολύ χαμηλό επίπεδο, σχετικά με αυτό που έχει στο μυαλό του κάποιος που ακούει το όνομά τους. Παρόλο που τα αποτελέσματά τους είναι έγκυρα και με πολύ μικρά ποσοστά σφάλματος υπό ιδανικές συνθήκες, δυσκολεύονται ιδιαίτερα όταν αυτές δεν πληρούνται. Για παράδειγμα, ο ερευνητής Ralph Gross του Ινστιτούτου Carnegie Mellon Robotics στο Pittsburgh, δηλώνει (-σε ελεύθερη μετάφραση-) "Η αναγνώριση προσώπου πηγαίνει πολύ καλά με πρόσωπα στραμμένα στο φακό έως και 20 μοίρες διαφορετικά, αλλά όσο μετακινείσαι προς το προφίλ, υπάρχουν προβλήματα"

Παρόμοια προβλήματα εμφανίζονται όταν δεν υπάρχει επαρκής φωτισμός, όταν τα πρόσωπα φέρουν γυαλιά ηλίου, όταν τα μαλλιά του προσώπου εμπλέκονται στο πρόσωπο και γενικά οτιδήποτε μπορεί να ελαττώσει τα χαρακτηριστικά που αντιλαμβάνεται το πληροφοριακό σύστημα για το πρόσωπο. Μειώνοντας τα χαρακτηριστικά, το σύστημα χάνει την ευστάθειά του και δεν μπορεί να λάβει απόφαση με την ίδια σιγουριά, όπως αν είχε όλες τις παραμέτρους.

3.7 Υλοποίηση

Το MTCNN είναι ένας αλγόριθμος αποτελούμενος από 3 στάδια, τα οποία ανιχνεύουν τα πλαίσια οριοθέτησης των προσώπων σε μια εικόνα μαζί με τα ορόσημα 5 σημείων προσώπου . Κάθε στάδιο βελτιώνει σταδιακά τα αποτελέσματα της ανίχνευσης διαβιβάζοντας τις εισόδους του μέσω ενός CNN, το οποίο επιστρέφει τα υποψήφια όρια με τα αποτελέσματά τους, ακολουθούμενα από μη καταστολή.

Στο στάδιο 1 η εικόνα εισόδου έχει κλιμακωθεί πολλές φορές για να δημιουργηθεί μια πυραμίδα εικόνας και κάθε κλιμακωτή έκδοση της εικόνας διαβιβάζεται μέσω του CNN. Στη φάση 2 και 3 εξάγουμε τις ετικέτες εικόνων για κάθε κιβώτιο οριοθέτησης και τις αλλάζουμε (24x24 στο στάδιο 2 και 48x48 στο στάδιο 3) και τις προωθούμε μέσω του CNN εκείνου του σταδίου. Πέραν των πλαισίων οριοθέτησης και των βαθμολογιών, το στάδιο 3 υπολογίζει επιπλέον 5 σημεία ορόσημων για κάθε οριοθετημένο πλαίσιο.

Αφού συγκρίνουμε τα αποτελέσματα με κάποιες υλοποιήσεις MTCNN, αποδεικνύεται ότι μπορούμε πραγματικά να έχουμε αρκετά καλά αποτελέσματα ανίχνευσης σε πολύ χαμηλότερους χρόνους συμπερασμάτων σε σύγκριση με το SSD Mobilenet v1, ακόμα και με την εκτέλεση συμπερασμάτων στην CPU. Ως πρόσθετο μπόνους, από τα 5 Point Face Landmarks, έχουμε ευθυγράμμιση προσώπου. Με αυτόν τον τρόπο δεν χρειάζεται να πραγματοποιήσουμε ανίχνευση 68 σημείων προσανατολισμού προσώπου ως ένα ενδιάμεσο βήμα προτού υπολογίσουμε έναν μηχανισμό αναγνώρισης του προσώπου.

3.7.1 Μοντέλο χρήσης συστήματος

Για να διατηρήσουμε το μοντέλο αναγνώρισης των χρηστών μας απλό, αυτό που πραγματικά θέλουμε να επιτύχουμε είναι να εντοπίσουμε ένα άτομο που έχει μια εικόνα του προσώπου του, π.χ. την εικόνα που παρέδωσε στην γραμματεία κατά την εγγραφή του στη σχολή.

Ο τρόπος που το κάνουμε αυτό είναι να παρέχουμε μία (ή περισσότερες) εικόνες για κάθε άτομο που θέλουμε να αναγνωρίσουμε, με ετικέτα με το όνομα προσώπου. Η διαδικασία αυτή λαμβάνει χώρα κατά την εγγραφή του χρήστη στη σχολή του όπου ο φοιτητής ακολουθώντας τις έως τώρα διαδικασίες χωρίς να προσθέσουμε περισσότερο φόρτο εργασίας θα παρέχει στη γραμματεία της σχολής μία καθαρή και επικαιροποιημένη φωτογραφία του τύπου ταυτότητας. Το σύστημα μαζί με αυτή θα κρατά ανά εξεταστική περίοδο και μία νέα φωτογραφία ώστε να είναι πιο ενημερωμένο σε τυχαία χρονική στιγμή μετά από μία επιτυχή σύνδεση του χρήστη. Ο σκοπός της λήψης των περισσότερων φωτογραφιών έγκειται τόσο στην ερευνητική μελέτη του συστήματος όσο και την διαρκή ενημέρωση του συστήματος με επικαιροποιημένες φωτογραφίες των χρηστών για να καθίσταται πιο έγκυρο. Όλες αυτές οι εικόνες αποτελούν τα δεδομένα αναφοράς ως προς το σύστημά μας.

Έπειτα κάθε φορά που θα θέλει ο χρήστης να συνδεθεί το σύστημα θα συγκρίνει την εικόνα εισόδου με τα δεδομένα αναφοράς και βρίσκει την πιο παρόμοια εικόνα αναφοράς. Εάν και οι δύο εικόνες είναι αρκετά παρόμοιες, γίνεται η ταυτοποίηση και ο χρήστης συνδέεται πλέον στην πλατφόρμα εξ αποστάσεως εκπαίδευσης (στην περίπτωσή μας moodle).

Ωστόσο, παραμένουν δύο προβλήματα. Πρώτον, τι γίνεται αν έχουμε μια εικόνα που δείχνει πολλά άτομα και θέλουμε να τα αναγνωρίσουμε όλα; Και δεύτερον, πρέπει να είμαστε σε θέση να λάβουμε ένα τέτοιο μέτρο ομοιότητας για δύο εικόνες προσώπου για να τις συγκρίνουμε.

Ακόμη ένα ζήτημα είναι οι περιπτώσεις λανθασμένης πιστοποίησης. Οι περιπτώσεις δηλαδή στις οποίες ο χρήστης απέτυχε να αναγνωριστεί από το σύστημα. Σε αυτές τις περιπτώσεις υπάρχει καταγραφή των λανθασμένων προσπαθειών και έπειτα από τρεις αποτυχημένες προσπάθειες σύνδεσης υπάρχει η δυνατότητα είτε να ενημερώνεται η γραμματεία και να ελέγχει τις φωτογραφίες των αποτυχημένων προσπαθειών είτε εναλλακτικά να δίνεται στο χρήστη το δικαίωμα να συμπληρώσει περισσότερες πληροφορίες όπως ο αριθμός ταυτότητάς του, το login του, η ημερομηνία γέννησης και το τηλέφωνό του ώστε να του επιτραπεί η σύνδεση. Πληροφορίες που μονάχα ο χρήστης και το σύστημα μπορούν να γνωρίζουν.

3.7.2 Παρουσίαση αλγορίθμου αναγνώρισης προσώπου

Η απάντηση στο πρώτο πρόβλημα είναι η ανίχνευση προσώπου. Με απλά λόγια, θα εντοπίσουμε πρώτα όλα τα πρόσωπα στην εικόνα εισόδου. Το Face-api.js εφαρμόζει τεχνικές ανίχνευσης πολλαπλών προσώπων για διαφορετικές περιπτώσεις χρήσης.

Ο πιο ακριβής ανιχνευτής προσώπου είναι ένας ανιχνευτής SSD (Single Shot Multibox Detector), ο οποίος βασικά είναι CNN βασισμένος στο MobileNet V1, με μερικά πρόσθετα στρώματα πρόβλεψης κουτιού στοιβαγμένα στην κορυφή του δικτύου.

Επιπλέον το face-api.js υλοποιεί έναν βελτιστοποιημένο μικροσκοπικό ανιχνευτή προσώπου, βασικά μια ακόμα πιο μικρή έκδοση του Tiny Yolo v2, χρησιμοποιώντας βαθιές ξεχωριστές περιελίξεις αντί για τακτικές περιστροφές, που είναι πολύ πιο γρήγορος, αλλά ελαφρώς λιγότερο ακριβής σε σύγκριση με το SSD MobileNet V1.

Τέλος, υπάρχει επίσης μία MTCNN (Multi-task Cascaded Convolutional Neuteric Network) εφαρμογή, η οποία χρησιμοποιείται κυρίως για πειραματικούς σκοπούς.

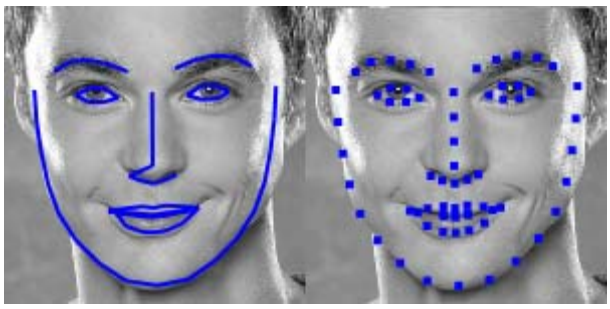
Τα δίκτυα επιστρέφουν τα πλαίσια οριοθέτησης κάθε προσώπου, με τις αντίστοιχες βαθμολογίες τους, π.χ. η πιθανότητα κάθε πλαισίου οριοθέτησης να δείχνει ένα πρόσωπο. Οι βαθμολογίες χρησιμοποιούνται για να φιλτράρουν τα κιβώτια οριοθέτησης, καθώς μπορεί να είναι ότι μια εικόνα δεν περιέχει κανένα πρόσωπο. Σημειώστε ότι αυτή η ανίχνευση προσώπου

θα πρέπει να εκτελεστεί ακόμα και αν υπάρχει μόνο ένα άτομο στη φωτογραφία.

Εικόνα 1: Παράδειγμα πλαισίων οριοθέτησης κάθε προσώπου, με τις αντίστοιχες βαθμολογίες

Το πρώτο πρόβλημα λύνεται! Ωστόσο, θέλω να επισημάνω ότι θέλουμε να ευθυγραμμίσουμε τα κιβώτια οριοθέτησης έτσι ώστε να μπορέσουμε να εξάγουμε τις εικόνες με κέντρο το πρόσωπο για κάθε κουτί πριν τις περάσουμε στο δίκτυο αναγνώρισης προσώπου, καθώς αυτό θα κάνει την αναγνώριση προσώπων πολύ ακριβέστερη.

Για το σκοπό αυτό το face-api.js υλοποιεί ένα απλό CNN, το οποίο επιστρέφει τα ορόσημα 68 σημείων προσώπου μιας δεδομένης εικόνας όπως φαίνεται και στο παρακάτω παράδειγμα:



Εικόνα 2: Παράδειγμα σήμανσης 68 ορόσημων σημείων προσώπου

Από τις θέσεις των ορόσημων, το πλαίσιο οριοθέτησης μπορεί να είναι κεντραρισμένο στο πρόσωπο. Στη συνέχεια, μπορείτε να δείτε το αποτέλεσμα ανίχνευσης προσώπου (αριστερά) σε

σύγκριση με την ευθυγραμμισμένη εικόνα προσώπου (δεξιά) όπως στα παραδείγματα παρακάτω:

Εικόνα 3: Παράδειγμα απομόνωσης και κεντραρίσματος προσώπων προς έλεγχο

Για την ανίχνευση προσώπου, το συγκεκριμένο εργαλείο υλοποιεί ένα SSD (Single Shot Multibox Detector) με βάση το MobileNetV1. Ο αλγόριθμος υπολογίζει τις θέσεις κάθε προσώπου σε μια εικόνα και θα επιστρέψει τα κιβώτια οριοθέτησης μαζί με την πιθανότητα για κάθε πρόσωπο. Αυτός ο ανιχνευτής προσώπου στοχεύει στην επίτευξη υψηλής ακρίβειας στην ανίχνευση πλαισίων οριοθέτησης προσώπου αντί για χαμηλό χρόνο συμπερασμάτων.

Ο Tiny Face Detector είναι ένας πολύ αποτελεσματικός ανιχνευτής προσώπου σε πραγματικό χρόνο, ο οποίος είναι πολύ ταχύτερος, μικρότερος και λιγότερος πόρος που καταναλώνει σε σύγκριση με τον ανιχνευτή προσώπου SSD Mobilenet V1, ενώ αντίθετα αποδίδει ελαφρώς λιγότερο καλά στην ανίχνευση μικρών προσώπων. Αυτό το μοντέλο είναι εξαιρετικά συμβατό και φιλικό προς διαδικτυακές εφαρμογές αλλά και διάφορα μέσα πλοήγησης, καθώς θα πρέπει ο ανιχνευτής προσώπου να λειτουργεί και σε κινητές συσκευές και clients περιορισμένης πρόσβασης.

Αυτό το μοντέλο είναι βασικά μια ακόμη πιο μικρή έκδοση του Tiny Yolo V2, αντικαθιστώντας τις συνηθισμένες συνέλιες του Yolo με βάσιμες διαχωρίσιμες περιελίξεις. Το Yolo είναι πλήρως συνελικτικό, έτσι μπορεί εύκολα να προσαρμοστεί σε διαφορετικά μεγέθη εικόνων εισόδου για να ανταλλάξει την ακρίβεια για την απόδοση (χρόνος συμπερασμάτων).

Το MTCNN (Multi-task Cascaded Convolutional Neural Networks) αντιπροσωπεύει έναν εναλλακτικό ανιχνευτή προσώπου στα SSD Mobilenet v1 και Tiny Yolo v2, ο οποίος προσφέρει πολύ περισσότερο χώρο για διαμόρφωση. Ρυθμίζοντας τις παραμέτρους εισόδου, το MTCNN είναι σε θέση να ανιχνεύει ένα ευρύ φάσμα μεγεθών κουτιού. Το MTCNN είναι ένα κλιμακωτό CNN τριών σταδίων, το οποίο επιστρέφει ταυτόχρονα 5 σημεία ορόσημο μαζί με τα πλαίσια και βαθμολογίες για κάθε πρόσωπο. Επιπλέον, το μέγεθος μοντέλου είναι μόνο 2MB.

Το MTCNN έχει παρουσιαστεί στη χαρτογράφηση κοινής ανίχνευσης και ευθυγράμμισης προσώπων με τη χρήση πολυφασικών συνεστραμμένων δικτύων πολλαπλών εργασιών από τον Zhang et al. και τα βάρη του μοντέλου παρέχονται στην επίσημη απογραφή της εφαρμογής MTCNN.

Το μοντέλο αναγνώρισης έκφρασης προσώπου είναι ελαφρύ, γρήγορο και παρέχει λογική ακρίβεια. Το μοντέλο έχει μέγεθος περίπου 310kb και χρησιμοποιεί διαχωρίσιμες συρράξεις και πυκνά συνδεδεμένα μπλοκ σε βάθος.

3.7.3 Παρουσίαση αλγορίθμου ταυτοποίησης χαρακτηριστικών προσώπου

Τώρα μπορούμε να τροφοδοτήσουμε τις εξαγόμενες και ευθυγραμμισμένες εικόνες προσώπου στο δίκτυο αναγνώρισης προσώπου, το οποίο βασίζεται σε μια αρχιτεκτονική όπως το ResNet-34 και βασικά αντιστοιχεί στην αρχιτεκτονική που υλοποιείται στο dlib. Το εργαλείο αναγνώρισης έχει εκπαιδευτεί για να μάθει να χαρτογραφεί τα χαρακτηριστικά ενός ανθρώπινου προσώπου σε έναν «περιγραφέα» προσώπου (ένα διάνυσμα χαρακτηριστικών με 128 τιμές), το οποίο επίσης συχνά αναφέρεται ως ενσωματωμένο πρόσωπο.

Τώρα για να επιστρέψουμε στο αρχικό μας πρόβλημα σύγκρισης δύο προσώπων: Θα χρησιμοποιήσουμε τον «περιγραφέα» προσώπου για κάθε εξωγενή εικόνα προσώπου και θα τα συγκρίνουμε με τους «περιγραφείς» προσώπου των δεδομένων αναφοράς. Πιο συγκεκριμένα, μπορούμε να υπολογίσουμε την ευκλείδεια απόσταση ανάμεσα σε δύο «περιγραφείς» προσώπου και να κρίνουμε εάν δύο όψεις είναι παρόμοιες με βάση μια τιμή κατωφλίου (για 150 x 150 εικόνες μεγέθους προσώπου 0.6 είναι μια καλή τιμή κατωφλίου). Η χρήση της ευκλείδειας

απόστασης λειτουργεί εκπληκτικά καλά, αλλά φυσικά μπορούμε να χρησιμοποιήσουμε οποιοδήποτε άλλο είδος αλγορίθμου ταξινόμησης θα θέλαμε.

Στα πλαίσια της υλοποίησής μας εφαρμόζουμε έναν πολύ ελαφρύ και γρήγορο, αλλά ακριβή ανιχνευτή ορόσημο 68 σημείων. Το προεπιλεγμένο μοντέλο έχει μέγεθος μόλις 350kb (face_landmark_68_model) και το μικροσκοπικό μοντέλο είναι μόνο 80kb (face_landmark_68_tiny_model). Και τα δύο μοντέλα χρησιμοποιούν τις ιδέες των διαχωριζόμενων συρραφών κατά βάθος καθώς και των πυκνά συνδεδεμένων μπλοκ. Για αναγνώριση προσώπου, υλοποιείται μια αρχιτεκτονική όπως το ResNet-34 για τον υπολογισμό ενός «περιγραφέα» προσώπου (ένα διάνυσμα χαρακτηριστικών με 128 τιμές) από οποιαδήποτε δεδομένη εικόνα προσώπου, η οποία χρησιμοποιείται για να περιγράψει τα χαρακτηριστικά ενός ατόμου προσώπου. Το μοντέλο δεν περιορίζεται στο σύνολο των προσώπων που χρησιμοποιούνται για την εκπαίδευση, που σημαίνει ότι μπορούμε να το χρησιμοποιήσουμε για αναγνώριση προσώπου από οποιοδήποτε άτομο. Μπορούμε να προσδιορίσουμε την ομοιότητα δύο αυθαίρετων όψεων, συγκρίνοντας τους περιγραφείς προσώπου τους.

3.7.4 Παραμετροποίηση εργαλείων αναγνώρισης προσώπου

Θα δούμε τώρα πώς εφαρμόσαμε την παρακολούθηση προσώπου και την αναγνώριση προσώπου χρησιμοποιώντας την κάμερα web. Σε αυτό το παράδειγμα θα χρησιμοποιήσω την κάμερα web για να παρακολουθήσω και να αναγνωρίσω ξανά τα πρόσωπα ορισμένων ατόμων, αλλά φυσικά μπορείτε να χρησιμοποιήσετε τον αντίστοιχο κώδικα για την παρακολούθηση και την αναγνώρισή άλλων ανάλογων προσώπων.

Για να εμφανίσουμε καρέ από την κάμερά μας, μπορούμε απλά να χρησιμοποιήσουμε ένα στοιχείο βίντεο ως εξής. Επιπλέον, τοποθετώ έναν απολύτως τοποθετημένο καμβά στην κορυφή του βίντεο, με το ίδιο ύψος και πλάτος. Θα χρησιμοποιήσουμε τον καμβά ως διαφανή επικάλυψη, την οποία μπορούμε αργότερα να αντλήσουμε τα αποτελέσματα της ανίχνευσης σε ένα αντίστοιχο στοιχείο της σελίδας μας.

```
<div style="position: relative" class="margin">
 <video onplay="onPlay(this)" id="inputVideo" autoplay m
 <canvas id="overlay" />
</div>
```

Μόλις φορτωθεί η σελίδα, θα φορτώσουμε το μοντέλο MTCNN καθώς και το μοντέλο αναγνώρισης προσώπου για να υπολογίσουμε τους περιγραφείς προσώπου. Επιπλέον, συνδέουμε τη ροή της κάμεράς μας με το στοιχείο βίντεο χρησιμοποιώντας το navigator.getUserMedia

```
$(document).ready(function() {
 run()
})

async function run() {
 // load the models
 await faceapi.loadMtcnnModel('/')
 await faceapi.loadFaceRecognitionModel('/')

 // try to access users webcam and stream the images
 // to the video element
 const videoEl = document.getElementById('inputVideo')
 navigator.getUserMedia(
  { video: {} },
  stream => videoEl.srcObject = stream,
  err => console.error(err)
 )
}
```

Θα πρέπει τώρα να μας ζητηθεί να παραχωρήσουμε στο πρόγραμμα περιήγησης πρόσβαση στην κάμερά μας. Στην ανάκληση κλήσεων onPlay που καθορίσαμε για το στοιχείο βίντεο, θα χειριστούμε την πραγματική επεξεργασία για κάθε καρέ. Σημειώνουμε ότι το event onplay, ενεργοποιείται μόλις ξεκινήσει η αναπαραγωγή του βίντεο.

Όπως αναφέραμε, μπορούμε να διαμορφώσουμε κάποιες παραμέτρους ανίχνευσης των εργαλείων. Οι προεπιλεγμένες παράμετροι είναι οι εξής:

```
const mtcnnForwardParams = {
 // number of scaled versions of the input image passed through the CNN
 // of the first stage, lower numbers will result in lower inference time,
```

```
  // but will also be less accurate
  maxNumScales: 10,
  // scale factor used to calculate the scale steps of the image
  // pyramid used in stage 1
  scaleFactor: 0.709,
  // the score threshold values used to filter the bounding
  // boxes of stage 1, 2 and 3
  scoreThresholds: [0.6, 0.7, 0.7],
  // mininum face size to expect, the higher the faster processing will be,
  // but smaller faces won't be detected
  minFaceSize: 20
}
```

Για την παρακολούθηση προσώπων από την κάμερά, θα αυξήσουμε το minFaceSize σε atleast 200px. Αν ανιχνεύσουμε μόνο πρόσωπα μεγαλύτερων μεγεθών, μπορούμε να επιτύχουμε πολύ χαμηλότερους χρόνους συμπερασμάτων, καθώς το δίκτυο θα μειώσει τις εικόνες με πολύ μεγαλύτερο συντελεστή

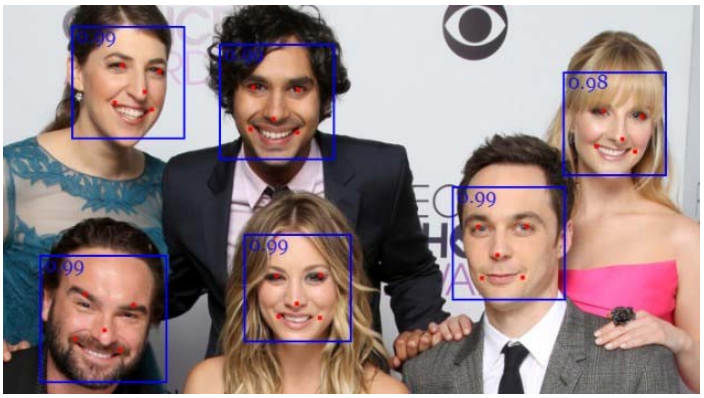
```
const mtcnnForwardParams = { // limiting the search space to larger faces for webcam detection
minFaceSize: 200} const mtcnnResults = await
faceapi.mtcnn(document.getElementById('inputVideo'), mtcnnForwardParams)
```

Όπως διαπιστώνουμε, μπορούμε απλά να τα τροφοδοτήσουμε με το βίντεο, ακριβώς όπως ένα στοιχείο εικόνας ή καμβά.

Ένα πέρασμα προς τα εμπρός μέσω του MTCNN μας δίνει μια σειρά FaceDetections (bounding box + score) μαζί με τα FaceLandmark5s για κάθε ανιχνευμένο πρόσωπο. Τώρα μπορούμε να αντλήσουμε τα αποτελέσματα.

```
faceapi.drawDetection('overlay', mtcnnResults.map(res => res.faceDetection), { withScore: false
})faceapi.drawLandmarks('overlay', mtcnnResults.map(res => res.faceLandmarks), { lineWidth: 4,
color: 'red' })
```

Για να δείξουμε μόνο ένα παράδειγμα, μέχρι τώρα θα καταλήξουμε στα εξής.



Εικόνα 4: Παράδειγμα οριοθέτησης πολλαπλών προσώπων και τα σκορ της πιθανότητας οι οριοθετήσεις να είναι ορθά πρόσωπα

Πλέον θέλουμε να ευθυγραμμίσουμε τα πλαίσια πλαισίωσης από τις θέσεις των ορόσημων προσώπου πριν υπολογίσουμε οποιονδήποτε περιγραφείς προσώπου. Από τα ευθυγραμμισμένα πλαίσια, εξάγουμε τον ευθυγραμμισμένο συντελεστή προσώπου, τον οποίο μπορούμε να περάσουμε μέσω του δικτύου αναγνώρισης προσώπου:

```
const alignedFaceBoxes = results.map(
 ({ faceLandmarks }) => faceLandmarks.align()
)


const alignedFaceTensors = await extractFaceTensors(input, alignedFaceBoxes)


const descriptors = await Promise.all(alignedFaceTensors.map(
 faceTensor => faceapi.computeFaceDescriptor(faceTensor)
))


// free memory
alignedFaceTensors.forEach(t => t.dispose())
```

3.7.5 Παραμετροποίηση εργαλείων ταυτοποίησης προσώπου

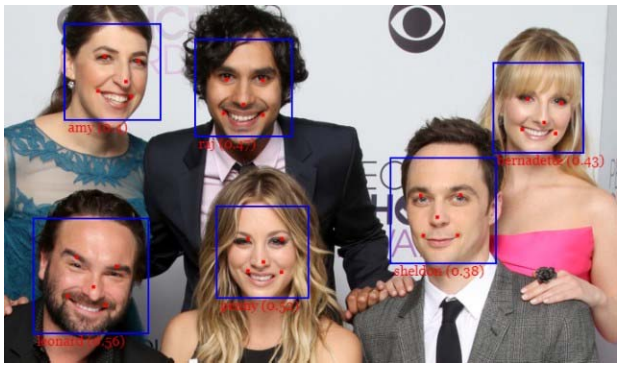
Από εδώ και στο εξής, προχωρούμε απλά με τον ίδιο τρόπο. Υπενθυμίζουμε ότι για να προσδιορίσουμε ένα πρόσωπο, πριν εκτελέσουμε τον κύριο βρόχο, πρέπει να προ-υπολογίσουμε έναν περιγραφέα προσώπου (από τουλάχιστον ένα) από μια εικόνα παραδείγματος για κάθε άτομο που θέλουμε να αναγνωρίσουμε (δεδομένα αναφοράς):

```
const labels = ['sheldon' 'raj', 'leonard', 'howard']


const labeledFaceDescriptors = await Promise.all(
 labels.map(async label => {
  // fetch image data from urls and convert blob to HTMLImage element
  const imgUrl = `${label}.png`
  const img = await faceapi.fetchImage(imgUrl)
```

```
  // detect the face with the highest score in the image and compute it's landmarks and
face descriptor
  const fullFaceDescription = await
faceapi.detectSingleFace(img).withFaceLandmarks().withFaceDescriptor()

  if (!fullFaceDescription) {
   throw new Error(`no faces detected for ${label}`)
  }

  const faceDescriptors = [fullFaceDescription.descriptor]
  return new faceapi.LabeledFaceDescriptors(label, faceDescriptors)
 })
)
```

Για να αποφασίσουμε ποιο άτομο κάθεται μπροστά από την κάμερα, υπολογίζουμε την απόσταση του περιγραφέα προσώπου της ζωντανής εικόνας και την απόσταση στους περιγραφείς προσώπου στα δεδομένα αναφοράς χρησιμοποιώντας faceapi.FaceMatcher ξανά και επιστρέφουμε την πιο κοντινή αντιστοίχιση:

```
// 0.6 is a good distance threshold value to judge
// whether the descriptors match or not
const maxDescriptorDistance = 0.6
const faceMatcher = new faceapi.FaceMatcher(labeledFaceDescriptors, maxDescriptorDistance)
const results = fullFaceDescriptions.map(fd => faceMatcher.findBestMatch(fd.descriptor))
```



Εικόνα 5: Παράδειγμα οριοθέτησης πολλαπλών προσώπων και τα σκορ της πιθανότητας αναγνώρισής τους

3.7.6 Διασύνδεση ηλεκτρονικής πλατφόρμας με το σύστημά μας

Σύμφωνα λοιπόν με τις τεχνικές που αναφέραμε παραπάνω φτάνουμε να έχουμε ένα αποτέλεσμα που αφορά το όνομα ή το αναγνωριστικό την δική μας περίπτωση του χρήστη που ανιχνεύτηκε. Αυτό το αναγνωριστικό θα δώσουμε ως είσοδο στο σύστημα εξ αποστάσεως εκπαίδευσης της εργασίας μας ώστε να προχωρήσει με τη σύνδεση του χρήστη.

Πως λειτουργεί όμως το σύστημα login του εργαλείου που χρησιμοποιούμε? (Στην περίπτωσή μας η πλατφόρμα moodle)

Παρουσίαση συστήματος user authentication της πλατφόρμας εξ αποστάσεως εκπαίδευσης.

Ο έλεγχος ταυτότητας είναι η διαδικασία που επιτρέπει σε έναν χρήστη να συνδεθεί σε έναν ιστότοπο Moodle με όνομα χρήστη και κωδικό πρόσβασης. Το Moodle παρέχει πολλούς τρόπους διαχείρισης της ταυτότητας, που ονομάζονται plugins πιστοποίησης. Κάποια από αυτά είναι τα παρακάτω:

- Manual accounts - οι λογαριασμοί δημιουργούνται χειροκίνητα από έναν διαχειριστή
- No login - αναστολή συγκεκριμένου λογαριασμού χρήστη
- Email-based self-registration - Ηλεκτρονική εγγραφή με βάση το ηλεκτρονικό ταχυδρομείο - για να επιτρέπετε στους χρήστες να δημιουργούν τους δικούς τους λογαριασμούς
- CAS server (SSO) - τα στοιχεία του λογαριασμού βρίσκονται σε έναν εξωτερικό διακομιστή CAS
- External database - τα στοιχεία του λογαριασμού βρίσκονται σε μια εξωτερική βάση δεδομένων
- LDAP server - τα στοιχεία του λογαριασμού βρίσκονται σε έναν εξωτερικό διακομιστή LDAP
- LTI - λειτουργεί με τη μέθοδο εγγραφής εργαλείου "Δημοσίευση ως εργαλείο LTI" για τη σύνδεση μαθημάτων και δραστηριοτήτων
- Moodle Network authentication - πώς μπορούν να συνδεθούν οι διαφορετικοί ιστότοποι Moodle και να πιστοποιήσουν τους χρήστες

- No authentication - για σκοπούς δοκιμής ή αν ο ιστότοπος Moodle δεν είναι διαθέσιμος στο Διαδίκτυο. ΔΕΝ χρησιμοποιείτε σε δημόσιους διακομιστές!

- Shibboleth - τα στοιχεία του λογαριασμού βρίσκονται σε έναν εξωτερικό διακομιστή Shibboleth

- Web services authentication

Στα παραπάνω συμπληρώνεται και η πρότασή μας καθώς μέσω του εργαλείου μας και της αναγνώρισης του χρήστη ο τελευταίος μπορεί να αποκτά πλέον πρόσβαση στην ηλεκτρονική πλατφόρμα εξ αποστάσεως εκπαίδευσης. Πιο συγκεκριμένα επεκτείνουμε την τρίτη επιλογή συνδέσεων (Ηλεκτρονική εγγραφή με βάση το ηλεκτρονικό ταχυδρομείο - για να επιτρέπετε στους χρήστες να δημιουργούν τους δικούς τους λογαριασμούς) καθώς, αφού η γραμματεία ή ο υπεύθυνος οργανισμός έχει δημιουργήσει τον λογαριασμό του χρήστη αυτός θα χρησιμοποιήσει κατά την πρώτη του εγγραφή το email του και σε κάθε άλλη σύνδεση την οπτική αναγνώριση για την ταυτοποίησή του ακολουθώντας το παρακάτω μοντέλο.

Κατά την υλοποίηση του συστήματος μας θα πρέπει να καλύπτονται κάποιες συγκεκριμένες προδιαγραφές όπως αυτές αναλύονται παρακάτω.

1. Αρχικά ο εκπαιδευόμενος/εκπαιδευτικός κατά την εγγραφή του θα παρέχει μία καθαρή φωτογραφία ταυτότητας την οποία το σύστημα θα χρησιμοποιεί ως σημείο 0.

2. Ο διαχειριστής του συστήματος όταν θα δημιουργεί ένα νέο λογαριασμό για ένα εκπαιδευόμενο/εκπαιδευτικό θα αντιστοιχίζει την φωτογραφία ταυτότητάς του στο σύστημα.

3. Ο εκπαιδευόμενος/εκπαιδευτικός κατά την πρώτη προσπάθεια σύνδεσης στο σύστημα και αφού καταχωρήσει τα στοιχεία ορθά και συνδεθεί θα πρέπει να παρέχει μία «ζωντανή» φωτογραφία εκείνης της στιγμής μέσω της κάμερας της ηλεκτρονικής συσκευής που χρησιμοποιεί. Η είσοδός του στο σύστημα δεν θα επιτρέπεται μέχρι την υποβολή της φωτογραφίας. Αυτή η φωτογραφία αρχικά θα συγκρίνεται με την υπάρχουσα αποθηκευμένη και έπειτα θα αποθηκεύεται στο σύστημα ως δεύτερος οδηγός.

4. Έπειτα, και για κάθε άλλη προσπάθεια σύνδεσης, ο εκπαιδευόμενος/εκπαιδευτικός θα έχει τη δυνατότητα να συνδεθεί είτε χρησιμοποιώντας το σύστημα αναγνώρισης προσώπου είτε το κλασσικό σύστημα του ζεύγους email/password.

5. Κάθε προσπάθεια ταυτοποίησης του εκπαιδευόμενου/εκπαιδευτικού θα έχει ως αποτέλεσμα ένα αριθμό ακρίβειας. Όταν αυτός ο αριθμός θα είναι κάτω από ένα ορισμένο threshold για ορισμένο αριθμό προσπαθειών το σύστημα αναγνώρισης προσώπου θα απενεργοποιείται. Ο εκπαιδευόμενος/εκπαιδευτικός θα μπορεί να συνδεθεί μονάχα με τον κωδικό του ενώ μετά από επιτυχή σύνδεση θα του παρουσιάζονται και οι αντίστοιχες φωτογραφίες των εσφαλμένων προσπαθειών προς ενημέρωσή του με στόχο την αναγνώριση πιθανών κακόβουλων προσπαθειών σύνδεσης από τρίτους.

Εννοείται πως εάν το επιθυμεί ο ίδιος ανά πάσα στιγμή θα μπορεί να συνδεθεί και με τη χρήση των στοιχείων του email και του κωδικού του.

3.8 Δοκιμές - Πειραματικές αξιολογήσεις

Για τις ανάγκες τις εργασίας μία ομάδα δέκα ατόμων δοκίμασε το σύστημα.

Το σύστημα ανταποκρίθηκε επιτυχώς στο 75% των περιπτώσεων καθώς όταν δόθηκαν φωτογραφίες με αλλαγμένα πρόσωπα (κυρίως σε περιπτώσεις διαφοροποιήσεων εξαιτίας γενειάδας) δεν κατέστη δυνατό να γίνει αναγνώριση των προσώπων.

Όσον αφορά ωστόσο την αξιοπιστία των αλγορίθμων που χρησιμοποιήθηκαν Ο ανιχνευτής προσώπου έχει εκπαιδευτεί σε ένα προσαρμοσμένο σύνολο εικόνων με ~ 14K εικόνες που φέρουν ετικέτες με δεσμευτικά πλαίσια. Επιπλέον, το μοντέλο έχει εκπαιδευτεί για την πρόβλεψη οριοθετημένων κιβωτίων, τα οποία καλύπτουν εξ ολοκλήρου τα χαρακτηριστικά γνωρίσματα του προσώπου, έτσι γενικά παράγει καλύτερα αποτελέσματα σε συνδυασμό με την επακόλουθη ανίχνευση ορόσημων από το SSD Mobilenet V1.

Έχει εκπαιδευτεί σε μια ποικιλία εικόνων από διαθέσιμα στο κοινό σύνολα δεδομένων καθώς και σε εικόνες που έχουν αποκτηθεί από τον ιστό. Σημειώστε ότι η χρήση γυαλιών μπορεί να μειώσει την ακρίβεια των αποτελεσμάτων πρόβλεψης όπως αναφέραμε ήδη παραπάνω.

Τα μοντέλα έχουν εκπαιδευτεί σε ένα σύνολο δεδομένων ~ 35k προσώπων που έχουν επισημανθεί με 68 σημεία ορόσημο.

Το νευρωνικό δίχτυ είναι ισοδύναμο με το FaceRecognizerNet που χρησιμοποιείται στο face-recognition.js και το δίχτυ που χρησιμοποιείται στο παράδειγμα αναγνώρισης προσώπου dlib. Τα βάρη έχουν εκπαιδευτεί με davisking και το μοντέλο επιτυγχάνει ακρίβεια πρόβλεψης 99 Labeled Faces in the Wild) για αναγνώριση προσώπου.

Γενικά, άλλοι ανιχνευτές προσώπου πρέπει να έχουν καλύτερη απόδοση, αλλά φυσικά στα πλαίσια της εργασίας προσπαθούμε για το καλύτερο δυνατό αποτέλεσμα.

Σημειώστε ότι η ανασυγκρότηση των περιγραφών προσώπου ερωτήματος για κάθε ξεχωριστό πλαίσιο είναι μια πολύ αφελής προσέγγιση. Προφανώς μπορούμε να βρούμε μια πιο αποτελεσματική προσέγγιση, όπως την παρακολούθηση και την ενημέρωση των περιγραφών προσώπου των αποτελεσμάτων ανίχνευσης σας κάθε x πλαίσια. Συνήθως η στάση του κυματοειδούς προσώπου δεν αλλάζει δραστικά σε λίγα πλαίσια. Αλλά για λόγους απλότητας στα πλαίσια μίας ακαδημαϊκής εργασίας χρησιμοποιούμε πιο απλή υλοποίηση.

Τέλος θα πρέπει να αναφέρουμε ότι στις σχετικές δοκιμές που έγιναν σχετικά με τη χρήστη του συστήματος απαιτήθηκαν κατά μέσο όρο περί τα 10”-15” για τη σύνδεση του κάθε χρήστη. Αυτό το χρονικό διάστημα ήταν διαφορετικό, κυρίως υψηλότερο, σε περιπτώσεις που το περιβάλλον και οι συνθήκες φωτισμού κατά τις προσπάθειες πιστοποίησης ήταν κακές.

3.9 Απόδοση συστήματος (Σε επίπεδο διακομιστή)

Όσον αφορά την απόδοση συστημάτων που θα μπορούσαν να φιλοξενήσουν το εργαλείο παρατηρήσαμε ότι η μόνη επίπτωση σε τεχνικό επίπεδο είχε να κάνει με τα επίπεδα της χωρητικότητας των δίσκων του διακομιστή ώστε να είναι σε θέση να καταγράφουν τον μεγάλο όγκο οπτικού υλικού και στην ανάγκη για ύπαρξη υποδομών υψηλού bandwidth ώστε να μεταφέρεται ο όγκος των δεδομένων πιο γρήγορα.

3.10 Κόστος και εκπαίδευση

Το κόστος παραμένει μηδενικό καθώς όλα τα εργαλεία και οι αλγόριθμοι που χρησιμοποιήθηκαν είναι open source και καλύπτονται από άδειες ελεύθερης διακίνησης. Παρόλα αυτά κρίνεται απαραίτητη η ύπαρξη του αντίστοιχου τεχνικού προσωπικού που θα είναι υπεύθυνο για την ορθή λειτουργία, υποστήριξη, συντήρηση και αναβάθμιση του λογισμικού.

Ομοίως εκτιμάται ότι θα απαιτηθούν περί τις 24 ανθρωποώρες για την σωστή εκπαίδευση του αντίστοιχου προσωπικού (μέλη γραμματείας) για την σωστή χρήση του.

3.11 Περιορισμοί

Οι κύριοι περιορισμοί που καταγράφονται κινούνται γύρω από τρείς κύριους τομείς:

Υψηλά κόστη υλοποίησης: Η αναγνώριση προσώπου απαιτεί κάμερες υψηλής ποιότητας και προηγμένο λογισμικό για την εξασφάλιση της ακρίβειας και της ταχύτητας. Ωστόσο, η Allied Market Research προβλέπει ότι οι τεχνολογικές εξελίξεις είναι πιθανό να μειώσουν τις τιμές των συστημάτων αναγνώρισης προσώπου στο μέλλον.

Αποθήκευση δεδομένων: Το βίντεο και οι εικόνες υψηλής ποιότητας που απαιτούνται για την αναγνώριση προσώπου αναλαμβάνουν σημαντική αποθήκευση. Προκειμένου τα συστήματα αναγνώρισης προσώπου να είναι αποτελεσματικά, επεξεργάζονται μόνο το 10 έως 25% των βίντεο. Αυτό οδηγεί τους οργανισμούς να χρησιμοποιούν πολλούς υπολογιστές για να επεξεργάζονται τα πάντα και να το κάνουν γρήγορα.

Αλλαγές στην εμφάνιση και τη γωνία της κάμερας: Οποιεσδήποτε σημαντικές αλλαγές στην εμφάνιση, συμπεριλαμβανομένων των μαλλιών του προσώπου και των αλλαγών βάρους, μπορούν να απορρίψουν την τεχνολογία. Σε αυτές τις περιπτώσεις απαιτείται μια νέα εικόνα. Η γωνία της κάμερας μπορεί επίσης να προκαλέσει προβλήματα επειδή απαιτούνται πολλές γωνίες για την αναγνώριση ενός προσώπου.

Ο Ralph Gross, ερευνητής στο Ινστιτούτο Ρομποτικής της Carnegie Mellon το 2008, περιγράφει ένα εμπόδιο που σχετίζεται με τη γωνία θέασης του προσώπου: "Η αναγνώριση προσώπου έχει γίνει αρκετά καλή σε πλήρη μετωπικά πρόσωπα και 20 βαθμούς μακριά, αλλά μόλις πάτε προς προφίλ, υπήρξαν προβλήματα. " Εκτός από τις παραλλαγές θέτουν, οι εικόνες προσώπου χαμηλής ανάλυσης είναι επίσης πολύ δύσκολο να αναγνωριστούν. Αυτό αποτελεί ένα από τα κύρια εμπόδια της αναγνώρισης προσώπου στα συστήματα επιτήρησης.

Η αναγνώριση προσώπου είναι λιγότερο αποτελεσματική εάν οι εκφράσεις του προσώπου ποικίλλουν. Ένα μεγάλο χαμόγελο μπορεί να καταστήσει το σύστημα λιγότερο αποτελεσματικό. Παραδείγματος χάριν: ο Καναδάς, το 2009, επέτρεψε μόνο ουδέτερες εκφράσεις προσώπου σε φωτογραφίες διαβατηρίου.

Υπάρχει επίσης ασυνέχεια στα σύνολα δεδομένων που χρησιμοποιούνται από τους ερευνητές. Οι ερευνητές μπορούν να χρησιμοποιήσουν οπουδήποτε από διάφορα θέματα σε πολλά θέματα και μερικές εκατοντάδες εικόνες σε χιλιάδες εικόνες. Είναι σημαντικό οι ερευνητές να διαθέτουν τα σύνολα δεδομένων που χρησιμοποιούν μεταξύ τους ή να διαθέτουν τουλάχιστον ένα τυποποιημένο σύνολο δεδομένων.

Το ιδιωτικό απόρρητο δεδομένων αποτελεί το κύριο μέλημα όσον αφορά την αποθήκευση δεδομένων βιομετρικών δεδομένων σε εταιρείες. Οι αποθηκευμένες πληροφορίες σχετικά με το πρόσωπο ή τα βιομετρικά στοιχεία μπορούν να έχουν πρόσβαση από το τρίτο μέρος, εάν δεν αποθηκευτούν σωστά ή έχουν πειραχτεί. Στο Techworld, ο Parris προσθέτει (2017) ότι "οι χάκερς θα προσπαθήσουν ήδη να αναπαράγουν τα πρόσωπα των ανθρώπων για να εξαπατήσουν τα συστήματα αναγνώρισης προσώπου, αλλά η τεχνολογία αποδείχθηκε πιο δύσκολη από την αποτύπωση δακτυλικών αποτυπωμάτων ή τεχνολογίας αναγνώρισης φωνής στο παρελθόν".

Κεφάλαιο 4
Προσωπικά δεδομένα

Μέχρι τώρα η βιομετρική τεχνολογία λειτουργούσε σε αρκετά κλειστά περιβάλλοντα. Το υπάρχον νομικό πλαίσιο δεν παρεμποδίζει δημόσιες και ιδιωτικές πρωτοβουλίες από το να αναπτυχθούν τέτοιου είδους εφαρμογές. Η ανάπτυξη των βιομετρικών δεν απειλεί διαδικαστικά δικαιώματα, όπως δικαιώματα στο δικαστήριο.

Αν και το γεγονός ότι έχουν δημιουργηθεί κάποια ζητήματα εξαιτίας του νομικού πλαισίου που ισχύει για την προστασία δεδομένων, αυτό δεν αποτέλεσε εμπόδιο για τις πρόσφατες επιλογές για τα βιομετρικά στα ευρωπαϊκά διαβατήρια. Όμως η ευρεία εφαρμογή τους και ο φόβος μιας κοινωνίας "επιτήρησης" εξαιτίας του "φαινομένου της διάχυσης", επιβάλλουν την αναθεώρηση των διαθέσιμων νομικών εργαλείων.

Αν εξαιρέσουμε την ανάλυση DNA, την αναγνώριση δακτυλικών αποτυπωμάτων και την αναγνώριση προσώπου, δεν υπάρχει αρκετή νομοθεσία στην Ευρώπη που να αφορά τα

βιομετρικά. Τα βιομετρικά που χρησιμοποιούνται σε ιδιωτικές συνδιαλλαγές βασίζονται στη συγκατάβαση. Όταν όμως η χρήση τους γίνεται υποχρεωτική, όπως για παράδειγμα στα ηλεκτρονικά διαβατήρια, θα χρειαστεί καινούρια νομοθεσία.

Πολύ σημαντική είναι η ιδιωτικότητα, ένα θεμελιώδες δικαίωμα όπως αναφέρεται στο άρθρο 8 της Ευρωπαϊκής Συνθήκης για την Προστασία των Ανθρώπινων Δικαιωμάτων και θεμελιωδών ελευθεριών. Ανάμειξη στα δικαιώματα και στις ελευθερίες του ατόμου θα πρέπει να απαγορεύεται ρητά, εκτός και αν συντρέχει νόμιμος λόγος για να γίνει κάτι τέτοιο. Τα περισσότερα βιομετρικά δεν απαιτούν διείσδυση στο ανθρώπινο σώμα, οπότε μπορεί να υποτεθεί ότι η χρήση αυτών των τεχνολογιών δεν θα θεωρηθεί αδικαιολόγητα παρεμβατική όταν βασίζεται στο νόμο ή τη συγκατάθεση.

Οπότε κάθε εφαρμογή , όπως η χρησιμοποίηση βιομετρικών στα διαβατήρια και στο σύστημα της Visa από τον Ευρωπαίο νομοθέτη, θα πρέπει να εκπληρώνει τέσσερις προϋποθέσεις: αξιοπιστία, αναλογικότητα, την ύπαρξη επιλογής υποχώρησης και τη συγκατάθεση ή την εξ' αρχής γνώση. Ακόμα κι αν υπάρξουν διαφωνίες με την τωρινή ευρωπαϊκή νομοθεσία, όταν αυτές οι τέσσερις προϋποθέσεις εκπληρώνονται, οι αποφάσεις τηρούν την Ευρωπαϊκή Συνθήκη των Ανθρωπίνων Δικαιωμάτων.

Πρωταρχικά, θα πρέπει να αποφασιστεί το κατά πόσο τα βιομετρικά θα επιτρέπονται και πότε. Η ανάπτυξη εννοιών όπως "βιομετρική ανωνυμία" και "δικαίωμα ιδιοκτησίας βιομετρικών δεδομένων", ίσως βοηθήσει στην επίτευξη αυτού του στόχου. Μόλις ο νομοθέτης καθορίσει τη νόμιμη χρήση τους, έπεται ενίσχυση των διαθέσιμων εργαλείων διαφάνειας. Μόνο μετά την αναγνώριση της νόμιμης χρήσης των βιομετρικών διαδικασιών, θα πρέπει να καθοριστούν κανόνες και συνθήκες ορθής χρήσης. Συνεπώς υπάρχει ανάγκη βασικών αρχών, όπως: ισότητα πρόσβασης στο δίκτυο, απόλυτη ακρίβεια στόχευσης από κλειστά συστήματα παρακολούθησης, συστήματα που θα εξασφαλίζουν την ακρίβεια των δεδομένων που διατηρούνται από τέτοια συστήματα, μηχανισμούς τροποποίησης ψεύδους, μη ακριβή ή τροποποιημένα δεδομένα, συστήματα για να προστατευθούν οι χρήστης από την κλίση τους να ανταλλάσσουν την ιδιωτικότητά τους. Αυτό το βιομετρικό πλαίσιο θα πρέπει να είναι βασισμένο σε κατάλληλη ανάλυση επικινδυνότητας (risk assessment), το οποίο διακρίνει τη νόμιμη από τη μη νόμιμη χρήση των βιομετρικών.

Από τη στιγμή που η ανάλυση DNA προσφέρει πολύ μεγαλύτερη ασφάλεια και αξιοπιστία από παλαιότερες μεθόδους συλλογής αποδεικτικών στοιχείων, υπάρχει ο κίνδυνος ότι οι δικαστές θα

μπουν στη διαδικασία να παραχωρήσουν πολύ σημαντικό ρόλο στη λήψη αποφάσεων στη συγκεκριμένη βιομετρική τεχνική (με την προϋπόθεση ότι η διαδικασία γίνεται σωστά και από πιστοποιημένους οργανισμούς).

Αυτό μπορεί να είναι επιζήμιο στο σύστημα της ελεύθερης αξιολόγησης των αποδείξεων από τους δικαστές. Αυτή η προειδοποίηση μπορεί να γενικευτεί σε όλες τις βιομετρικές τεχνικές και σε όλα τα συστήματα συλλογής αποδείξεων στην Ευρώπη. Όποτε οι έρευνες γίνονται πολύπλοκες και οι μέθοδοι της έρευνας γίνονται επίσημες, το αποτέλεσμα θα γίνεται όλο και πιο δύσκολο να αξιολογηθεί από το δικαστήριο και την υπεράσπιση. Για να αποτρέψουμε τους ειδικούς να πάρουν τη θέση των δικαστών, χρειάζεται νόμιμη αναγνώριση του δικαιώματος της αντεξέτασης.

Στα βιομετρικά συστήματα ασφαλείας η κατασκευή προφίλ γίνεται για ταυτοποίηση, με μερικό τρόπο, υπό συγκεκριμένο πλαίσιο λειτουργίας και για έναν συγκεκριμένο σκοπό, όπως η εκχώρηση πρόσβασης. Θα πρέπει να σημειωθεί, όπως θα δούμε και παρακάτω, ότι και η σύνδεση με προφίλ (profiling) αντιπροσωπεύει μια έννοια η οποία μπορεί να σχετίζεται με την ταυτοποίηση. Ο όρος αυτός αφορά στη διαδικασία κατασκευής ή εφαρμογής ενός προφίλ ενός ατόμου ή μιας ομάδας. Ένα προφίλ αποτελείται από πρότυπα συσχετισμένων δεδομένων.

Στα βιομετρικά συστήματα τα οποία εξετάζονται στα πλαίσια της παρούσας διατριβής, τα χαρακτηριστικά του ατόμου συλλέγονται και επεξεργάζονται με σκοπό τη δημιουργία προσωπικού προφίλ για αναγνώριση ή ταυτοποίηση προσώπου, Εν τούτοις, το θέμα της συλλογής και επεξεργασίας δεδομένων από την καθημερινή ζωή ανθρώπων και δει ατόμων που ενδεχομένως να μη μπορούν να παρέχουν επί γνώσει συναίνεση (informed consent) εγείρει διάφορα ερωτήματα νομικής και ηθικής φύσεως.

4.1 Ορισμοί

Προσωπικά δεδομένα είναι κάθε πληροφορία που αναφέρεται στο πρόσωπο του κάθε ατόμου, όπως: το όνομα και το επάγγελμά του, η οικογενειακή του κατάσταση, η ηλικία του, ο τόπος κατοικίας, η φυλετική του προέλευση, τα πολιτικά του φρονήματα, η θρησκεία που πιστεύει, οι φιλοσοφικές του απόψεις, η συνδικαλιστική του δράση, η υγεία του, η ερωτική του ζωή και οι τυχόν ποινικές του διώξεις και καταδίκες.

Δεν θεωρούνται προσωπικά δεδομένα πληροφορίες από τις οποίες δεν δύναται να ταυτοποιηθεί ένα συγκεκριμένο άτομο.

Ευαίσθητα προσωπικά δεδομένα

Από τα παραπάνω προσωπικά δεδομένα πολλά είναι ευαίσθητα, έχουν δηλαδή ιδιαίτερη βαρύτητα για το σχηματισμό της εικόνας της προσωπικότητάς του ατόμου. Αυτά είναι η φυλετική ή εθνική προέλευση, τα πολιτικά φρονήματα, οι θρησκευτικές ή φιλοσοφικές πεποιθήσεις, η συμμετοχή σε ένωση, σωματείο και συνδικαλιστική οργάνωση, η υγεία, η κοινωνική πρόνοια και η ερωτική ζωή καθώς και τα σχετικά με ποινικές διώξεις ή καταδίκες.

Υποκείμενο των δεδομένων

Ως Υποκείμενο των δεδομένων ορίζεται το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική.

Επεξεργασία δεδομένων προσωπικού χαρακτήρα

Επεξεργασία δεδομένων προσωπικού χαρακτήρα λέγεται κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή.

Υπεύθυνος επεξεργασίας

Υπεύθυνος επεξεργασίας προσωπικών δεδομένων είναι οποιοσδήποτε καθορίζει τον σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός. Όταν ο σκοπός και ο τρόπος της επεξεργασίας καθορίζονται με διατάξεις νόμου ή κανονιστικές διατάξεις εθνικού ή

κοινοτικού δικαίου, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια βάσει των οποίων γίνεται η επιλογή του καθορίζονται αντίστοιχα από το εθνικό ή το κοινοτικό δίκαιο.

Εκτελών την επεξεργασία

Εκτελών την επεξεργασία λέγεται οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπεύθυνου επεξεργασίας, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός.

Τρίτος

Ως τρίτος ορίζεται κάθε φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία, ή οποιοσδήποτε άλλος οργανισμός, εκτός από το υποκείμενο των δεδομένων, τον υπεύθυνο επεξεργασίας και τα πρόσωπα που είναι εξουσιοδοτημένα να επεξεργάζονται τα δεδομένα προσωπικού χαρακτήρα, εφόσον ενεργούν υπό την άμεση εποπτεία ή για λογαριασμό του υπεύθυνου επεξεργασίας.

Για να έχει κάποιος φορέας ή φυσικό πρόσωπο δικαίωμα επεξεργασίας των προσωπικών δεδομένων άλλου ατόμου, πρέπει να πληρούνται οι παρακάτω προϋποθέσεις:

- Η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνον όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του. Κατ' εξαίρεση επιτρέπεται η επεξεργασία και χωρίς τη συγκατάθεση, όταν:

- Η επεξεργασία είναι αναγκαία για την εκτέλεση σύμβασης, στην οποία συμβαλλόμενο μέρος είναι υποκείμενο δεδομένων ή για τη λήψη μέτρων κατόπιν αιτήσεως του υποκειμένου .

- Η επεξεργασία είναι αναγκαία για την εκπλήρωση υποχρεώσεως του υπεύθυνου επεξεργασίας, η οποία επιβάλλεται από το νόμο.

- Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου, εάν αυτό τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

- Η επεξεργασία είναι αναγκαία για την εκτέλεση έργου δημόσιου συμφέροντος ή έργου που εμπίπτει στην άσκηση δημόσιας εξουσίας και εκτελείται από δημόσια αρχή ή έχει ανατεθεί

από αυτή είτε στον υπεύθυνο επεξεργασίας είτε σε τρίτο, στον οποίο γνωστοποιούνται τα δεδομένα.

- Η επεξεργασία είναι απολύτως αναγκαία για την ικανοποίηση του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ή ο τρίτος ή οι τρίτοι στους οποίους ανακοινώνονται τα δεδομένα και υπό τον όρο ότι τούτο υπερέχει προφανώς των δικαιωμάτων και συμφερόντων των προσώπων στα οποία αναφέρονται τα δεδομένα και δεν θίγονται οι θεμελιώδεις ελευθερίες αυτών.

Η Αρχή Προστασίας Προσωπικών Δεδομένων μπορεί να εκδίδει ειδικούς κανόνες επεξεργασίας για τις πλέον συνήθεις κατηγορίες επεξεργασιών και αρχείων, οι οποίες προφανώς δεν θίγουν τα δικαιώματα και τις ελευθερίες των προσώπων στα οποία αναφέρονται τα δεδομένα. Οι κατηγορίες αυτές προσδιορίζονται με κανονισμούς που καταρτίζει η Αρχή και κυρώνονται με προεδρικά διατάγματα, τα οποία εκδίδονται με πρόταση του Υπουργού Δικαιοσύνης. Σύμφωνα με αποφάσεις της Αρχής Προστασίας Προσωπικών Δεδομένων η δημοσίευση φωτογραφιών που έχουν ληφθεί σε δημόσιους χώρους δεν θεωρούνται παραβίαση ή επεξεργασία προσωπικών δεδομένων εφόσον ο σκοπός της δημοσίευσης είναι πολιτιστικός, καλλιτεχνικός, ενημερωτικός, δημοσιογραφικός, εκπαιδευτικός ή ιστοριογραφικός καθώς το δικαίωμα λήψης φωτογραφιών σε δημόσιους χώρους και δημοσίευσης αυτών καλύπτεται από τα άρθρα 5, 14, και 16 του Συντάγματος.

Επεξεργασία προσωπικών δεδομένων

Τα δεδομένα προσωπικού χαρακτήρα για να τύχουν νόμιμης επεξεργασίας πρέπει :

- Να συλλέγονται για καθορισμένους, σαφείς και νόμιμους σκοπούς και να υφίστανται θεμιτή και νόμιμη επεξεργασία ενόψει των σκοπών αυτών.

- Να είναι συναφή, πρόσφορα, και όχι περισσότερα από όσα κάθε φορά απαιτείται για τους σκοπούς της επεξεργασίας.

- Να είναι ακριβή και, εφόσον χρειάζεται, να υποβάλλονται σε ενημέρωση.

- Να διατηρούνται σε μορφή που να επιτρέπει τον προσδιορισμό της ταυτότητας των υποκειμένων τους μόνο κατά τη διάρκεια της περιόδου που απαιτείται, κατά την κρίση της Αρχής Προστασίας Προσωπικών Δεδομένων, για την πραγματοποίηση των σκοπών της

συλλογής τους και της επεξεργασίας τους. Μετά την παρέλευση της περιόδου αυτής, η Αρχή μπορεί, με αιτιολογημένη απόφασή της, να επιτρέπει τη διατήρηση δεδομένων προσωπικού χαρακτήρα για ιστορικούς, επιστημονικούς ή στατιστικούς σκοπούς, εφόσον κρίνει ότι δεν θίγονται σε κάθε συγκεκριμένη περίπτωση τα δικαιώματα των υποκειμένων τους ή και τρίτων.

Δεδομένα προσωπικού χαρακτήρα που έχουν συλλεχθεί ή υφίστανται επεξεργασία κατά παράβαση του νόμου πρέπει να καταστρέφονται με ευθύνη του υπεύθυνου επεξεργασίας. Η Αρχή, εάν εξακριβώσει αυτεπαγγέλτως ή μετά από σχετική καταγγελία παράβαση των διατάξεων της προηγούμενης παραγράφου, επιβάλλει την διακοπή της συλλογής ή της επεξεργασίας και την καταστροφή των δεδομένων προσωπικού χαρακτήρα που έχουν ήδη συλλεχθεί ή έχουν επεξεργαστεί.

Επεξεργασία ευαίσθητων προσωπικών δεδομένων

Συγκεκριμένα για τα ευαίσθητα προσωπικά δεδομένα, ισχύουν τα εξής: Απαγορεύεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων. Κατ΄ εξαίρεση επιτρέπεται η συλλογή και η επεξεργασία ευαίσθητων δεδομένων, καθώς και η ίδρυση και λειτουργία σχετικού αρχείου, ύστερα από άδεια της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, όταν συντρέχουν μία ή περισσότερες από τις ακόλουθες προϋποθέσεις:

- Το υποκείμενο έδωσε τη γραπτή συγκατάθεσή του, εκτός εάν η συγκατάθεση έχει αποσπασθεί με τρόπο που αντίκειται στο νόμο ή τα χρηστά ήθη.

- Η επεξεργασία είναι αναγκαία για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου ή προβλεπόμενου από το νόμο συμφέροντος τρίτου, εάν το υποκείμενο τελεί σε φυσική ή νομική αδυναμία να δώσει τη συγκατάθεσή του.

- Η επεξεργασία αφορά δεδομένα που δημοσιοποιεί το ίδιο το υποκείμενο ή είναι αναγκαία για την αναγνώριση, άσκηση ή υπεράσπιση δικαιώματος ενώπιον δικαστηρίου ή πειθαρχικού οργάνου.

- Η επεξεργασία αφορά θέματα υγείας και εκτελείται από πρόσωπο που ασχολείται κατ' επάγγελμα με την παροχή υπηρεσιών υγείας και υπόκειται σε καθήκον εχεμύθειας ή σε

συναφείς κώδικες δεοντολογίας, υπό τον όρο ότι η επεξεργασία είναι απαραίτητη για την ιατρική πρόληψη, διάγνωση, περίθαλψη ή τη διαχείριση υπηρεσιών υγείας.

- Η επεξεργασία εκτελείται από Δημόσια Αρχή και είναι αναγκαία είτε για λόγους εθνικής ασφάλειας, είτε για την εξυπηρέτηση των αναγκών εγκληματολογικής ή σωφρονιστικής πολιτικής και αφορά τη διακρίβωση εγκλημάτων, ποινικές καταδίκες ή μέτρα ασφαλείας είτε για λόγους προστασίας της δημόσιας υγείας, είτε για την άσκηση δημόσιου φορολογικού ελέγχου ή δημόσιου ελέγχου κοινωνικών παροχών.

- Η επεξεργασία πραγματοποιείται για ερευνητικούς και επιστημονικούς αποκλειστικά σκοπούς και υπό τον όρο ότι τηρείται η ανωνυμία και λαμβάνονται όλα τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των προσώπων στα οποία αναφέρονται.

- Η επεξεργασία αφορά δεδομένα δημοσίων προσώπων, εφόσον αυτά συνδέονται με την άσκηση δημοσίου λειτουργήματος ή τη διαχείριση συμφερόντων τρίτων, και πραγματοποιείται αποκλειστικά για την άσκηση του δημοσιογραφικού επαγγέλματος. Η άδεια της Αρχής χορηγείται μόνο εφόσον η επεξεργασία είναι απολύτως αναγκαία για την εξασφάλιση του δικαιώματος πληροφόρησης επί θεμάτων δημοσίου ενδιαφέροντος καθώς και στο πλαίσιο καλλιτεχνικής έκφρασης και εφόσον δεν παραβιάζεται με οποιονδήποτε τρόπο το δικαίωμα προστασίας της ιδιωτικής και οικογενειακής ζωής.

Η Αρχή χορηγεί άδεια συλλογής και επεξεργασίας ευαίσθητων δεδομένων, καθώς και άδεια ιδρύσεως και λειτουργίας σχετικού αρχείου, ύστερα από αίτηση του υπεύθυνου επεξεργασίας. Εφόσον η Αρχή διαπιστώσει ότι πραγματοποιείται επεξεργασία ευαίσθητων δεδομένων, η γνωστοποίηση αρχείου επέχει θέση αιτήσεως για τη χορήγηση άδειας. Η Αρχή μπορεί να επιβάλλει όρους και προϋποθέσεις για την αποτελεσματικότερη προστασία του δικαιώματος ιδιωτικής ζωής των υποκειμένων ή τρίτων. Πριν χορηγήσει την άδεια, η Αρχή καλεί σε ακρόαση τον υπεύθυνο επεξεργασίας ή τον εκπρόσωπο του και τον εκτελούντα την επεξεργασία.

Η άδεια εκδίδεται για ορισμένο χρόνο, ανάλογα με τον σκοπό της επεξεργασίας. Μπορεί να ανανεωθεί ύστερα από αίτηση του υπεύθυνου επεξεργασίας.

4.2 Παράγοντες για τη αποδοχή των χρηστών

Εγείρονται κάποια θέματα ηθικής όσον αφορά τη χρησιμοποίηση των βιομετρικών. Η συλλογή κάποιων βιομετρικών πληροφοριών όπως τα δακτυλικά αποτυπώματα, είναι συσχετισμένη με εγκληματίες στο μυαλό πολλών ανθρώπων. Παραδοσιακά, λεπτομερείς βιομετρικές πληροφορίες συγκεντρώνονται από μεγάλους οργανισμούς, όπως η αστυνομία και ο στρατός. Οι άνθρωποι ίσως νιώσουν ότι χάνεται η έννοια της ιδιωτικότητας και την προσωπικής αξιοπρέπειας. Αυτόματη αναγνώριση προσώπων σε δημόσια μέρη, μπορεί να χρησιμοποιηθεί έτσι ώστε κάποιος να παρακολουθείτε χωρίς να το ξέρει ή να έχει δώσει τη συγκατάθεσή του. Οι άνθρωποι νιώθουν ντροπή όταν σε ένα δημόσιο μέρος απορρίπτονται από έναν αναγνώστη (scanner). Επίσης όσον αφορά το γενετικό υλικό, κάποιες θρησκείες απαγορεύουν τη λήψη αίματος, καθώς και συστήματα που αναλύουν το γενετικό υλικό χρησιμοποιώντας ανθρώπινες τρίχες θα απέκλειαν τους ανθρώπους χωρίς μαλλιά. Ανησυχίες επίσης υπάρχουν και με τον τρόπο αποθήκευσης των πληροφοριών και πού θα αποθηκεύονται. Δεν είναι δηλαδή κάποιες κάρτες που θα μπορούσαν να φυλάσσονται σε ένα ασφαλές κτήριο. Είναι ηλεκτρονικές πληροφορίες που εύκολα μεταφέρονται και αντιγράφονται. Επίσης ποιος θα έχει πρόσβαση σε αυτές τις πληροφορίες. Για παράδειγμα μεγάλες εταιρείες θα έχουν πρόσβαση σε βιομετρικά προσώπου, επιτρέποντας την αναγνώριση πελατών σε καταστήματα. Πως θα σας φαινόταν να μπαίνατε σε ένα πολυκατάστημα που δεν έχετε πάει ποτέ πιο πριν και ο πωλητής να σας υποδεχτεί γνωρίζοντας το μικρό σας όνομα, αφού πρώτα διαβάσει μια σύντομη περίληψη των στοιχείων σας και των τελευταίων αγορών σας;

4.3 Αποδοχή των βιομετρικών συστημάτων

Οι άνθρωποι από τη φύση τους δεν εμπιστεύονται νέες τεχνολογίες που εννοιολογικά δεν γνωρίζουν .Και όταν ακούει κάποιος για πρώτη φορά Σύστημα Βιομετρικής τεχνολογίας, συνήθως δεν μπορεί να καταλάβει τι σημαίνει. Έτσι λοιπόν με το παραπάνω οι ίδιοι αυτοί άνθρωποι μπορούν να θεωρήσουν ότι η μυστικότητά των δεδομένων τους μπορεί να απειληθεί με τη χρήση αυτών των βιομετρικών μεθόδων. Είναι πολύ σημαντικό λοιπόν να κατανοήσει ο κάθε νέος χρήστης την έννοια, τον ρόλο καθώς και τη σημαντικότητα της δημιουργίας των βιομετρικών συστημάτων για την ασφάλεια κάθε πληροφορίας, για να μπορέσει να τα

αποδεχτεί. Και για να κατανοήσουν όλα τα παραπάνω θα πρέπει οι εκπρόσωποι αυτών των συστημάτων να τους βοηθήσουν.

Για να επιτευχθεί όμως η αποδοχή, η συνεργασία χρηστών είναι απαραίτητη για πολλές εφαρμογές της βιομετρικής τεχνολογίας. Υπάρχουν τρεις σημαντικοί παράγοντες που οδηγούν στην αποδοχή των χρηστών:

1. Οι χρήστες έχουν την ανάγκη για αυξανόμενη ασφάλεια, και θεωρούν ότι η βιομετρική τεχνολογία μπορεί να αυξήσει την ασφάλεια.

2. Τα βιομετρικά συστήματα είναι καταλληλότερα στο να χρησιμοποιούνται σε σχέση με τα προηγούμενα/εναλλακτικά συστήματα.

3. Οι χρήστες εμπιστεύονται εκείνα τα συστήματα που προστατεύουν τα στοιχεία τους κρατώντας τα ασφαλή και όχι τα συστήματα που χρησιμοποιούν για οποιονδήποτε άλλο σκοπό.

Παρακάτω παραθέτω και κάποιου ακόμη λόγους για τους οποίους πολλές οι χρήστες μπορεί να είναι διστακτικοί στη χρήση βιομετρικών τεχνολογιών. Για την ασφαλή (μακροπρόθεσμη) χρήση των συστημάτων (πολλοί χρήστες έχουν ανησυχίες για την διαδικασία αναγνώρισης της ίριδας θεωρώντας ότι είναι καταστρεπτικό για τα μάτια τους, όπως επίσης ανησυχούν για το ότι οι εγκληματίες θα κόψουν τα δάχτυλά τους ή θα αφαιρέσουν τα μάτια τους για να αποκτήσουν πρόσβαση στα συστήματα αυτά). Πολλοί χρήστες ανησυχούν για την αξιοπιστία της αναγνώρισης (π.χ. όταν κάποιο βιομετρικό σύστημα διαπράξει κάποιο λάθος και δώσει πρόσβαση σε κάποιο κακόβουλο χρήστη). Ανησυχούν για το αν τα στοιχεία τους χρησιμοποιούνται για άλλο εκτός από τον προοριζόμενο σκοπό (π.χ. διάγνωση υγείας, υποκλοπή, άμεσο μάρκετινγκ). Ανησυχούν για την αποτελεσματικότητα ή την υποχρέωση των συστημάτων αυτών που φυλάσσουν τα στοιχεία τους για το αν μπορούν να τα κρατήσουν ασφαλή από τους εσωτερικούς και εξωτερικούς επιτιθεμένους (κακόβουλοι υπάλληλοι, χάκερ κ.α).

4.4 Κατευθύνσεις για τη χρήση Βιομετρικών μεθόδων

Η προστασία των προσωπικών δεδομένων και της ιδιωτικής ζωής αποτελεί θεμελιώδες αν-θρώπινο δικαίωμα. Ο νόμος παρέχει ορισμένα δικαιώματα στα φυσικά πρόσωπα (τα υποκείμενα των δεδομένων) και θέτει συγκεκριμένες υποχρεώσεις σε όσους τηρούν και επεξεργάζονται προ-σωπικά δεδομένα (τους υπευθύνους επεξεργασίας).Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) είναι συνταγματικά κα-τοχυρωμένη ανεξάρτητη Αρχή. Η ΑΠΔΠΧ ιδρύθηκε με το νόμο 2472/1997, ο οποίος ενσωματώνει στο ελληνικό δίκαιο την Ευρωπαϊκή Οδηγία 95/46/ΕΚ. Η Οδηγία αυτή θέτει κανόνες για την προ-στασία των προσωπικών δεδομένων σε όλες τις χώρες της Ευρωπαϊκής Ένωσης. Επίσης, όσον α-φορά την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, η ΑΠΔΠΧ εφαρμόζει τον νόμο 3471/2006 που αντίστοιχα ενσωματώνει στο εθνικό δίκαιο την Ευρωπαϊκή Οδηγία 58/2002.Αποστολή της Αρχής αποτελεί η προστασία των δικαιωμάτων της προσωπικότητας και της ι-διωτικής ζωής του ατόμου στην Ελλάδα, σύμφωνα με τις διατάξεις των Ν. 2472/1997 και 3471/2006.Πρωταρχικός σκοπός της Αρχής είναι η προστασία του πολίτη από την παράνομη επεξεργα-σία των προσωπικών του δεδομένων αλλά και η συνδρομή προς αυτόν σε κάθε περίπτωση που δια-πιστώνεται παραβίαση των σχετικών δικαιωμάτων του σε κάθε επιχειρησιακό τομέα (χρηματοπι-στωτικά, υγεία, ασφάλιση, εκπαίδευση, δημόσια διοίκηση, μεταφορές, ΜΜΕ, κ.ο.κ.). Επίσης, σκοπός της Αρχής είναι η υποστήριξη και καθοδήγηση των υπεύθυνων επεξεργασίας στην εκπλήρωση των υποχρεώσεων τους απέναντι στο νόμο, λαμβάνοντας υπόψη τις νέες ανάγκες υπηρεσιών της ελληνικής κοινωνίας, καθώς και την διείσδυση των σύγχρονων ψηφιακών επικοινω-νιών και δικτύων. Ως εκ τούτου, η Αρχή στρέφει ιδιαίτερα την προσοχή της μεταξύ άλλων στην παρατήρηση και αντιμετώπιση ζητημάτων που προκύπτουν με την εξέλιξη των νέων τεχνολογιών και εφαρμογών.

1. Αρχείο γνωστοποιήσεων - Έκδοση αδειών. Οι υπεύθυνοι επεξεργασίας υποχρεούνται να υποβάλλουν γνωστοποίηση προς την Αρχή όσον αφορά στη σύσταση και λειτουργία αρχείου, λαμβάνοντας υπόψη τις εξαιρέσεις που αναφέρονται στον Ν. 2472/1997. Βάσει των ανωτέρω γνωστοποιήσεων και στις περιπτώσεις που αυτό απαιτείται από τον Ν. 2472/1997, η Αρχή εκδίδει άδειες για τη συλλογή και επεξεργασία δεδομένων προσωπι-κού χαρακτήρα, για τη διαβίβαση δεδομένων σε χώρες εκτός Ε.Ε. ή/και για τη διασύνδεση δεδομέ-νων. Οι άδειες χορηγούνται με συγκεκριμένους όρους και προϋποθέσεις για την αποτελεσματικότε-ρη προστασία του δικαιώματος της ιδιωτικής

ζωής των υποκειμένων ή τρίτων, ενώ η Αρχή απευθύ-νει υποδείξεις και συστάσεις σχετικά με το απόρρητο και την ασφάλεια της επεξεργασίας.

2. Διενέργεια διοικητικών ελέγχων. Η Αρχή ενεργεί αυτεπαγγέλτως ή κατόπιν καταγγελίας διοικητικούς ελέγχους σε αρχεία, τόσο του δημόσιου όσο και του ιδιωτικού τομέα. Οι έλεγχοι διενεργούνται από εντεταλμένους υπαλλή-λους του Τμήματος των Ελεγκτών, οι οποίοι συνοδεύονται σε περιπτώσεις που κρίνονται σημαντι-κές από μέλη της Αρχής. Οι διενεργούντες τον έλεγχο, ως ειδικοί ανακριτικοί υπάλληλοι, έχουν δι-καίωμα πρόσβασης σε κάθε αρχείο χωρίς να μπορεί να τους αντιταχθεί κανενός είδους απόρρητο. Κατά τον έλεγχο εξετάζεται καταρχήν η εναρμόνισή του ελεγχόμενου με τις απαιτήσεις των Ν.2472/97, 3471/2006 (γνωστοποίηση, ενημέρωση, λοιπές υποχρεώσεις κατά περίπτωση, αποδει-κτικά στοιχεία). Στη συνέχεια πραγματοποιείται έλεγχος του πληροφοριακού του συστήματος, όπου σύμφωνα με τα άρθρα 6 και 10 του ν. 2472/1997, εξετάζονται τα βασικά χαρακτηριστικά του συ-στήματος, η φύση των δεδομένων, καθώς και το επίπεδο ασφαλείας που εξασφαλίζουν τα οργανω-τικά και τεχνικά μέτρα που έχει λάβει ο υπεύθυνος επεξεργασίας για την προστασία των δεδομέ-νων. Η ολοκλήρωση του ελέγχου οδηγεί στην σύνταξη πορίσματος το οποίο υποβάλλεται στην ο-λομέλεια της Αρχής. Η Αρχή ασκεί επίσης ανεξάρτητο έλεγχο στο εθνικό τμήμα του Συστήματος Πληροφοριών Σένγκεν, σύμφωνα με το άρθρο 114 παράγραφος 1 της Σύμβασης Εφαρμογής της Συμφωνίας Σένγκεν (ν. 2514/1997 ΦΕΚ 140 Α'), ασκεί τις αρμοδιότητες της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 23 της Σύμβασης ΕΥΡΩΠΟΛ (ν. 2605/1998 ΦΕΚ 88 Α'), και τις αρμοδιότητες της εθνικής εποπτικής αρχής που προβλέπεται στο άρθρο 17 της Σύμβασης για τη χρήση της πληροφο-ρικής στον τελωνειακό τομέα (ν. 2706/1999 ΦΕΚ 77 Α'), καθώς και τις αρμοδιότητες εποπτείας που προκύπτουν από οποιαδήποτε άλλη διεθνή συμφωνία.

3. Εξέταση προσφυγών-καταγγελιών-ερωτημάτων Η ΑΠΔΠΧ εξετάζει παράπονα και ερωτήματα σχετικά με την εφαρμογή του νόμου και την προστασία των δικαιωμάτων των αιτούντων όταν αυτά θίγονται από την επεξεργασία δεδομένων και εκδίδει σχετικές Αποφάσεις. Επίσης, επιβάλλει στους υπεύθυνους επεξεργασίας ή στους τυχόν εκπροσώπους τους διοικητικές κυρώσεις, για παράβαση των υποχρεώσεών τους που απορρέουν από τον νόμο 2472/97 και από κάθε άλλη ρύθμιση που αφορά την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

4. Τέλος, η Αρχή μπορεί να καταγγέλλει τις παρα-βάσεις των διατάξεων του νόμου στις αρμόδιες διοικητικές και δικαστικές αρχές.

Παράλληλα ωστόσο, από τον Μάιο του 2018 έχει τεθεί σε εφαρμογή και ο Ευρωπαϊκός κανονισμός προστασίας προσωπικών δεδομένων.

Ο Γενικός Κανονισμός Προστασίας Δεδομένων (General Data Protection Regulation / GDPR, https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679) («Κανονισμός») περιλαμβάνει το νέο νομικό πλαίσιο για την προστασία δεδομένων. Δημοσιεύθηκε στις 27 Απριλίου 2016 και τίθεται σε εφαρμογή από τις 25 Μαΐου 2018. Ο Κανονισμός έχει άμεση εφαρμογή σε όλα τα κράτη μέλη της Ευρωπαϊκής Ένωσης και δεν χρειάζεται τα τελευταία να ενσωματώσουν τις διατάξεις του στην εθνική νομοθεσία τους. Στην Ελλάδα αναμένεται η ψήφιση νόμου για την προστασία δεδομένων προσωπικού χαρακτήρα, το δε νομοσχέδιο είναι δημοσιευμένο στην διεύθυνση http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf. Με το νέο νόμο θα καταργηθεί ο ισχύον Νόμος 2472/1997 και θα τεθούν σε ισχύ διατάξεις που συμπληρώνουν τον Κανονισμό και εξειδικεύουν ορισμένες από τις υποχρεώσεις που θεσπίζει ο Κανονισμός.

Ο Κανονισμός εισάγει αρκετές αλλαγές στο προηγούμενο νομικό καθεστώς για την προστασία των φυσικών προσώπων αναφορικά με την επεξεργασία των προσωπικών δεδομένων τους και θεσπίζει αυξημένες υποχρεώσεις για οποιονδήποτε οργανισμό επεξεργάζεται προσωπικά δεδομένα.

Κατάργηση γνωστοποιήσεων / αδειών: Πλέον δεν απαιτείται προηγούμενη γνωστοποίηση της επεξεργασίας δεδομένων στην αρχή προστασίας δεδομένων ούτε είναι απαραίτητο να ληφθεί προηγούμενη άδεια της αρχής σε περιπτώσεις επεξεργασίας ευαίσθητων δεδομένων (ή «ειδικών κατηγοριών δεδομένων» σύμφωνα με τους όρο που χρησιμοποιείται στον Κανονισμό), όπως τα δεδομένα που αφορούν την υγεία. Είναι όμως αναγκαίο να λαμβάνονται τα απαραίτητα μέτρα για την προστασία των δικαιωμάτων των ατόμων. Όσοι επεξεργάζονται προσωπικά δεδομένων θα πρέπει να είναι σε θέση να αποδεικνύουν τη συμμόρφωσή τους με το νέο νομικό πλαίσιο και να ενημερώνουν αντίστοιχα την αρμόδια αρχή και τα ενδιαφερόμενα πρόσωπα.

Αρχή της Λογοδοσίας: Ο Κανονισμός εισάγει την αρχή της «λογοδοσίας», που σημαίνει ότι όσοι επεξεργάζονται προσωπικά δεδομένα δεν αρκεί να συμμορφώνονται με τις υποχρεώσεις τους, αλλά πρέπει και να είναι σε θέση να αποδείξουν τη συμμόρφωσή τους. Συγκεκριμένα, πρέπει να

τηρούν επικαιροποιημένα αρχεία των δραστηριοτήτων επεξεργασίας προσωπικών δεδομένων καθώς και να εφαρμόζουν διαδικασίες που αντανακλούν όλες τις αρχές τις επεξεργασίας και αντιμετωπίζουν ορθά οποιαδήποτε αιτήματα προβάλλουν τα υποκείμενα των δεδομένων. Όποιος επεξεργάζεται προσωπικά δεδομένα πρέπει να ορίζει και να καταγράφει τη νομική βάση και τον σκοπό της επεξεργασίας και να προάγει την διαφάνεια κάθε επεξεργασίας. Σε ορισμένες περιπτώσεις, όπως αναφέρεται κατωτέρω, εκείνοι που επεξεργάζονται προσωπικά δεδομένα χρειάζεται να διενεργούν Εκτιμήσεις Αντικτύπου σχετικά με την Προστασία Δεδομένων, όταν η επεξεργασία δεδομένων είναι υψηλού ρίσκου, και να διορίζουν, εφόσον απαιτείται, Υπεύθυνο Προστασίας Δεδομένων.

Αρχές Επεξεργασίας & Ενισχυμένα δικαιώματα των υποκειμένων: Ο Κανονισμός ορίζει πλέον με σαφή τρόπο τις βασικές αρχές που πρέπει να τηρούνται σε κάθε επεξεργασία προσωπικών δεδομένων και ενισχύει τα δικαιώματα των επηρεαζόμενων προσώπων.

Επεξεργασία προσωπικών δεδομένων χωρεί μόνο όταν πληρούνται τα κριτήρια που θέτει η νομοθεσία για την προστασία των δεδομένων. Όποιος επεξεργάζεται προσωπικά δεδομένα οφείλει να τηρεί τις αρχές του Κανονισμού, όπως η ελαχιστοποίηση των δεδομένων, η ακρίβεια, η ακεραιότητα και η εμπιστευτικότητα των δεδομένων, κτλ.

Αυστηρότερες προϋποθέσεις για να είναι έγκυρη η συναίνεση: Όταν η επεξεργασία των δεδομένων βασίζεται στην συγκατάθεση του ατόμου, θα πρέπει να διασφαλίζεται, επιπλέον των κριτηρίων που είχαν τεθεί από το προηγούμενο νομικό πλαίσιο, ότι η συγκατάθεση είναι σαφής και λεπτομερής. Πριν συναινέσει πρέπει να έχει ενημερωθεί επαρκώς σχετικά με το ποιος θα επεξεργαστεί τα δεδομένα του και για ποιο σκοπό. Ειδικά για τα δεδομένα υγείας, όταν η επεξεργασία τους βασίζεται σε συγκατάθεση, πρέπει αυτή να είναι ρητή.

Νέα δικαιώματα: Στα υποκείμενα των δεδομένων παρέχονται περισσότερα δικαιώματα σε σχέση με το προηγούμενο καθεστώς (δικαίωμα διαγραφής – «δικαίωμα στη λήθη», δικαίωμα στη φορητότητα δεδομένων, κτλ.).

Προστασία Δεδομένων εκ του σχεδιασμού: Τα μέτρα για την προστασία των προσωπικών δεδομένων πρέπει να λαμβάνονται ήδη από τον σχεδιασμό των διαδικασιών και εξ ορισμού.

Συνεργασία με τρίτους για επεξεργασία δεδομένων: Όποιος επεξεργάζεται προσωπικά δεδομένα θα πρέπει να εφαρμόζει νέες προδιαγραφές στις συνεργασίες του με τρίτα μέρη, οι οποίοι

ενδέχεται να ενεργούν ως υπεύθυνοι ή συνυπεύθυνοι της επεξεργασίας ή εκτελούντες την επεξεργασία.

Γνωστοποίηση παραβιάσεων: Σε περίπτωση διαπιστωμένης παραβίασης προσωπικών δεδομένων θα πρέπει να γίνεται γνωστοποίηση στην αρμόδια εποπτική αρχή με τον τρόπο και εντός της προθεσμίας που προβλέπεται από το νομικό πλαίσιο. Περισσότερες λεπτομέρειες για τις παραπάνω έννοιες (αρχές, δικαιώματα, τεχνικά και οργανωτικά μέτρα, υποχρεώσεις γνωστοποίησης παραβίασης προσωπικών δεδομένων) θα βρείτε στις επόμενες ενότητες.

Κίνδυνος μη συμμόρφωσης: Ο Κανονισμός αυξάνει σημαντικά τους κινδύνους εκ της μη συμμόρφωσης για τα φυσικά ή νομικά πρόσωπα που επεξεργάζονται δεδομένα. Τα πρόστιμα που προβλέπονται σε περίπτωση παραβίασης της νομοθεσίας για την προστασία των προσωπικών δεδομένων μπορούν να αγγίξουν τα 20 εκατομμύρια Ευρώ ή το 4% του ετήσιου παγκόσμιου κύκλου εργασιών, ανάλογα με το ποιο είναι υψηλότερο. Επιπρόσθετα, αυξάνονται οι ελεγκτικές αρμοδιότητες των αρχών για την προστασία των προσωπικών δεδομένων, οι οποίες μπορούν να διενεργούν ελέγχους και επιτόπιες εφόδους, πρόσβαση στα προσωπικά δεδομένα που αποτελούν αντικείμενο επεξεργασίας, κτλ.

4.5 Βασικές αρχές που διέπουν το σύστημά μας

Σύμφωνα με τις γενικές αρχές προστασίας των προσωπικών δεδομένων, είναι σημαντικός ο τόπος αποθήκευσης των «προτύπων». Η αποθήκευση εξαρτάται κυρίως από το σκοπό εφαρμογής του βιομετρικού συστήματος καθώς και από το μέγεθος των προτύπων. Τα πρότυπα μπορούν να αποθηκευτούν:

- Στη μνήμη της βιομετρικής συσκευής
- Σε κεντρική βάση δεδομένων
- Σε πλαστικές ή έξυπνες κάρτες. Ο συγκεκριμένος τρόπος επιτρέπει στους χρήστες να έχουν μαζί τους τα βιομετρικά τους στοιχεία.

Συστήματα που επιτρέπουν την αποθήκευση των προτύπων σε μέσα που είναι υπό τον πλήρη έλεγχο του υποκειμένου θεωρούνται περισσότερο φιλικά ως προς την προστασία των προσωπικών δεδομένων.

Για αυτό ακριβώς το λόγο στην περίπτωση της υλοποίησής μας τα προσωπικά δεδομένα αποθηκεύονται στο σύνολό τους στα πληροφοριακά συστήματα του κάθε ιδρύματος/οργανισμού που θα χρησιμοποιεί την εφαρμογή. Το βιομετρικό δείγμα μπορεί να αποθηκευτεί σε μια εξωτερική βάση δεδομένων. Σε εκείνη την περίπτωση η βιομετρική πληροφορία πρέπει να σταλεί πέρα από το δίκτυο κάθε φορά που θέλει να ελεγχθεί ο χρήστης. Κατά τη διάρκεια της μεταφοράς οι πληροφορίες κρυπτογραφούνται, οι οποίες αποθηκεύονται στην εξωτερική βάση δεδομένων . Το πρόβλημα είναι ότι ο χρήστης δεν έχει κανέναν έλεγχο του βιομετρικού στοιχείου του. Οι πληροφορίες θα μπορούσαν να κλαπούν από τη βάση δεδομένων και να τροποποιηθούν, ή να χρησιμοποιηθούν με κάποιο ψευδή τρόπο. Ένα άλλο πρόβλημα είναι ο χρόνος απόκρισης: μπορεί να πάρει κάποιο χρόνο για να εκτελεσθεί η επαλήθευση των στοιχείων ενός χρήστη όταν οι πληροφορίες στέλνονται πέρα από το δίκτυο λόγω της υπερφόρτωσης και το μέγεθος του αρχείου. Ένα πλεονέκτημα είναι ότι , δεν απαιτεί τόση μνήμη όσο σε μία κινητή μονάδα εάν το δείγμα αποθηκεύεται στην εξωτερική βάση δεδομένων.

Το βιομετρικό σύστημα που υλοποιήσαμε στα πλαίσια της εργασίας θα μπορεί να λειτουργήσει αποκλειστικά σε δοκιμαστική βάση και δεν θα αντικαταστήσει τα υπάρχοντα συστήματα ελέγχου πρόσβασης. Η δοκιμαστική λειτουργία θα έχει ως εξής: κατά τη φάση της εγγραφής στο βιομετρικό σύστημα, θα λαμβάνονται μία ή περισσότερες φωτογραφίες των εθελοντών, από τα οποία θα παράγονται οι βιομετρικές τους «ταυτότητές». Οι πολλαπλές βιομετρικές ταυτότητες απαιτούνται όταν υπάρχουν διαβαθμισμένα δικαιώματα πρόσβασης για το ίδιο άτομο σε διαφορετικές εφαρμογές. Οι βιομετρικές ταυτότητες θα αποθηκεύονται στη συνέχεια σε κεντρική βάση δεδομένων στο σύστημα, μαζί με κάποια ακόμα στοιχεία των εθελοντών που απαιτούνται για την ταυτοποίησή τους, ήτοι ονοματεπώνυμο, φωτογραφία. Τα στοιχεία αυτά τηρούνται ήδη από τον υπεύθυνο επεξεργασίας για την σύνδεση στο πληροφοριακό σύστημα εξ αποστάσεως εκπαίδευσης. Βάσει των βιομετρικών ταυτοτήτων και των λοιπών δεδομένων θα ελέγχεται στη συνέχεια η είσοδος των εθελοντών στο πιλοτικό σύστημα. Μέρος της παραπάνω επεξεργασίας θα γίνεται από εκτελούντες την επεξεργασία. Τα δεδομένα του βιομετρικού συστήματος θα τηρούνται για ένα ορισμένο χρονικό διάστημα.

Θα πρέπει να τονίσουμε ότι σε κάθε περίπτωση που ο φοιτητής/σπουδαστής επιθυμεί να μη χρησιμοποιεί το σύστημα της αναγνώρισης προσώπου θα μπορεί να επιλέξει το αντίστοιχο πεδίο και τότε και μόνον τότε θα μπορεί να συνεχίσει στην χρήση της εφαρμογής. Σε αυτή την περίπτωση για την επιλογή του θα ενημερώνεται και η γραμματεία της σχολής.

Παράλληλα στην έως τώρα υλοποίηση δεν υπάρχει λειτουργία κατά την οποία ο φοιτητής/σπουδαστής θα μπορούσε να τροποποιήσει τις προσωπικές του φωτογραφίες. Η συγκεκριμένη λειτουργία προστίθεται στη λίστα των επεκτάσεων που σε μελλοντικό χρόνο μπορούν να υλοποιηθούν.

Κεφάλαιο 5
Σύνοψη

5.1 Σύνοψη

Η εργασία είχε ως στόχο την υλοποίηση ενός εργαλείου που θα παρέχει σε πλατφόρμες εξ αποστάσεως εκπαίδευσης τη δυνατότητα σύνδεσης των χρηστών με τη χρήση βιομετρικής αναγνώρισης και ποιο συγκεκριμένα με τη χρήση τεχνολογιών αναγνώρισης προσώπου.

Η υλοποίηση του εργαλείου ολοκληρώθηκε σε ακαδημαϊκά πλαίσια, καθώς υπάρχουν αρκετά σημεία όπως θα εμφανιστούν και στο επόμενο κεφάλαιο που είτε χρήζουν είτε απαιτούν περεταίρω ανάπτυξης. Η υλοποίηση έγινε με τη χρήση εργαλείων ανοιχτού κώδικα, ώστε να μην υπάρξει κόστος, αποδεχόμενοι για αυτό το σκοπό χαμηλότερα επίπεδα λειτουργικότητας.

Υπάρχει η δυνατότητα χρήσης του εργαλείου σε συνεργασία με την πλατφόρμα εξ αποστάσεως εκπαίδευσης Moodle στην έκδοση 3.1.3 της τελευταίας. Το εργαλείο που παράχθηκε από την εργασία μετά από μελέτη αποδείχθηκε ότι μπορεί να λειτουργεί με ένα threshold 75% στις

περιπτώσεις αναγνώρισης προσώπων κάτω υπό σχεδόν ιδανικές συνθήκες λειτουργίες ενώ παράλληλα είναι εύκολο τόσο στη χρήση, όσο στην εκπαίδευση των χρηστών και τη συντήρησή του.

Ένας ακόμη στόχος που επιτεύχθηκε ήταν η υλοποίηση του συστήματος βασιζόμενοι σε ένα μοντέλο χρήσης που όπως περιεγράφηκε δεν προσθέτει στους θεσμικούς λειτουργούς του εκάστοτε ιδρύματος που θα το χρησιμοποιήσουν περισσότερο φόρτο εργασίας από ότι έχουν μέχρι στιγμής επιμεριστεί.

Παράλληλα αποδείχθηκε ότι μειώνει το χρόνο που χρειάζονται οι χρήστες για τη σύνδεση σε ένα σύστημα εξ αποστάσεως εκπαίδευσης ενώ σε ιδανικά επίπεδα θα τους διευκολύνει καθώς δεν χρειάζεται πλέον να απομνημόνευση ενός ακόμη σετ ονόματος χρήστη κωδικού χρήστη.

Τέλος πρέπει να αναφερθεί ότι πρέπει έχουνε ληφθεί όλα τα μέτρα που μπορούν να εγγυηθούν τη ορθή συμμόρφωση με όλες της οδηγίες του Ευρωπαϊκού Κανονισμού Προστασίας Προσωπικών Δεδομένων.

5.2 Μελλοντική έρευνα

Όπως έχουμε ήδη αναφέρει και σε προηγούμενα κεφάλαια, η υλοποίηση του εργαλείου της αναγνώρισης προσώπου για συστήματα εξ αποστάσεως εκπαίδευσης έχει γίνει σε ακαδημαϊκό επίπεδο. Αυτό σημαίνει ότι υπάρχει ένα σύνολο από παραμέτρους που έχουνε μεν μελετηθεί όμως δεν έχουν υλοποιηθεί στο παραδοτέο αποτέλεσμα. Αυτές οι παράμετροι αποτελούν την απαρχή μίας συνεχούς ανάπτυξης και επέκτασης του εργαλείου που υλοποιήθηκε με στόχο την όσο το δυνατόν καλύτερη και ακριβέστερη λειτουργία χωρίς προβλήματα.

Αρχικά θα μπορούσαμε να επικεντρωθούμε στις παρακάτω κύριες κατηγορίες που αφήνουμε ως ιδέες για μελλοντική επέκταση του εργαλείου μας.

- Το εργαλείο θα πρέπει να μπορεί να αντιδρά καλύτερα και να παρέχει αναγνώριση των χρηστών και κάτω από ειδικές συνθήκες όπως ο χαμηλός φωτισμός ή η κακή ποιότητα

της κάμερας καθώς το υλικό που μπορεί να χρησιμοποιούν οι χρήστες υποθέτουμε ότι δεν θα είναι πάντα στην καλύτερη δυνατή κατάσταση.

- Το εργαλείο θα πρέπει να επεκταθεί με τέτοιο τρόπο ώστε να εφαρμοστεί και κάποιος αντίστοιχος αλγόριθμος αναγνώρισης της «ζωντάνιας» ενός προσώπου. Έτσι θα μπορούσε να αρνηθεί την είσοδο σε κάποιο κακόβουλο χρήστη ο οποίος θα προσπαθούνε να αποκτήσει πρόσβαση στην πλατφόρμα εξ αποστάσεως εκπαίδευσης σε περίπτωση που χρησιμοποιούσε ως είσοδο μία φωτογραφία ενός τρίτου προσώπου.

- Αυτή τη στιγμή το εργαλείο για να κάνει την ταυτοποίηση ενός προσώπου συγκρίνει το πρόσωπο της εισόδου με όλα αυτά που έχει στη βάση του έως ότου έχει κάποιο θετικό αποτέλεσμα ή έως ότου να μην υπάρχει άλλο πρόσωπο προς έλεγχο οπότε και θεωρούμε ότι έχουμε μία αρνητική ταυτοποίηση. Μία εναλλακτική προσέγγιση που θα μπορούσε να υλοποιηθεί αυξάνοντας δραματικά την απόδοση του συστήματός μας αλλά και ακόμη μεγαλύτερη μείωση του χρόνου πιστοποίησης ενός χρήστη θα ήταν η των προτέρων εξέταση των προσώπων και η αποθήκευση των μαθηματικών διανυσμάτων των υπολογισμών στη βάση μας. Σε δεύτερο χρόνο, στην περίπτωση ενός νέου προσώπου εισόδου το εργαλείο θα μπορούσε να υπολογίσει τα διανύσματα αυτού και να τα συγκρίνει απευθείας με μαθηματική μορφή με όσα δεδομένα είναι αποθηκευμένα στη βάση μας. Σε αυτή την περίπτωση οι χρόνοι λειτουργίας θα ήταν σαφέστατα πολύ μειωμένοι.

- Τέλος μια σημαντική επέκταση που θα μπορούσε να υλοποιηθεί είναι η ενσωμάτωση όλων εκείνων των διαδικασιών που θα μπορούσαν να συμμορφώσουν το εργαλείο μας με τις δυνατότητες επεξεργασίας των προσωπικών δεδομένων των χρηστών από τους ίδιους. Η υλοποίηση δηλαδή ενός περιβάλλοντος μέσω του οποίου οι χρήστες θα μπορούν να διαχειρίζονται τις προσωπικές πληροφορίες τους που χρησιμοποιεί και διαχειρίζεται ή επεξεργάζεται το εργαλείο μας.

Βιβλιογραφία

[01] Asha, S. a. (2008). Authentication of e-learners using multimodal biometric technology." Biometrics and Security Technologies. ISBAST 2008. International Symposium on. IEEE.

[02] Castiglione, Aniello. (n.d.). Biometrics in the cloud: Challenges and research opportunities. IEEE Cloud Computing. 2017.

[03] CLAROLINE. (2003). Ανάκτηση από Claroline Open Source Management System, University of Louvain: http://www.claroline.net/

[04] COSE. (2003). Ανάκτηση από Creation of Study Environments, Staffordshire University: http://www.staffs.ac.uk/COSE/

[05] Development and Implementation of a Biometric Verification System for E-learning Platforms. (2004.). Στο E. González-Agulla, EduTech Computer-Aided Design Meets Computer-Aided Learning (σσ. 155-164). Boston, MA: Springer.

[06] Kang, B. H. (2015). Proposal: a design of e-learning user authentication system. International Journal of Security and Its Applications 9.1, 45-50.

[07] Ken Kennedy. (1997).

[08] Moodle. (2019, 13 2). Ανάκτηση από Moodle: https://moodle.org/

[09] Sayed, Mohamed, and Farid Jradi. (2014). Biometrics: effectiveness and applications within the blended learning environment. Computer Engineering and Intelligent Systems.

[10] Security and Privacy in m-learning and beyond: Challenges and state of the art. (2013). International Journal of u-and e-Service, Science and Technology .

[11] Wayman, J. (2005). Biometric Systems. Στο An introduction to biometric authentication systems. (σσ. 1-20). London: Springer.

[12] Wikipedia. (2018, 3 21). Ανάκτηση από Wikipedia: https://el.wikipedia.org/wiki/%CE%A0%CE%BB%CE%B7%CF%81%CE%BF%CF%86%CE%BF%CF%81%CE%B9%CE%B1%CE%BA%CE%AC_%CF%83%CF%85%CF%83%CF%84%CE%AE%CE%BC%CE%B1%CF%84%CE%B1

[13] Wikipedia. (2019, 2 14). Ανάκτηση από Moodle: https://el.wikipedia.org/wiki/Moodle

[14] Γώγουλος, Γ., Λιακοπούλου, Ε., Μπαριτάκη, Μ., Νταλούκας, Ν. & Χαρπαντίδου, Ζ. (2001). Επιμόρφωση εκπαιδευτικών για την αξιοποίηση του Moodle μέσω ασύγχρονης τηλεκπαίδευσης. Πρακτικά 6ου Πανελλήνιου Συνεδρίου των Εκπαιδευτικών για τις ΤΠΕ.

[15] Medion7. (2019, 2 13). Ανάκτηση από Medion7: http://www.medion7.com/el/product/e-learning-platform_el

[16] Σύνταγμα της Ελλάδας. (2008). (σσ. Άρθρο 5Α, παράγραφος 2). Βουλή των Ελλήνων.

[17] Τεχνολογίες και Πρότυπα για την Υποστήριξη Εκπαιδευτικών Περιβαλλόντων Διαδικτύου. (2019, 2 13). Ανάκτηση από kallipos.gr: https://repository.kallipos.gr/bitstream/11419/3204/1/02_chapter_4.pdf

[18] Τζιμόπουλος, Τσεπαπαδάκης, Κόκκαλης, & Πουχτού . (2009). Αξιοποίηση των Τεχνολογιών της Πληροφορίας και της Επικοινωνίας στη Διδακτική Πράξη. 5Ο ΠΑΝΕΛΛΗΝΙΟ ΣΥΝΕΔΡΙΟ ΤΩΝ ΕΚΠΑΙΔΕΥΤΙΚΩΝ ΓΙΑ ΤΙΣ ΤΠΕ. Πνευματικό Κέντρο Δήμου Ερμούπολης.

[19] Moodle in Greece - Yiannis Arapoglou, Stamos Sp (previously Aggelos Panagiotakis)

[20] I. El Khalkhali, "The use of DOKEOS e-learning platform in a Moroccan Business School," 2014 International Conference on Multimedia Computing and Systems (ICMCS), Marrakech, 2014, pp. 633-638.

[21] doi: 10.1109/ICMCS.2014.6911146

[22] Karadimas, Nikolaos & Karamanoli, Vassia. (2017). Asynchronous e-Learning Platform used for Psychological Research in a Military Environment. Journal of Computations & Modelling. 7. 57-83.

[23] Sakai 11, Educational Community License, Version 2.0, April 2007 https://github.com/sakaiproject/sakai

[24] Wikipedia contributors. (2019, April 26). Client–server model. In Wikipedia, The Free Encyclopedia. Retrieved 13:13, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Client%E2%80%93server_model&oldid=894200374

[25] Wikipedia contributors. (2019, April 22). Learning management system. In Wikipedia, The Free Encyclopedia. Retrieved 13:14, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Learning_management_system&oldid=893628764

[26] Wikipedia contributors. (2019, April 5). Virtual learning environment. In Wikipedia, The Free Encyclopedia. Retrieved 13:14, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Virtual_learning_environment&oldid=891099857

[27] Wikipedia contributors. (2019, April 12). Moodle. In Wikipedia, The Free Encyclopedia. Retrieved 13:15, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Moodle&oldid=892136711

[28] Wikipedia contributors. (2019, April 8). Software as a service. In Wikipedia, The Free Encyclopedia. Retrieved 13:15, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Software_as_a_service&oldid=891562243

[29] Τσιάτσος, Θ. 2015. Τεχνολογίες και Πρότυπα για την Υποστήριξη Εκπαιδευτικών Περιβαλλόντων Διαδικτύου. [Κεφάλαιο Συγγράμματος]. Στο Τσιάτσος, Θ. 2015. Εκπαιδευτικά περιβάλλοντα διαδικτύου. [ηλεκτρ. βιβλ.] Αθήνα:Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών. κεφ 4. Διαθέσιμο στο: http://hdl.handle.net/11419/3204

[30] Wayman, James & Jain, Anil & Maltoni, Davide & Maio, Dario. (2005). An Introduction to Biometric Authentication Systems. 10.1007/1-84628-064-8_1.

[31] Kambourakis, Georgios. (2013). Security and privacy in m-learning and beyond: Challenges and state-of-the-art. International Journal of U-and E-Service, Science and Technology. 6. 67-84.

[32] González Agulla, Elisardo & Argones Rúa, Enrique & García-Mateo, Carmen & W. Marquez-Florez, Oscar. (2004). Development and Implementation of a Biometric Verification System for E-Learning Platforms. International Federation for Information Processing Digital Library; EduTech Computer-Aided Design Meets Computer-Aided Learning;. 10.1007/1-4020-8162-6_17.

[33] De Silva, Sam and Liu, Anthony and LLP, Nabarro, 2017, Biometric Technology Today, English, pages = {5-7}, doi:10.1016/S0969-4765(17)30033-4

[34] Y. Makihara, M. A. Hossain and Y. Yagi, "How to Control Acceptance Threshold for Biometric Signatures with Different Confidence Values?," 2010 20th International Conference on Pattern Recognition, Istanbul, 2010, pp. 1208-1211., doi: 10.1109/ICPR.2010.301

[35] Wikipedia contributors. (2019, April 24). Biometrics. In Wikipedia, The Free Encyclopedia. Retrieved 13:24, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Biometrics&oldid=893867239

[36] Norman Poh, Alvin Martin, and Samy Bengio. 2007. Performance Generalization in Biometric Authentication Using Joint User-Specific and Sample Bootstraps. IEEE Trans. Pattern Anal. Mach. Intell. 29, 3 (March 2007), 492-498. DOI=http://dx.doi.org/10.1109/TPAMI.2007.55

[37] Choudhury, Bismita & Then, Patrick & Issac, Biju & Raman, Valliappan & Haldar, Manas. (2018). A Survey on Biometrics and Cancelable Biometrics Systems. International Journal of Image and Graphics. 18. 1850006. 10.1142/S0219467818500067.

[38] Wikipedia contributors. (2019, May 5). Convolutional neural network. In Wikipedia, The Free Encyclopedia. Retrieved 13:26, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=Convolutional_neural_network&oldid=895542745

[39] LeCun, Y., Bengio, Y. and Hinton, G., 2015. Deep learning. Nature, 521(7553), pp.436-444.

[40] K. Zhang, Z. Zhang, Z. Li and Y. Qiao, "Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks," in IEEE Signal Processing Letters, vol. 23, no. 10, pp. 1499-1503, Oct. 2016.

[41] M. Ordowski and G. G. L. Meyer, "Geometric linear discriminant analysis," 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No.01CH37221), Salt Lake City, UT, USA, 2001, pp. 3173-3176 vol.5.

[42] Laurenz Wiskott, Jean-Marc Fellous, Norbert Krüger, and Christopher von der Malsburg. 1997. Face Recognition by Elastic Bunch Graph Matching. IEEE Trans. Pattern Anal. Mach. Intell. 19, 7 (July 1997), 775-779. DOI=http://dx.doi.org/10.1109/34.598235

[43] L. Sirovich and M. Kirby, "A Low-Dimensional Procedure for the Characterization of Human Faces," J. Optical Soc. Am. A, 1987, Vol. 4, No.3, 519-524.

[44] Jolliffe, I. T., & Cadima, J. (2016). Principal component analysis: a review and recent developments. Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 374(2065), 20150202. doi:10.1098/rsta.2015.0202

[45] L. Rabiner and B. Juang, "An introduction to hidden Markov models," in IEEE ASSP Magazine, vol. 3, no. 1, pp. 4-16, Jan 1986.

[46] H. Umeki and H. Mizutani, "Dynamic link matching for multiple object recognition," Proceedings of 13th International Conference on Pattern Recognition, Vienna, Austria, 1996, pp. 65-69 vol.4.doi: 10.1109/ICPR.1996.547235

[47] Zhu, J., von der Malsburg, C.(2003). Object recognition by Dynamic Link Matching in biologically realistic time [Abstract]. Journal of Vision, 3(9): 195, 195a, http://journalofvision.org/3/9/195/, doi:10.1167/3.9.195.

[48] S. Jetley and D. Selven, "Applying machining vision to surface texture analysis," Proceedings of 36th Midwest Symposium on Circuits and Systems, Detroit, MI, USA, 1993, pp. 1456-1459 vol.2. doi: 10.1109/MWSCAS.1993.343385

[49] Gross, Ralph & Sweeney, Latanya & Cohn, Jeffrey & De la Torre, Fernando & Baker, Simon. (2009). Face De-identification. 10.1007/978-1-84882-301-3_8.

[50] P. Hu and D. Ramanan, "Finding Tiny Faces," 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Honolulu, HI, 2017, pp. 1522-1530. doi: 10.1109/CVPR.2017.166

[51] Redmon, & Farhadi(2016) 2016 arXiv161208242R, Redmon, J., & Farhadi, A. 2016, arXiv e-prints , arXiv:1612.08242.

[52] Wikipedia contributors. (2019, May 3). General Data Protection Regulation. In Wikipedia, The Free Encyclopedia. Retrieved 13:44, May 6, 2019, from https://en.wikipedia.org/w/index.php?title=General_Data_Protection_Regulation&oldid=895366658

[53] Privacy notices under the EU General Data Protection Regulation". ico.org.uk. 19 January 2018. Archived from the original on 23 May 2018. Retrieved 22 May 2018.

[54] Privacy and Data Protection by Design – ENISA". Europa (web portal). Archived from the original on 5 April 2017. Retrieved 4 April 2017.

[55] EUR-Lex - L:2016:119:TOC - EN - EUR-Lex

Παράρτημα

Index.php

```
<? include("header.php"); ?>
<!-- Example row of columns -->
<div class="jumbotron">
  <div class="control-group">
    <h1>Εγγραφή χρήστη (προσομοίωση πρώτης σύνδεσης)</h1>
    <h2>1. Δώστε το email σας</h2>
    <div class="controls">
      <form action=register.php method=post id=submit>
        <input type=hidden id=x name=x>
        <input type=hidden id=y name=y>
        <input type=hidden id=w name=w>
        <input type=hidden id=h name=h>
        <input type=hidden id=dataimg name=dataimg>
        <input type="text" class="input-xlarge" id="email" name=email
placeholder="Email address">
      </form>
    </div>
  </div>
  <h2>2. Τοποθετήστε το πρόσωπό σας</h2>
  <p id="info">Παρακαλούμε επιτρέψτε την κάμερα να καταγράφει<br>Δείτε την
ειδοποίηση στο πάνω μέρος του παραθύρου<br><img src=allow.png></p>
  <canvas id="output"></canvas>
  <p>Σιγουρευτείτε ότι το πρόσωπό σας είναι εντός του μπλε
τετραγώνου<br>Σιγουρευτείτε ότι το πρόσωπό σας αναγνωρίζεται ορθά.</p>
  <script src="ccv.js"></script>
  <script src="face.js"></script>
  <p><a class="btn btn-lg btn-success" href="#" role="button"
onClick="capture()">Ολοκλήρωση εγγραφής</a></p>
  <script>
    // requestAnimationFrame shim
    (function() {
      var i = 0,
        lastTime = 0,
        vendors = ['ms', 'moz', 'webkit', 'o'];

      while (i < vendors.length && !window.requestAnimationFrame) {
        window.requestAnimationFrame = window[vendors[i] +
'RequestAnimationFrame'];
        i++;
      }

      if (!window.requestAnimationFrame) {
        window.requestAnimationFrame = function(callback, element) {
          var currTime = new Date().getTime(),
            timeToCall = Math.max(0, 1000 / 60 - currTime + lastTime),
            id = setTimeout(function() {
              callback(currTime + timeToCall);
            }, timeToCall);
```

```
        lastTime = currTime + timeToCall;
        return id;
      };
    }
  }());

  var App = {
    start: function(stream) {
      App.video.addEventListener('canplay', function() {
        setTimeout(function() {
          App.video.play();
          App.canvas.style.display = 'inline';
          App.info.style.display = 'none';
          App.canvas.width = App.video.videoWidth;
          App.canvas.height = App.video.videoHeight;
          App.backCanvas.width = App.video.videoWidth / 4;
          App.backCanvas.height = App.video.videoHeight / 4;
          App.backContext = App.backCanvas.getContext('2d');

          var w = 300 / 4 * 0.8,
            h = 270 / 4 * 0.8;

          App.comp = [{
            x: (App.video.videoWidth / 4 - w) / 2,
            y: (App.video.videoHeight / 4 - h) / 2,
            width: w,
            height: h,
          }];

          App.drawToCanvas();
        }, 500);
      }, true);

      var domURL = window.URL.createObjectURL;
      App.video.srcObject = stream;
    },
    denied: function() {
      App.info.innerHTML = 'Camera access denied!<br>Please reload and
try again.';
    },
    error: function(e) {
      if (e) {
        console.error(e);
      }
      App.info.innerHTML = 'Please go to about:flags in Google Chrome and
enable the &amp;quot;MediaStream&amp;quot; flag.';
    },
    drawToCanvas: function() {
      requestAnimationFrame(App.drawToCanvas);

      var video = App.video,
        ctx = App.context,
        backCtx = App.backContext,
        m = 4,
        w = 4,
        i,
        comp;
```

```
        ctx.drawImage(video, 0, 0, App.canvas.width, App.canvas.height);

        backCtx.drawImage(video, 0, 0, App.backCanvas.width,
App.backCanvas.height);
        comp = ccv.detect_objects(App.ccv = App.ccv || {
          canvas: App.backCanvas,
          cascade: cascade,
          interval: 4,
          min_neighbors: 1
        });

        if (comp.length) {
          App.comp = comp;
        }
        for (i = App.comp.length; i--;) {
          ctx.drawImage(App.glasses, (App.comp[i].x - w / 2) * m,
(App.comp[i].y - w / 2) * m, (App.comp[i].width + w) * m,
(App.comp[i].height + w) * m);

          document.getElementById('x').value = (App.comp[i].x - w / 2) * m;
          document.getElementById('y').value = (App.comp[i].y - w / 2) * m;
          document.getElementById('w').value = (App.comp[i].width + w) * m;
          document.getElementById('h').value = (App.comp[i].height + w) *
m;


        }
      }
    };

    App.glasses = new Image();
    App.glasses.src = 'glasses.png';

    App.init = function() {
      App.video = document.createElement('video');
      App.backCanvas = document.createElement('canvas');
      App.canvas = document.querySelector('#output');
      App.canvas.style.display = 'none';
      App.context = App.canvas.getContext('2d');
      App.info = document.querySelector('#info');

      navigator.getUserMedia_ = navigator.getUserMedia ||
navigator.webkitGetUserMedia || navigator.mozGetUserMedia ||
navigator.msGetUserMedia;

      try {
        navigator.getUserMedia_({
          video: true,
          audio: false
        }, App.start, App.denied);
      } catch (e) {
        try {
          navigator.getUserMedia_('video', App.start, App.denied);
        } catch (e) {
          App.error(e);
        }
      }

      App.video.loop = App.video.muted = true;
```

```
      App.video.load();
    };

    App.init();

    function capture() {
      var email = document.getElementById("email").value;
      if (validateEmail(email)) {
        var canvas = document.getElementById("output");
        var img = canvas.toDataURL();

//location.href='register.php?image='+img+'&x='+document.getElementById("y"
).value+'&y='+document.getElementById("y").value+'&w='+document.getElementB
yId("w").value+'&h='+document.getElementById("h").value;

        document.getElementById("dataimg").value = img;

        document.getElementById("submit").submit();
        return false;

      } else {

        alert("wrong email");
      }


    }


    function validateEmail(email) {
      var re =
/^(([^<>()[\]\\.,;:\s@\"]+(\.[^<>()[\]\\.,;:\s@\"]+)*)|(\".+\"))@((\[[0-
9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\])|(([a-zA-Z\-0-9]+\.)+[a-zA-
Z]{2,}))$/;
      return re.test(email);
    }
  </script>

  </p>
</div>
<!-- Jumbotron -->
<div class="jumbotron">
</div>
<!-- Site footer -->
<div class="footer">
</div>
</div> <!-- /container -->

<!-- Bootstrap core JavaScript
  ================================================== -->
<!-- Placed at the end of the document so the pages load faster -->


</body>

</html>
```

Login.php

```
print 'hello world!'<? include("header.php"); ?>
    <!-- Example row of columns -->
   <div class="jumbotron">

<div class="control-group">
<h1>Εγγραφή χρήστη (προσομοίωση πρώτης σύνδεσης)</h1>
<h2>1. Δώστε το email σας</h2>
<div class="controls"><form action=register.php method=post id=submit >
<input type=hidden id=x name=x>
<input type=hidden id=y name=y>
<input type=hidden id=w name=w>
<input type=hidden id=h name=h>
<input type=hidden id=dataimg name=dataimg>
<input type="text" class="input-xlarge" id="email" name=email
placeholder="Email address" >
</form>
</div>
</div>
<h2>2. Τοποθετήστε το πρόσωπό σας</h2><p id="info">Παρακαλούμε επιτρέψτε
την κάμερα να καταγράφει<br>Δείτε την ειδοποίηση στο πάνω μέρος του
παραθύρου<br><img src=allow.png></p>


    <canvas id="output"></canvas>
    <p>Σιγουρευτείτε ότι το πρόσωπό σας είναι εντός του μπλε
τετραγώνου<br>Σιγουρευτείτε ότι το πρόσωπό σας αναγνωρίζεται ορθά.</p>
    <script src="ccv.js"></script>
    <script src="face.js"></script>
     <p><a class="btn btn-lg btn-success" href="#" role="button"
onClick="capture()">Ολοκλήρωση εγγραφής</a></p>
    <script>// requestAnimationFrame shim
(function() {
  var i = 0,
    lastTime = 0,
    vendors = ['ms', 'moz', 'webkit', 'o'];  while (i < vendors.length &&
!window.requestAnimationFrame) {
    window.requestAnimationFrame = window[vendors[i] +
'RequestAnimationFrame'];
    i++;
  }  if (!window.requestAnimationFrame) {
    window.requestAnimationFrame = function(callback, element) {
      var currTime = new Date().getTime(),
        timeToCall = Math.max(0, 1000 / 60 - currTime + lastTime),
        id = setTimeout(function() { callback(currTime + timeToCall); },
timeToCall);

      lastTime = currTime + timeToCall;
      return id;
    };
  }
}());var App = {
```

```
  start: function(stream) {
    App.video.addEventListener('canplay', function() {
      setTimeout(function() {
        App.video.play();
        App.canvas.style.display = 'inline';
        App.info.style.display = 'none';
        App.canvas.width = App.video.videoWidth;
        App.canvas.height = App.video.videoHeight;
        App.backCanvas.width = App.video.videoWidth / 4;
        App.backCanvas.height = App.video.videoHeight / 4;
        App.backContext = App.backCanvas.getContext('2d');

        var w = 300 / 4 * 0.8,
          h = 270 / 4 * 0.8;

        App.comp = [{
          x: (App.video.videoWidth / 4 - w) / 2,
          y: (App.video.videoHeight / 4 - h) / 2,
          width: w,
          height: h,
        }];

        App.drawToCanvas();
      }, 500);
    }, true);

    var domURL = window.URL.createObjectURL;
    App.video.srcObject = stream;
  },
  denied: function() {
    App.info.innerHTML = 'Camera access denied!<br>Please reload and try
again.';
  },
  error: function(e) {
    if (e) {
      console.error(e);
    }
    App.info.innerHTML = 'Please go to about:flags in Google Chrome and
enable the &quot;MediaStream&quot; flag.';
  },
  drawToCanvas: function() {
    requestAnimationFrame(App.drawToCanvas);

    var video = App.video,
      ctx = App.context,
      backCtx = App.backContext,
      m = 4,
      w = 4,
      i,
      comp;

    ctx.drawImage(video, 0, 0, App.canvas.width, App.canvas.height);

    backCtx.drawImage(video, 0, 0, App.backCanvas.width,
App.backCanvas.height);

    comp = ccv.detect_objects(App.ccv = App.ccv || {
      canvas: App.backCanvas,
      cascade: cascade,
```

```
      interval: 4,
      min_neighbors: 1
    });

    if (comp.length) {
      App.comp = comp;
    }



    for (i = App.comp.length; i--; ) {
      ctx.drawImage(App.glasses, (App.comp[i].x - w / 2) * m,
(App.comp[i].y - w / 2) * m, (App.comp[i].width + w) * m,
(App.comp[i].height + w) * m);

      document.getElementById('x').value=(App.comp[i].x - w / 2) * m;
      document.getElementById('y').value=(App.comp[i].y - w / 2) * m;
      document.getElementById('w').value=(App.comp[i].width + w) * m;
      document.getElementById('h').value=(App.comp[i].height + w) * m;


    }
  }
};App.glasses = new Image();
App.glasses.src = 'glasses.png';App.init = function() {
  App.video = document.createElement('video');
  App.backCanvas = document.createElement('canvas');
  App.canvas = document.querySelector('#output');
  App.canvas.style.display = 'none';
  App.context = App.canvas.getContext('2d');
  App.info = document.querySelector('#info');  navigator.getUserMedia_ =
navigator.getUserMedia || navigator.webkitGetUserMedia ||
navigator.mozGetUserMedia || navigator.msGetUserMedia;  try {
    navigator.getUserMedia_({
      video: true,
      audio: false
    }, App.start, App.denied);
  } catch (e) {
    try {
      navigator.getUserMedia_('video', App.start, App.denied);
    } catch (e) {
      App.error(e);
    }
  }  App.video.loop = App.video.muted = true;
  App.video.load();
};App.init();  function capture() {
    var email = document.getElementById("email").value;
    if (validateEmail(email) ) {
     var canvas = document.getElementById("output");
    var img  = canvas.toDataURL();
//location.href='register.php?image='+img+'&x='+document.getElementById("y"
).value+'&y='+document.getElementById("y").value+'&w='+document.getElementB
yId("w").value+'&h='+document.getElementById("h").value;document.getElement
ById("dataimg").value=img;document.getElementById("submit").submit();
return false;} else {alert("wrong email");
}
    }
```

```
    function validateEmail(email) {
  var re =
/^(([^<>()[\]\\.,;:\s@\"]+(\.[^<>()[\]\\.,;:\s@\"]+)*)|(\".+\"))@((\[[0-
9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\])|(([a-zA-Z\-0-9]+\.)+[a-zA-
Z]{2,}))$/;
  return re.test(email);
}
    </script>   </p>

    </div>
   <!-- Jumbotron -->
 <div class="jumbotron">
   </div>
   <!-- Site footer -->
   <div class="footer">   </div>  </div> <!-- /container -->
  <!-- Bootstrap core JavaScript
  ================================================== -->
  <!-- Placed at the end of the document so the pages load faster -->
 </body></html>
```

Register.php

```
<?php

include("header.php");

if (file_exists("faces/".md5($_POST["email"])) ) {

echo "This email has been already registered. You can try to <a
href=login.php>login</a> with your email address and your face!";
} else {
$_POST["dataimg"]=str_replace("","",$_POST["dataimg"]
);

$_POST["dataimg"]= base64_decode($_POST["dataimg"]);

$email=filter_var($_POST["email"],FILTER_VALIDATE_EMAIL);
file_put_contents($facestorage."faces/".md5($email),$_POST["dataimg"]);


$dst_x = 0;  // X-coordinate of destination point.
$dst_y = 0;  // Y --coordinate of destination point.
$array1["x"] = $_POST[x]; // Crop Start X position in original image
$array1["y"]= $_POST[y]; // Crop Srart Y position in original image
$array1["width"]= $_POST[w]; // Thumb width
$array1["height"] = $_POST[h]; // Thumb height
$src_w = $src_x + $dst_w; // $src_x + $dst_w Crop end X position in
original image
$src_h = src_y + $dst_h; // $src_y + $dst_h Crop end Y position in original
image


// Create image instances
$src = imagecreatefrompng($facestorage."faces/".md5($email));
```

```
$dest = imagecreatetruecolor(intval($array1["width"])-10,
intval($array1["height"])-10 ) or die('Cannot Initialize new GD image
stream');

// Copy
imagecopy($dest, $src, 0, 0,$array1["x"]+5, $array1["y"]+5,
$array1["width"], $array1["height"]);

imagepng($dest, $facestorage."faces/cropped-".md5($email).".png");
//imagegd($dest);

echo "<br>Your face has been added. Now try to <a href=login.php>login</a>
with your email address and your face!";
}
?>
```

TμFace.js

```
var
cascade={count:16,width:24,height:24,stage_classifier:[{count:4,threshold:-
4.57753,feature:[{size:4,px:[3,5,8,11],py:[2,2,6,3],pz:[2,1,1,0],nx:[8,4,0,
0],ny:[4,4,0,0],nz:[1,1,-1,-1]},{size:3,px:[3,6,7],py:[7,13,0],pz:[1,0,-
1],nx:[2,3,4],ny:[5,4,4],nz:[2,1,1]},{size:5,px:[5,3,10,13,11],py:[1,0,3,2,
2],pz:[1,2,0,0,0],nx:[0,11,0,11,11],ny:[0,2,3,1,1],nz:[1,1,0,1,-
1]},{size:5,px:[6,12,12,9,12],py:[4,13,12,7,11],pz:[1,0,0,1,0],nx:[8,0,8,2,
11],ny:[4,0,8,5,1],nz:[1,-1,-1,-1,-1]}],alpha:[-2.879683,2.879683,
-1.569341,1.569341,-1.286131,1.286131,-
1.157626,1.157626]},{count:4,threshold:-
4.339908,feature:[{size:5,px:[13,12,3,11,17],py:[3,3,1,4,13],pz:[0,0,2,0,0]
,nx:[4,3,8,15,15],ny:[4,5,4,8,8],nz:[1,2,1,0,-
1]},{size:5,px:[6,7,6,3,3],py:[13,13,4,2,7],pz:[0,0,1,2,1],nx:[4,8,3,0,15],
ny:[4,4,4,3,8],nz:[1,1,-1,-1,-
1]},{size:3,px:[2,2,11],py:[3,2,5],pz:[2,2,0],nx:[3,8,3],ny:[4,4,4],nz:[1,-
1,-
1]},{size:5,px:[15,13,9,11,7],py:[2,1,2,1,0],pz:[0,0,0,0,1],nx:[23,11,23,22
,23],ny:[1,0,2,0,0],nz:[0,1,0,0,0]}],alpha:[-2.466029,
2.466029,-1.83951,1.83951,-1.060559,1.060559,-
1.094927,1.094927]},{count:7,threshold:-
5.052474,feature:[{size:5,px:[17,13,3,11,10],py:[13,2,1,4,3],pz:[0,0,2,0,0]
,nx:[4,8,8,3,7],ny:[2,8,4,5,4],nz:[2,0,1,2,1]},{size:5,px:[6,7,3,6,6],py:[4
,12,2,13,14],pz:[1,0,2,0,0],nx:[8,3,4,4,3],ny:[4,4,2,0,2],nz:[1,1,-1,-1,-
1]},{size:5,px:[7,4,5,3,3],py:[2,1,3,1,1],pz:[0,1,0,1,-
1],nx:[1,0,1,1,0],ny:[1,3,2,0,4],nz:[0,0,0,0,0]},{size:5,px:[11,11,11,3,2],
py:[11,13,10,7,2],pz:[0,0,0,1,2],nx:[4,1,8,2,0],ny:[4,1,12,0,4],
nz:[1,-1,-1,-1,-1]},{size:3,px:[9,13,1],py:[7,19,4],pz:[1,-1,-
1],nx:[4,7,4],ny:[5,8,2],nz:[2,1,2]},{size:5,px:[12,8,16,4,4],py:[12,1,2,0,
0],pz:[0,1,0,2,-
1],nx:[11,22,11,23,23],ny:[2,0,1,1,5],nz:[1,0,1,0,0]},{size:3,px:[11,17,17]
,py:[6,11,12],pz:[0,0,0],nx:[15,1,11],ny:[9,1,1],nz:[0,-1,-1]}],alpha:[-
2.15689,2.15689,-1.718246,1.718246,-0.9651329,0.9651329,-
0.994809,0.994809,-0.8802466,0.8802466,-0.8486741,0.8486741,-
```

```
0.8141777,0.8141777]},{count:13,threshold:-
5.7744,feature:[{size:5,px:[6,10,3,12,14],
py:[5,3,1,2,2],pz:[1,0,2,0,0],nx:[3,4,14,8,4],ny:[5,4,8,4,2],nz:[2,1,0,1,2]
},{size:5,px:[10,6,11,5,12],py:[4,13,4,2,4],pz:[0,0,0,1,0],nx:[1,4,8,1,1],n
y:[2,4,4,4,3],nz:[0,1,1,0,0]},{size:3,px:[18,6,12],py:[12,4,8],pz:[0,1,0],n
x:[7,4,8],ny:[4,2,4],nz:[1,-1,-
1]},{size:5,px:[7,5,6,3,17],py:[13,12,3,8,13],pz:[0,0,1,1,0],nx:[3,3,0,1,8]
,ny:[4,5,5,10,4],nz:[1,-1,-1,-1,-
1]},{size:5,px:[16,7,16,7,7],py:[1,1,2,0,0],pz:[0,1,0,1,-
1],nx:[23,23,23,11,5],ny:[2,14,1,2,1],nz:[0,0,0,1,2]},{size:3,px:[9,18,16],
py:[7,
14,2],pz:[1,0,-
1],nx:[8,4,9],ny:[10,2,4],nz:[1,2,1]},{size:4,px:[3,16,1,22],py:[7,4,5,11],
pz:[1,-1,-1,-
1],nx:[3,9,4,2],ny:[4,9,7,5],nz:[1,0,1,2]},{size:5,px:[4,7,8,8,9],py:[0,2,2
,1,1],pz:[1,0,0,0,0],nx:[0,0,1,0,0],ny:[15,16,19,0,14],nz:[0,0,0,1,0]},{siz
e:5,px:[4,4,7,8,12],py:[2,5,6,7,10],pz:[2,2,1,1,0],nx:[8,5,10,0,0],ny:[4,2,
5,3,14],nz:[1,-1,-1,-1,-1]},{size:2,px:[11,0],py:[13,4],pz:[0,-
1],nx:[3,14],ny:[4,16],nz:[1,0]},{size:5,px:[17,8,18,4,4],py:[3,1,3,0,0],pz
:[0,1,0,2,-1],nx:[21,22,5,11,22],ny:[0,
1,0,1,2],nz:[0,0,2,1,0]},{size:4,px:[7,8,2,11],py:[13,12,2,7],pz:[0,0,2,0],
nx:[4,0,23,3],ny:[4,1,1,11],nz:[1,-1,-1,-
1]},{size:5,px:[4,18,8,9,15],py:[4,16,7,7,23],pz:[2,0,1,1,0],nx:[0,1,1,1,1]
,ny:[10,21,23,22,22],nz:[1,0,0,0,-1]}],alpha:[-1.956565,1.956565,-
1.262438,1.262438,-1.056941,1.056941,-0.9712509,0.9712509,-
0.8261028,0.8261028,-0.8456506,0.8456506,-0.6652113,0.6652113,-
0.6026287,0.6026287,-0.6915425,0.6915425,-0.5539286,0.5539286,-
0.5515072,0.5515072,-0.6685884,0.6685884,-0.465607,0.465607]},
```


CCV.js

```
if (parallable === undefined) {
  var parallable = function (file, funct) {
    parallable.core[funct.toString()] = funct().core;
    return function () {
      var i;
      var async, worker_num, params;
      if (arguments.length > 1) {
        async = arguments[arguments.length - 2];
        worker_num = arguments[arguments.length - 1];
        params = new Array(arguments.length - 2);
        for (i = 0; i < arguments.length - 2; i++)
          params[i] = arguments[i];
      } else {
        async = arguments[0].async;
        worker_num = arguments[0].worker;
        params = arguments[0];
        delete params["async"];
        delete params["worker"];
        params = [params];
      }
      var scope = {
        "shared": {}
      };
      var ctrl = funct.apply(scope, params);
      if (async) {
```

```
        return function (complete, error) {
          var executed = 0;
          var outputs = new Array(worker_num);
          var inputs = ctrl.pre.apply(scope, [worker_num]);
          /* sanitize scope shared because for Chrome/WebKit, worker only
support JSONable data */
          for (i in scope.shared)
            /* delete function, if any */
            if (typeof scope.shared[i] == "function")
              delete scope.shared[i];
            /* delete DOM object, if any */
            else if (scope.shared[i].tagName !== undefined)
            delete scope.shared[i];
          for (i = 0; i < worker_num; i++) {
            var worker = new Worker(file);
            worker.onmessage = (function (i) {
              return function (event) {
                outputs[i] = (typeof event.data == "string") ?
JSON.parse(event.data) : event.data;
                executed++;
                if (executed == worker_num)
                  complete(ctrl.post.apply(scope, [outputs]));
              }
            })(i);
            var msg = {
              "input": inputs[i],
              "name": funct.toString(),
              "shared": scope.shared,
              "id": i,
              "worker": params.worker_num
            };
            try {
              worker.postMessage(msg);
            } catch (e) {
              worker.postMessage(JSON.stringify(msg));
            }
          }
        }
      } else {
        return ctrl.post.apply(scope, [[ctrl.core.apply(scope,
[ctrl.pre.apply(scope, [1])[0], 0, 1])]]);
      }
    }
  };
  parallable.core = {};
}

function get_named_arguments(params, names) {
  if (params.length > 1) {
    var new_params = {};
    for (var i = 0; i < names.length; i++)
      new_params[names[i]] = params[i];
    return new_params;
  } else if (params.length == 1) {
    return params[0];
  } else {
    return {};
  }
}
```

```
var ccv = {
  pre: function (image) {
    if (image.tagName.toLowerCase() == "img") {
      var canvas = document.createElement("canvas");
      document.body.appendChild(image);
      canvas.width = image.offsetWidth;
      canvas.style.width = image.offsetWidth.toString() + "px";
      canvas.height = image.offsetHeight;
      canvas.style.height = image.offsetHeight.toString() + "px";
      document.body.removeChild(image);
      var ctx = canvas.getContext("2d");
      ctx.drawImage(image, 0, 0);
      return canvas;
    }
    return image;
  },

  grayscale: function (canvas) {
    var ctx = canvas.getContext("2d");
    var imageData = ctx.getImageData(0, 0, canvas.width, canvas.height);
    var data = imageData.data;
    var pix1, pix2, pix = canvas.width * canvas.height * 4;
    while (pix > 0)
      data[pix -= 4] = data[pix1 = pix + 1] = data[pix2 = pix + 2] =
(data[pix] * 0.3 + data[pix1] * 0.59 + data[pix2] * 0.11);
    ctx.putImageData(imageData, 0, 0);
    return canvas;
  },

  array_group: function (seq, gfunc) {
    var i, j;
    var node = new Array(seq.length);
    for (i = 0; i < seq.length; i++)
      node[i] = {
        "parent": -1,
        "element": seq[i],
        "rank": 0
      };
    for (i = 0; i < seq.length; i++) {
      if (!node[i].element)
        continue;
      var root = i;
      while (node[root].parent != -1)
        root = node[root].parent;
      for (j = 0; j < seq.length; j++) {
        if (i != j && node[j].element && gfunc(node[i].element,
node[j].element)) {
          var root2 = j;

          while (node[root2].parent != -1)
            root2 = node[root2].parent;

          if (root2 != root) {
            if (node[root].rank > node[root2].rank)
              node[root2].parent = root;
            else {
              node[root].parent = root2;
              if (node[root].rank == node[root2].rank)
```

```
                node[root2].rank++;
              root = root2;
            }

            /* compress path from node2 to the root: */
            var temp, node2 = j;
            while (node[node2].parent != -1) {
              temp = node2;
              node2 = node[node2].parent;
              node[temp].parent = root;
            }

            /* compress path from node to the root: */
            node2 = i;
            while (node[node2].parent != -1) {
              temp = node2;
              node2 = node[node2].parent;
              node[temp].parent = root;
            }
          }
        }
      }
    }
    var idx = new Array(seq.length);
    var class_idx = 0;
    for (i = 0; i < seq.length; i++) {
      j = -1;
      var node1 = i;
      if (node[node1].element) {
        while (node[node1].parent != -1)
          node1 = node[node1].parent;
        if (node[node1].rank >= 0)
          node[node1].rank = ~class_idx++;
        j = ~node[node1].rank;
      }
      idx[i] = j;
    }
    return {
      "index": idx,
      "cat": class_idx
    };
  },

  detect_objects: parallable("ccv.js", function (canvas, cascade, interval,
min_neighbors) {
    if (this.shared !== undefined) {
      var params = get_named_arguments(arguments, ["canvas", "cascade",
"interval", "min_neighbors"]);
      this.shared.canvas = params.canvas;
      this.shared.interval = params.interval;
      this.shared.min_neighbors = params.min_neighbors;
      this.shared.cascade = params.cascade;
      this.shared.scale = Math.pow(2, 1 / (params.interval + 1));
      this.shared.next = params.interval + 1;
      this.shared.scale_upto =
Math.floor(Math.log(Math.min(params.canvas.width / params.cascade.width,
params.canvas.height / params.cascade.height)) /
Math.log(this.shared.scale));
      var i;
```

```
      for (i = 0; i < this.shared.cascade.stage_classifier.length; i++)
        this.shared.cascade.stage_classifier[i].orig_feature =
this.shared.cascade.stage_classifier[i].feature;
    }

    function pre(worker_num) {
      var canvas = this.shared.canvas;
      var interval = this.shared.interval;
      var scale = this.shared.scale;
      var next = this.shared.next;
      var scale_upto = this.shared.scale_upto;
      var pyr = new Array((scale_upto + next * 2) * 4);
      var ret = new Array((scale_upto + next * 2) * 4);
      pyr[0] = canvas;
      ret[0] = {
        "width": pyr[0].width,
        "height": pyr[0].height,
        "data": pyr[0].getContext("2d").getImageData(0, 0, pyr[0].width,
pyr[0].height).data
      };
      var i;
      for (i = 1; i <= interval; i++) {
        pyr[i * 4] = document.createElement("canvas");
        pyr[i * 4].width = Math.floor(pyr[0].width / Math.pow(scale, i));
        pyr[i * 4].height = Math.floor(pyr[0].height / Math.pow(scale, i));
        pyr[i * 4].getContext("2d").drawImage(pyr[0], 0, 0, pyr[0].width,
pyr[0].height, 0, 0, pyr[i * 4].width, pyr[i * 4].height);
        ret[i * 4] = {
          "width": pyr[i * 4].width,
          "height": pyr[i * 4].height,
          "data": pyr[i * 4].getContext("2d").getImageData(0, 0, pyr[i *
4].width, pyr[i * 4].height).data
        };
      }
      for (i = next; i < scale_upto + next * 2; i++) {
        pyr[i * 4] = document.createElement("canvas");
        pyr[i * 4].width = Math.floor(pyr[i * 4 - next * 4].width / 2);
        pyr[i * 4].height = Math.floor(pyr[i * 4 - next * 4].height / 2);
        pyr[i * 4].getContext("2d").drawImage(pyr[i * 4 - next * 4], 0, 0,
pyr[i * 4 - next * 4].width, pyr[i * 4 - next * 4].height, 0, 0, pyr[i *
4].width, pyr[i * 4].height);
        ret[i * 4] = {
          "width": pyr[i * 4].width,
          "height": pyr[i * 4].height,
          "data": pyr[i * 4].getContext("2d").getImageData(0, 0, pyr[i *
4].width, pyr[i * 4].height).data
        };
      }
      for (i = next * 2; i < scale_upto + next * 2; i++) {
        pyr[i * 4 + 1] = document.createElement("canvas");
        pyr[i * 4 + 1].width = Math.floor(pyr[i * 4 - next * 4].width / 2);
        pyr[i * 4 + 1].height = Math.floor(pyr[i * 4 - next * 4].height /
2);
        pyr[i * 4 + 1].getContext("2d").drawImage(pyr[i * 4 - next * 4], 1,
0, pyr[i * 4 - next * 4].width - 1, pyr[i * 4 - next * 4].height, 0, 0,
pyr[i * 4 + 1].width - 2, pyr[i * 4 + 1].height);
        ret[i * 4 + 1] = {
          "width": pyr[i * 4 + 1].width,
          "height": pyr[i * 4 + 1].height,
```

```
          "data": pyr[i * 4 + 1].getContext("2d").getImageData(0, 0, pyr[i
* 4 + 1].width, pyr[i * 4 + 1].height).data
        };
        pyr[i * 4 + 2] = document.createElement("canvas");
        pyr[i * 4 + 2].width = Math.floor(pyr[i * 4 - next * 4].width / 2);
        pyr[i * 4 + 2].height = Math.floor(pyr[i * 4 - next * 4].height /
2);
        pyr[i * 4 + 2].getContext("2d").drawImage(pyr[i * 4 - next * 4], 0,
1, pyr[i * 4 - next * 4].width, pyr[i * 4 - next * 4].height - 1, 0, 0,
pyr[i * 4 + 2].width, pyr[i * 4 + 2].height - 2);
        ret[i * 4 + 2] = {
          "width": pyr[i * 4 + 2].width,
          "height": pyr[i * 4 + 2].height,
          "data": pyr[i * 4 + 2].getContext("2d").getImageData(0, 0, pyr[i
* 4 + 2].width, pyr[i * 4 + 2].height).data
        };
        pyr[i * 4 + 3] = document.createElement("canvas");
        pyr[i * 4 + 3].width = Math.floor(pyr[i * 4 - next * 4].width / 2);
        pyr[i * 4 + 3].height = Math.floor(pyr[i * 4 - next * 4].height /
2);
        pyr[i * 4 + 3].getContext("2d").drawImage(pyr[i * 4 - next * 4], 1,
1, pyr[i * 4 - next * 4].width - 1, pyr[i * 4 - next * 4].height - 1, 0, 0,
pyr[i * 4 + 3].width - 2, pyr[i * 4 + 3].height - 2);
        ret[i * 4 + 3] = {
          "width": pyr[i * 4 + 3].width,
          "height": pyr[i * 4 + 3].height,
          "data": pyr[i * 4 + 3].getContext("2d").getImageData(0, 0, pyr[i
* 4 + 3].width, pyr[i * 4 + 3].height).data
        };
      }
      return [ret];
    };

    function core(pyr, id, worker_num) {
      var cascade = this.shared.cascade;
      var interval = this.shared.interval;
      var scale = this.shared.scale;
      var next = this.shared.next;
      var scale_upto = this.shared.scale_upto;
      var i, j, k, x, y, q;
      var scale_x = 1,
        scale_y = 1;
      var dx = [0, 1, 0, 1];
      var dy = [0, 0, 1, 1];
      var seq = [];
      for (i = 0; i < scale_upto; i++) {
        var qw = pyr[i * 4 + next * 8].width - Math.floor(cascade.width /
4);
        var qh = pyr[i * 4 + next * 8].height - Math.floor(cascade.height /
4);
        var step = [pyr[i * 4].width * 4, pyr[i * 4 + next * 4].width * 4,
pyr[i * 4 + next * 8].width * 4];
        var paddings = [pyr[i * 4].width * 16 - qw * 16,
                                                          pyr[i * 4 +
next * 4].width * 8 - qw * 8,
                                                          pyr[i * 4 +
next * 8].width * 4 - qw * 4];
        for (j = 0; j < cascade.stage_classifier.length; j++) {
          var orig_feature = cascade.stage_classifier[j].orig_feature;
```

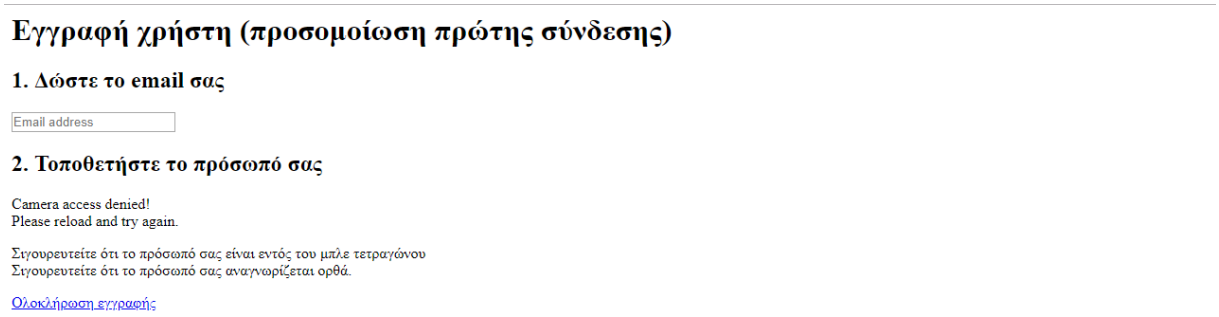
```
          var feature = cascade.stage_classifier[j].feature = new
Array(cascade.stage_classifier[j].count);
          for (k = 0; k < cascade.stage_classifier[j].count; k++) {
            feature[k] = {
              "size": orig_feature[k].size,
              "px": new Array(orig_feature[k].size),
              "pz": new Array(orig_feature[k].size),
              "nx": new Array(orig_feature[k].size),
              "nz": new Array(orig_feature[k].size)
            };
            for (q = 0; q < orig_feature[k].size; q++) {
              feature[k].px[q] = orig_feature[k].px[q] * 4 +
orig_feature[k].py[q] * step[orig_feature[k].pz[q]];
              feature[k].pz[q] = orig_feature[k].pz[q];
              feature[k].nx[q] = orig_feature[k].nx[q] * 4 +
orig_feature[k].ny[q] * step[orig_feature[k].nz[q]];
              feature[k].nz[q] = orig_feature[k].nz[q];
            }
          }
        }
        for (q = 0; q < 4; q++) {
          var u8 = [pyr[i * 4].data, pyr[i * 4 + next * 4].data, pyr[i * 4
+ next * 8 + q].data];
          var u8o = [dx[q] * 8 + dy[q] * pyr[i * 4].width * 8, dx[q] * 4 +
dy[q] * pyr[i * 4 + next * 4].width * 4, 0];
          for (y = 0; y < qh; y++) {
            for (x = 0; x < qw; x++) {
              var sum = 0;
              var flag = true;
              for (j = 0; j < cascade.stage_classifier.length; j++) {
                sum = 0;
                var alpha = cascade.stage_classifier[j].alpha;
                var feature = cascade.stage_classifier[j].feature;
                for (k = 0; k < cascade.stage_classifier[j].count; k++) {
                  var feature_k = feature[k];
                  var p, pmin = u8[feature_k.pz[0]][u8o[feature_k.pz[0]] +
feature_k.px[0]];
                  var n, nmax = u8[feature_k.nz[0]][u8o[feature_k.nz[0]] +
feature_k.nx[0]];
                  if (pmin <= nmax) {
                    sum += alpha[k * 2];
                  } else {
                    var f, shortcut = true;
                    for (f = 0; f < feature_k.size; f++) {
                      if (feature_k.pz[f] >= 0) {
                        p = u8[feature_k.pz[f]][u8o[feature_k.pz[f]] +
feature_k.px[f]];
                        if (p < pmin) {
                          if (p <= nmax) {
                            shortcut = false;
                            break;
                          }
                          pmin = p;
                        }
                      }
                      if (feature_k.nz[f] >= 0) {
                        n = u8[feature_k.nz[f]][u8o[feature_k.nz[f]] +
feature_k.nx[f]];
                        if (n > nmax) {
```

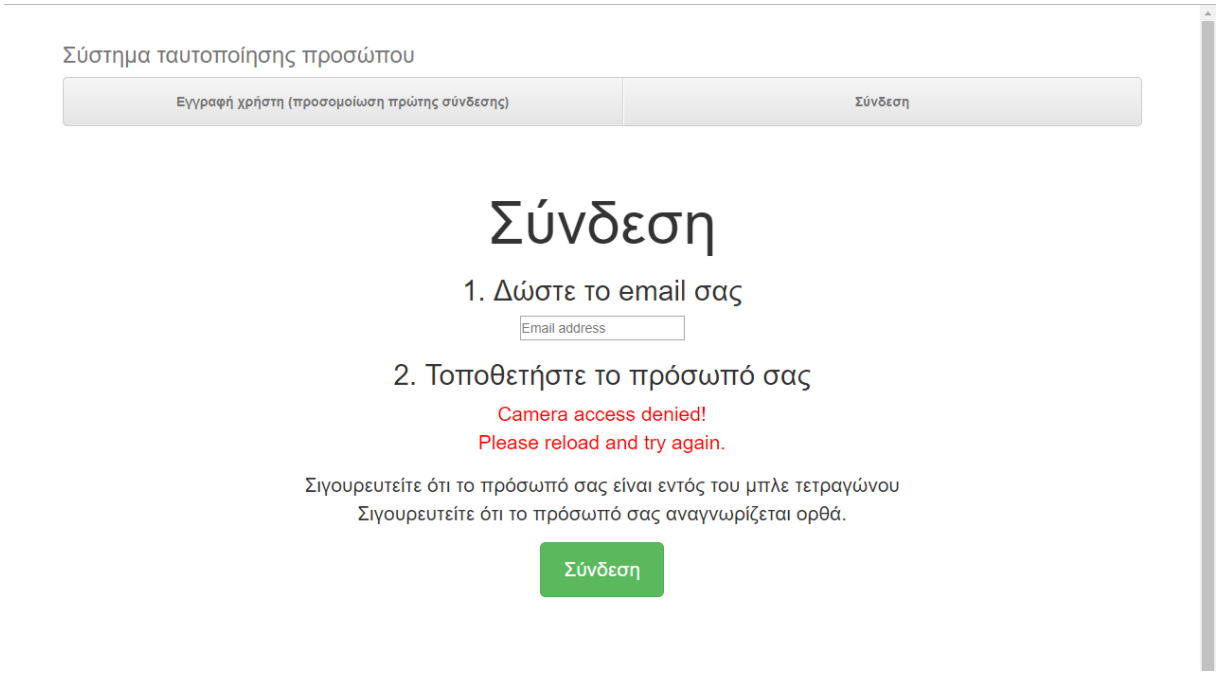
```
                        if (pmin <= n) {
                          shortcut = false;
                          break;
                        }
                        nmax = n;
                      }
                    }
                  }
                  sum += (shortcut) ? alpha[k * 2 + 1] : alpha[k * 2];
                }
              }
              if (sum < cascade.stage_classifier[j].threshold) {
                flag = false;
                break;
              }
            }
            if (flag) {
              seq.push({
                "x": (x * 4 + dx[q] * 2) * scale_x,
                "y": (y * 4 + dy[q] * 2) * scale_y,
                "width": cascade.width * scale_x,
                "height": cascade.height * scale_y,
                "neighbor": 1,
                "confidence": sum
              });
            }
            u8o[0] += 16;
            u8o[1] += 8;
            u8o[2] += 4;
          }
          u8o[0] += paddings[0];
          u8o[1] += paddings[1];
          u8o[2] += paddings[2];
        }
      }
      scale_x *= scale;
      scale_y *= scale;
    }
    return seq;
  };

  function post(seq) {
    var min_neighbors = this.shared.min_neighbors;
    var cascade = this.shared.cascade;
    var interval = this.shared.interval;
    var scale = this.shared.scale;
    var next = this.shared.next;
    var scale_upto = this.shared.scale_upto;
    var i, j;
    for (i = 0; i < cascade.stage_classifier.length; i++)
      cascade.stage_classifier[i].feature =
cascade.stage_classifier[i].orig_feature;
    seq = seq[0];
    if (!(min_neighbors > 0))
      return seq;
    else {
      var result = ccv.array_group(seq, function (r1, r2) {
        var distance = Math.floor(r1.width * 0.25 + 0.5);
```

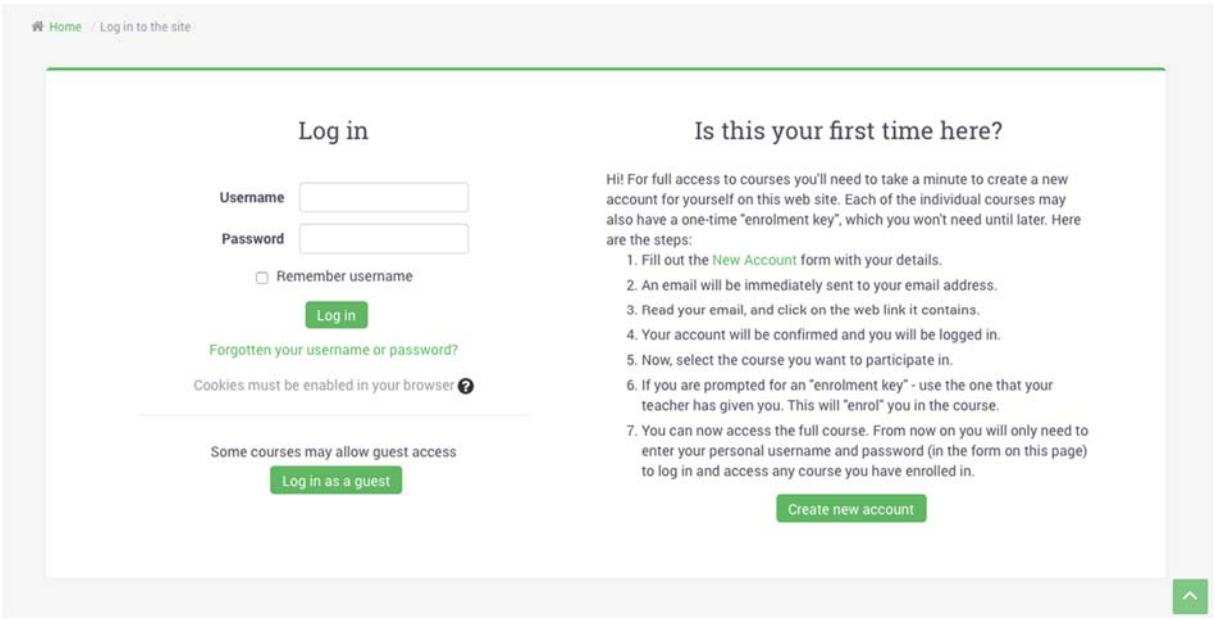
```
            return r2.x <= r1.x + distance &&
              r2.x >= r1.x - distance &&
              r2.y <= r1.y + distance &&
              r2.y >= r1.y - distance &&
              r2.width <= Math.floor(r1.width * 1.5 + 0.5) &&
              Math.floor(r2.width * 1.5 + 0.5) >= r1.width;
          });
          var ncomp = result.cat;
          var idx_seq = result.index;
          var comps = new Array(ncomp + 1);
          for (i = 0; i < comps.length; i++)
            comps[i] = {
              "neighbors": 0,
              "x": 0,
              "y": 0,
              "width": 0,
              "height": 0,
              "confidence": 0
            };

          // count number of neighbors
          for (i = 0; i < seq.length; i++) {
            var r1 = seq[i];
            var idx = idx_seq[i];

            if (comps[idx].neighbors == 0)
              comps[idx].confidence = r1.confidence;

            ++comps[idx].neighbors;

            comps[idx].x += r1.x;
            comps[idx].y += r1.y;
            comps[idx].width += r1.width;
            comps[idx].height += r1.height;
            comps[idx].confidence = Math.max(comps[idx].confidence,
r1.confidence);
          }

          var seq2 = [];
          // calculate average bounding box
          for (i = 0; i < ncomp; i++) {
            var n = comps[i].neighbors;
            if (n >= min_neighbors)
              seq2.push({
                "x": (comps[i].x * 2 + n) / (2 * n),
                "y": (comps[i].y * 2 + n) / (2 * n),
                "width": (comps[i].width * 2 + n) / (2 * n),
                "height": (comps[i].height * 2 + n) / (2 * n),
                "neighbors": comps[i].neighbors,
                "confidence": comps[i].confidence
              });
          }

          var result_seq = [];
          // filter out small face rectangles inside large face rectangles
          for (i = 0; i < seq2.length; i++) {
            var r1 = seq2[i];
            var flag = true;
            for (j = 0; j < seq2.length; j++) {
```

```
            var r2 = seq2[j];
            var distance = Math.floor(r2.width * 0.25 + 0.5);

            if (i != j &&
              r1.x >= r2.x - distance &&
              r1.y >= r2.y - distance &&
              r1.x + r1.width <= r2.x + r2.width + distance &&
              r1.y + r1.height <= r2.y + r2.height + distance &&
              (r2.neighbors > Math.max(3, r1.neighbors) || r1.neighbors <
3)) {
              flag = false;
              break;
            }
          }

          if (flag)
            result_seq.push(r1);
        }
        return result_seq;
      }
    };
    return {
      "pre": pre,
      "core": core,
      "post": post
    };
  })
}

onmessage = function (event) {
  var data = (typeof event.data == "string") ? JSON.parse(event.data) :
event.data;
  var scope = {
    "shared": data.shared
  };
  var result = parallable.core[data.name].apply(scope, [data.input,
data.id, data.worker]);
  try {
    postMessage(result);
  } catch (e) {
    postMessage(JSON.stringify(result));
  }
}
```

Στιγμιότυπα εφαρμογής






Home / Log in to the site
Log in
Username
Password
Remember username
Log in
Forgotten your username or password?
Cookies must be enabled in your browser
Some courses may allow guest access
Log in as a guest
Is this your first time here?
Hi! For full access to courses you'll need to take a minute to create a new account for yourself on this web site. Each of the individual courses may also have a one-time "enrolment key", which you won't need until later. Here are the steps:
1. Fill out the New Account form with your details.
2. An email will be immediately sent to your email address.
3. Read your email, and click on the web link it contains.
4. Your account will be confirmed and you will be logged in.
5. Now, select the course you want to participate in.
6. If you are prompted for an "enrolment key" - use the one that your teacher has given you. This will "enrol" you in the course.
7. You can now access the full course. From now on you will only need to enter your personal username and password (in the form on this page) to log in and access any course you have enrolled in.
Create new account