ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ

Διπλωματική Εργασία

ΕΦΑΡΜΟΓΗ ΑΛΓΟΡΙΘΜΟΥ ΑΝΑΓΝΩΡΙΣΗΣ ΠΡΟΤΥΠΩΝ ΣΕ ΕΙΚΟΝΕΣ ΠΡΟΣΩΠΩΝ

Φοιτήτρια: Παλιούρα Ευθυμία
ΑΜ: 50106548

Επιβλέπων Καθηγητής

Πάτσης Γεώργιος
Καθηγητής

ΑΘΗΝΑ-ΑΙΓΑΛΕΩ,ΙΟΥΛΙΟΣ 2021

UNIVERSITY OF WEST ATTICA
FACULTY OF ENGINEERING
DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING

Diploma Thesis

APPLICATION OF PATTERN RECOGNITION ALGORITHM ON THE IDENTIFICATION OF FACES FROM IMAGES

Student: Palioura Efthymia
Registration Number: 50106548

Supervisor

Patsis Georgios
Professor

ATHENS-EGALEO, JULY 2021

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

Πάτσης Γεώργιος, Καθηγητής	Ραγκούση Μαρία, Καθηγήτρια	Φαμέλης Ιωάννης, Καθηγητής
Georgios Patsis Digitally signed by Georgios Patsis Date: 2021.07.23 13:36:37 +03'00' (Υπογραφή)	(Υπογραφή)	(Υπογραφή)

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

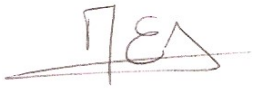
Η κάτωθι υπογεγραμμένη ...***Παλιούρα Ευθυμία...*** του ***…Γεωργίου***.., με αριθμό μητρώου …***50106548***… φοιτήτρια του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.
Επιθυμώ **άμεση διάθεση** στο πλήρες κείμενο της εργασίας μου.»

Η Δηλούσα

Παλιούρα Ευθυμία



Περίληψη

Ο σκοπός της εν λόγω διπλωματικής εργασίας είναι να επισημάνει την σημασία των αλγόριθμων που άλλαξαν ριζικά την χρήση του ηλεκτρονικού υπολογιστή, αλλά και ολόκληρης της κοινωνίας, αποδεικνύοντας για άλλη μια φορά ότι η τεχνολογική εξέλιξη ανοίγει καθημερινώς έναν ευρύ δρόμο προς τη βελτίωση του βιοτικού επιπέδου.

Θα αναλυθούν οι σημαντικότεροι αλγόριθμοι που αποτελούν τα θεμέλια της επιστήμης των υπολογιστών. Συγκεκριμένα, θα εξεταστεί η διαδικασία της ευρετηρίασης *(indexing)* που σχετίζεται με τον εντοπισμό *(matching)* και την κατάταξη *(ranking)* των πληροφοριών που αναζητούνται στο διαδίκτυο. Εν συνεχεία, θα παρουσιαστεί ο αξιοσημείωτος αλγόριθμος PageRank που άλλαξε την ιστορία της Google. Ακόμη, θα αναλυθεί η κρυπτογραφία δημόσιου κλειδιού *(public key cryptography)* και τα οφέλη που αποκομίζονται μέσω αυτής. Θα ειπωθεί επιπλέον ο πιο γνωστός κώδικας διόρθωσης σφαλμάτων *(error-correction code)*, υπογραμμίζοντας την χρησιμότητα εύρεσης του. Ακόμη, θα αναλυθεί η προσφορά της συμπίεσης δεδομένων *(data compression)* και θα επισημανθεί σε ποιές διεργασίες χρησιμοποιείται. Επιπλέον, συζητούνται οι βάσεις δεδομένων *(data bases*), διότι βελτίωσαν σημαντικά την αλληλεπίδρασή μας, παραδείγματος χάρη, με τα μέσα κοινωνικής δικτύωσης *(social media)* και τις διαδικτυακές αγορές. Στην πορεία, θα ερευνηθούν οι ψηφιακές υπογραφές *(digital signatures)* οι οποίες κατέχουν τη δική τους σημαντική θέση στο κόσμο των αλγόριθμων. Ύστερα, παρουσιάζεται ο τρόπος «εκπαίδευσης» των υπολογιστικών συσκευών όσον αφορά την αναγνώριση προτύπων *(pattern recognition)* και συγχρόνως θα παρουσιαστεί η διαδικασία και τα βήματα που απαιτούνται για μια επιτυχημένη αναγνώριση μέσω MATLAB. Τέλος, θα παρουσιαστούν κάποιοι αλγόριθμοι που είναι εν εξελίξει αλλά και πως μπορεί να μετεξελιχθεί ο αλγόριθμος που δημιουργήθηκε για την αναγνώριση προσώπων.

Λέξεις – κλειδιά

Ευρετηρίαση, PageRank, Κρυπτογραφία δημοσίου κλειδιού, Κώδικες διόρθωσης σφαλμάτων, Συμπίεση, Βάσεις δεδομένων, Ψηφιακές υπογραφές, Αναγνώριση προτύπων, Συνελικτικό Νευρωνικό Δίκτυο.

Abstract

The purpose of this thesis is to point out the importance of algorithms that radically changed the use of the computer, but also of the whole society, proving once again that technological development opens daily a wide road to the improvement of living standards.

The most important algorithms which are the foundation of computer science will be analyzed. Particularly, reference will be made to indexing which is related to the identification and classification of information searched on the internet. The remarkable PageRank algorithm that changed the history of Google will be presented. Furthermore, the public key cryptography and the benefits that are gained through it will be illustrated. Also, the creation of the most famous error correction code will be pointed out, emphasizing how useful it is. Data compression will be discussed next, and some applications in which it is used will be highlighted. Databases will be considered as well. These significantly improved our interaction with, for example, social media and online shopping. The digital signatures that hold their important place in the world of algorithms are investigated next. The method of "training" computing devices in respect of pattern recognition will be stated and at the same time will be highlighted the creation of a code which is capable to identify people. Finally, some algorithms currently being developed are also described but also how the algorithm of the chapter tree can be transformed.

Keywords

Indexing, PageRank, Public Key Cryptography, Error-Correction Codes, Data Compression, Databases, Digital Signatures, Pattern Recognition, Convolutional Neural Network.

Περιεχόμενα

Κατάλογος Πινάκων

Κατάλογος Εικόνων

Αλφαβητικό Ευρετήριο

ΕΙΣΑΓΩΓΗ

Ο αλγόριθμος ορίζεται ως μια πεπερασμένη σειρά ενεργειών, αυστηρά καθορισμένων και εκτελέσιμων σε πεπερασμένο χρόνο, στοχεύοντας στην επίλυση ενός προβλήματος.[1] Η αποδοτικότητα και η εύρυθμη λειτουργία της εκάστοτε υπολογιστικής συσκευής -laptop, smartphone, tablet- οφείλεται στους αλγόριθμους, διότι ακολουθώντας τα ακριβή βήματα τους ολοκληρώνεται το έργο. Γι' αυτό το λόγο θα γίνει αναφορά στους αλγόριθμους που συνέβαλαν στην τεχνολογική εξέλιξη και άλλαξαν μια για πάντα την χρήση του ηλεκτρονικού υπολογιστή.

Ιδιαίτερη έμφαση θα δοθεί σε κομμάτι της τεχνητής νοημοσύνης, εκείνο της αναγνώρισης προτύπων. Θα αναλυθεί διεξοδικά και συγχρόνως θα δημιουργηθεί κώδικας και με την βοήθεια του προγράμματος MATLAB και φυσικά μέσω συνελικτικού νευρωνικού δικτύου θα δέχεται ως είσοδος εικόνες διαφόρων προσώπων και θα ειδοποιεί αν τα αναγνωρίζει ή όχι.

Αντικείμενο της διπλωματικής εργασίας

Η συγκεκριμένη διπλωματική πραγματεύεται την εξοικείωση του απλού κόσμου με τους πιο αξιοσημείωτους αλγόριθμους που άλλαξαν ριζικά τον κόσμο δημιουργώντας ένα περιβάλλον με απεριόριστες ευκαιρίες για βελτίωση, ανάπτυξη και εξέλιξη. Αυτό θα επιτευχθεί μέσω απλών παραδειγμάτων από την καθημερινότητα, με αποτέλεσμα να ανοίγει ο δρόμος σε αυτόν το μαγικό ψηφιακό κόσμο.

Συνάμα αφού η αναγνώρισης προτύπων εξαπλώνεται με ταχύς ρυθμούς θα παρουσιαστεί εφαρμογή της κατά τη διαδικασία αναγνώρισης συγκεκριμένων ανθρώπων μέσω του συνελικτικού δικτύου συγκρίνοντας τα δεδομένα που δέχεται με εκείνα της βάσης δεδομένων που δημιουργήθηκε για τους σκοπούς της συγκεκριμένης διπλωματικής εργασίας.

Σκοπός και στόχοι

Μέσω της διπλωματικής θα γίνει άμεσα και πλήρως κατανοητό σε όλους, έχοντας ή μη μαθησιακό υπόβαθρο στην επιστήμη των υπολογιστών, η έννοια των αλγορίθμων και ιδιαίτερα τα οφέλη της βαθιάς μάθησης. Έτσι, κάθε φορά που θα χρησιμοποιείται η εκάστοτε υπολογιστική συσκευή, παραδείγματος χάρη για αναζήτηση πληροφοριών, ο χρήστης θα είναι σε θέση να γνωρίζει τον τρόπο που λειτουργεί και τι προϋποθέσεις χρειάζονται για την επίτευξη του κατάλληλου αποτελέσματος, ξεδιπλώνοντας ένα νέο κόσμο μπροστά του με απεριόριστες δυνατότητες για ενασχόληση.

Μεθοδολογία

Η μεθοδολογία της παρούσας διπλωματικής εργασίας διεξήχθη με στόχο την άντληση γνώσεων με ταυτόχρονη μελέτη βιβλιογραφίας επιστημονικών βιβλίων. Συγχρόνως, πραγματοποιήθηκε βιβλιογραφική επισκόπηση της τεχνολογικής αιχμής μέσω διαδικτύου αναζητώντας επιστημονικά άρθρα για εξελίξεις στο εν λόγω πεδίο. Εν κατακλείδι, έγινε χρήση του περιβάλλοντος *mySQL* και του περιβάλλοντος *MATLAB* στο κεφάλαιο αναγνώρισης προτύπων ώστε να υπάρξει διαφάνεια των λειτουργιών τους.

Καινοτομία

Η καινοτομία βρίσκεται στο ότι η εν λόγω διπλωματική απευθύνεται σε κάθε ηλικία προσαρμόζοντας καθημερινά γεγονότα συνδέοντας τα με τον ψηφιακό κόσμο παρουσιάζοντας την αίγλη, την γοητεία και τη δυνατότητα αυτού σε κάθε ενδιαφερόμενο. Συγχρόνως έχει δημιουργηθεί κώδικας ο οποίος θα αναγνωρίζει πρότυπα. Θα μπορούσε να χαρακτηριστεί και διαδραστικός αφού για την επιτυχημένη ολοκλήρωση του χρειάζεται αμφίδρομη αλληλεπίδραση από τον άνθρωπο, με εκείνον να καθορίζει πόσα και ποια δεδομένα επιθυμεί να δέχεται το συνελικτικό δίκτυο. Ο σχεδιασμός που βρίσκεται πίσω από την επιλογή και την παρουσίαση των συγκεκριμένων αλγόριθμων μπορεί να γίνει οδηγός για την πραγματοποίηση νέων ιδεών για άλλους σπουδαίους αλγόριθμούς που θα συμβάλλουν στην συνέχιση της βελτίωσης της ζωής του ανθρώπου σε κάθε τομέα, αφού το εύρος τους είναι μεγάλο και η συμβολή τους σε κάθε τομέα είναι υπαρκτή.

Δομή

Το πρώτο κεφάλαιο θα αναφερθεί στους αξιοσημείωτους αλγόριθμους που βελτίωσαν τον τομέα της τεχνολογίας, στην τεχνική της ευρετηρίασης, στον αλγόριθμό που εκτόξευσε την Google στην πρώτη θέση των μηχανών αναζήτησης, τον λεγόμενο PageRank, στη κρυπτογραφία δημόσιου κλειδιού εξηγώντας πως επιτυγχάνεται η ανταλλαγή «κλειδιών», στους κώδικες διόρθωσης σφαλμάτων που είναι η συχνότερη χρησιμοποιούμενη ιδέα, στην συμπίεση δεδομένων, στις βάσεις δεδομένων όπου χωρίς αυτές θα κατέρρεαν οι διαδικτυακές δραστηριότητες και στις ψηφιακές υπογραφές που αποτελούν αξιοσημείωτο τεχνολογικό επίτευγμα. Το δεύτερο κεφάλαιο συναντάται η αναγνώριση προτύπων μεταβλητών πληροφοριών και στο τρίτο κεφάλαιο θα γίνει η παρουσίαση εφαρμογών στην αναγνώριση προτύπων. Εν κατακλείδι, το τέταρτο κεφάλαιο συμπεριλαμβάνει τα συμπεράσματα και την αναφορά σε αλγόριθμους που θα βελτιώσουν το μέλλον.

1 ΚΕΦΑΛΑΙΟ 1ο : Υπολογιστικοί αλγόριθμοι που επηρεάζουν την καθημερινότητά

Ο στόχος του συγκεκριμένου κεφαλαίου είναι να επισημάνει την σημασία των αλγόριθμων που άλλαξαν ριζικά την χρήση των υπολογιστικών συσκευών. Θα αναλυθούν εκείνοι που αποτελούν τα θεμέλια για την τεχνολογική ανάπτυξη, που είναι άρρηκτα συνδεδεμένοι στην καθημερινότητα, ακόμη και των απλών χρηστών, που συμβάλουν στην επίλυση εύκολων ζητημάτων, αλλά και το πιο βασικό να σχετίζονται με την θεωρία της επιστήμης των υπολογιστών, αποκλείοντας αυτομάτως το υλισμικό του υπολογιστή και το δίκτυο.

1.1 Λειτουργία μηχανών αναζήτησης

Η αναζήτηση πληροφοριών στο διαδίκτυο αποτελεί καθημερινή δραστηριότητα για τους περισσότερους και είναι ομολογουμένως, η δημοφιλέστερη ενέργεια. Πίσω από την εκπληκτική τεχνολογία της **μηχανής αναζήτησης** *(search engine)*, κρύβεται μια ολόκληρη επιστήμη και μια τεράστια ομάδα ειδικών μηχανικών λογισμικού που κάνουν τα αδύνατα δυνατά για να εξυπηρετήσουν πάνω από τρεισήμισι δισεκατομμύρια αναζητήσεις ημερησίως. Γι' αυτό το λόγο μεγάλες εταιρείες και πανεπιστήμια προσπαθούν να βελτιώσουν με νέες και ευκολότερες μεθόδους την επίτευξη εύρεσης της ορθότερης και πιο εύστοχης απάντησης μέσα από τον τεράστιο όγκο πληροφοριών που εντοπίζονται μετά από μια επιτυχημένη ιστοαναζήτηση.

Το ερώτημα που προκύπτει λοιπόν είναι, *«Πως λειτουργεί μια μηχανή αναζήτησης;»*. Κάθε μεγάλη εταιρεία αναζήτησης διαθέτει ένα διεθνές δίκτυο από κέντρα δεδομένων, με χιλιάδες διακομιστές και προηγμένο εξοπλισμό δικτύωσης. Με το κατάλληλο υλισμικό και τους αλγόριθμους ισχυρό σύμμαχο επιτυχαίνεται η εύρεση της απάντησης που ταιριάζει περισσότερο. Ακολούθως παρουσιάζεται η διαδικασία.

1.1.1 Ανίχνευση

Για τη δημιουργία μιας μηχανής αναζήτησης που αναζητεί ιστοσελίδες *(web pages)*, είναι απαραίτητη προϋπόθεση η ύπαρξη αντιγράφων των σελίδων που θα αναζητηθούν. Οι ιστοσελίδες είναι εύκολο να αντιγραφούν, δεδομένου ότι προορίζονται για να ανακτηθούν μέσω διαδικτύου από τα προγράμματα περιήγησης *(browsers)*. Αυτομάτως λύνεται ένα σημαντικό πρόβλημα λήψης πληροφοριών αναζήτησης, δηλαδή ο τρόπος που θα λαμβάνονται τα δεδομένα από το μέρος που είναι αποθηκευμένα στη μηχανή αναζήτησης, το όνομα αυτής της διαδικασίας είναι **ανίχνευση** *(crawling)*.

Crawling είναι η διαδικασία που χρησιμοποιούν οι search engines τρέχοντας τα προγράμματα **crawlers** -εναλλακτικά robots ή spiders- για να ανιχνεύουν και να καταγράφουν στο **ευρετήριο** τους *(index)* ιστοσελίδες. Το πρόγραμμα που τις λαμβάνει ονομάζεται web crawler. Ο αλγόριθμος των crawlers που χρησιμοποιεί η εκάστοτε μηχανή αναζήτησης είναι διαφορετικός, αλλά η λειτουργία τους είναι παρόμοια. Ο crawler όταν ξεκινάει την ανίχνευση σε μια ιστοσελίδα διαβάζει πρώτα το αρχείο robots.txt –αρχείο που δημιουργείται από τον διαχειριστή της ιστοσελίδας περιέχοντας κανόνες προς τους ανιχνευτές για το που επιτρέπεται και που όχι να γίνει ανίχνευση-. Αν δεν υπάρχει το αρχείο γίνεται ανίχνευση σε όλες τις ιστοσελίδες του ιστότοπου. Περιηγείται λοιπόν στις ιστοσελίδες του ιστότοπου ακολουθώντας **συνδέσμους/υπερσυνδέσμους** *(links/hyperlinks)* μέσα σε αυτές, για να ανιχνεύσει περιεχόμενο σε νέες web pages μέχρι την εξάντληση όλων των links. Αν ο ανιχνευτής εντοπίσει link που οδηγεί σε άλλο website, τότε εκτελείται η διαδικασία του crawling και στις ιστοσελίδες του νέου ιστότοπου. Με αυτόν τον τρόπο ο crawler περιηγείται από ιστοσελίδα σε ιστοσελίδα προσπαθώντας να καταγράψει όσες περισσότερες μπορεί εμπλουτίζοντας το ευρετήριο της μηχανής αναζήτησης. Όσο πιο παλιό το site από το οποίο λαμβάνεται το link τόσο το καλύτερο, γιατί γίνεται ταχύτερα η διαδικασία ανίχνευσης από τη search engine.[3]

1.1.2 Ευρετηρίαση

Η έννοια της **ευρετηρίασης** *(indexing)* προέρχεται από πολύ παλιά, διεκδικώντας τον τίτλο της αρχαιότερης χρήσιμης ιδέας στην επιστήμη των υπολογιστών. Κατά τον εντοπισμό μίας καινούριας web page, εν ώρα crawling στον ιστό, οι crawlers εμφανίζουν το περιεχόμενο της ιστοσελίδας αυτής. Εκείνη τη στιγμή, η μηχανή αναζήτησης μετράει όλους τους παράγοντες κατάταξης που ισχύουν στον αλγόριθμο της για να κάνει ευρετηρίαση και κρατάει όλα αυτά τα δεδομένα στον δείκτη της Search Index που είναι μια τεράστια συστοιχία υπολογιστών με μεγάλο αποθηκευτικό χώρο άνω των 100 εκατομμυρίων GB.

Κάνοντας μια μικρή παρένθεση επιβάλλεται να αναφερθούν οι **παράγοντες κατάταξης** *(ranking factors)* που τοποθετούν μια web page στην πρώτη θέση της μηχανή αναζήτησης. Τονίζεται, ότι κάθε χρόνο προστίθεται και κάποιος νέος. Ο αριθμός των παραγόντων το 2021 ξεπερνάει τους διακόσιους. Η Google, που είναι η μεγαλύτερη και ισχυρότερη search engine, δεν έχει επιβεβαιώσει όλους του παράγοντες, αλλά μόνο τρείς εξ αυτών.[4] Οι παράγοντες μπορούν να χωρισθούν σε εννέα κατηγορίες. Σε κάθε κατηγορία θα αναφέρονται ενδεικτικά κάποια κριτήρια:

I. Domain Factors: αφορούν το όνομα της online παρουσίας *(domain name),* (ηλικία του site, λέξη κλειδί στην ονομασία).
II. Page-Level Factors: σχετίζονται με την ιστοσελίδα (πίνακας περιεχομένων, ταχύτητα φόρτωσης σελίδας στον browser Chrome).

III. Site-Level Factors: σχετίζονται με τον ιστότοπο (φόρμα επικοινωνίας, TrustRank).

IV. Backlink Factors: σχετίζεται με τους εισερχόμενους συνδέσμους (παλαιότερο domain τόσο το καλύτερο, πλήθος linking root domains δηλαδή ο αριθμός των domain που συνδέονται με ένα domain).

V. User Interaction: σχετίζεται με την αλληλεπίδραση των χρηστών (RankBrain μέρος αλγόριθμου artificial intelligence της Google, επανάληψη επισκεψιμότητας).

VI. Special Google Algorithm Rules: συμπεριλαμβάνει ειδικούς κανόνες (ωθεί νεότερες σελίδες, ιστορικό αναζήτησης χρηστών).

VII. Brand Signals: βασίζονται στο ποσοστό αναγνωσιμότητας του brand (αναζήτηση brand name και λέξης-κλειδί, σελίδα στο Facebook με πολλά likes, επίσημη σελίδα εταιρείας στο Linkedin).

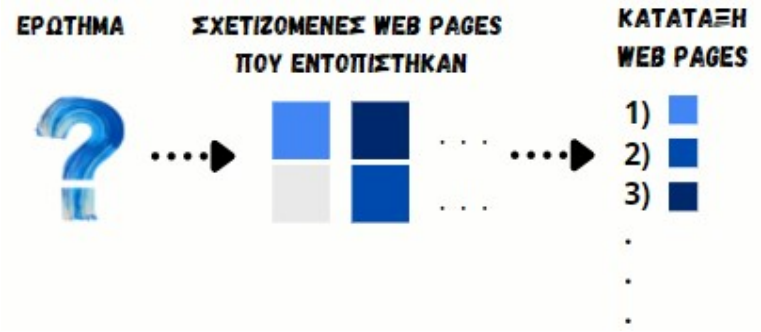
VIII. On-Site Web spam Factors: ιστορύπανση στο site (ανακατευθύνσεις, αναδυόμενα παράθυρα ή ανεπιθύμητες διαφημίσεις).

IX. Off-Site Web spam Factors: εξωτερικοί παράγοντες ιστορύπανσης (αφύσικη εισροή των συνδέσμων, σύνδεση προφίλ με υψηλό ποσοστό συνδέσμων χαμηλής ποιότητας).

Συνεχίζοντας με την έννοια της ευρετηρίασης κάθε καινούργια λέξη που εντοπίζει ο crawler την τοποθετεί αλφαβητικά. στο ευρετήριο όπου δηλώνεται πρώτα ο αριθμός της σελίδα, δεύτερον η θέση της λέξης στη σελίδα και οι μεταλέξεις και οι θέσεις αυτών αντιστοίχως. Οι **μεταλέξεις** *(metawords)* λειτουργούν σαν λέξεις κλειδιά που προσδιορίζουν πως ο web browser θα σχεδιάσει και θα παρουσιάσει το περιεχόμενο του, δηλαδή συμβάλλουν στη δομή των ιστοσελίδων. Η πιο διαδεδομένη μορφή γραφής ιστοσελίδων είναι η HTML και οι μεταλέξεις ονομάζονται ετικέτες *(tags).*Αν λοιπόν τεθεί κάποιο ερώτημα η μηχανή αναζήτησης μεταβαίνει γρήγορα στη καταχώρηση της λέξης στο index επιστρέφοντας ως απάντηση τις σελίδες στις οποίες βρίσκεται.

1.1.3 Εντοπισμός & Κατάταξη

Στο τρίτο και τελευταίο στάδιο προσπαθεί με βάση τον αλγόριθμο κατάταξης να ταξινομήσει στον δείκτη της τα πιο σχετικά και σημαντικότερα sites και web pages. Ο εντοπισμός επιτυγχάνεται με τις **μεταλέξεις** *(metawords)*, ενώ η κατάταξη με τον αλγόριθμο **PageRank** - θα αφιερωθεί η επόμενη υποενότητα 1.2 σε εκείνον-. Τη στιγμή που τίθεται ένα ερώτημα στις μηχανές αναζήτησης ο εντοπισμός και η κατάταξη -με τον εντοπισμό να ολοκληρώνεται πρώτος- συνδυάζονται στην ίδια διαδικασία ώστε να αυξηθεί η αποδοτικότητα. Η διαδικασία του εντοπισμού και της κατάταξης φαίνεται παρακάτω στην *εικόνα 1.1*.



Εικόνα 1.1 Εντοπισμός & Κατάταξη.

Όταν υποβάλλεται ένα ερώτημα στη μηχανή αναζήτησης προκύπτει πληθώρα αποτελεσμάτων με τον χρήστη να επιλέγει να εξετάσει τα πρώτα ελάχιστα. Γι' αυτό τον λόγο οι μηχανές αναζητητής πρέπει να εντοπίζουν τα καλύτερα αποτελέσματα και συγχρόνως να τα παρουσιάσουν κατατάσσοντας την καταλληλότερη σελίδα στην κορυφή και την λιγότερη σχετιζόμενη στο τέλος, όπως συνέβη και στην *εικόνα 1.1*, ταξινομούνται δηλαδή ανάλογα με την συνάφεια τους στο ερώτημα που τίθεται. Με την **εγγύτητα κατάταξης** *(ranking & nearness)* διασφαλίζεται η συνάφεια του ερωτήματος που τίθεται με τις σελίδες που εμφανίζονται. Για να κατατάξει ο υπολογιστής τις απαντήσεις σωστά υπάρχει μια εύκολη θεωρία η οποία υποστηρίζει, ότι όσο πιο κοντά εμφανίζονται οι λέξεις του ερωτήματος σε μία ιστοσελίδα τόσο πιθανότερο είναι να έχουν μεγαλύτερη συσχέτιση με το ερώτημα, συγκριτικά με εκείνες που απέχουν πιο πολύ.

1.2 PageRank

Οι συνιδρυτές της Google, Sergey Brin και Larry Page, σχεδίασαν τον αλγόριθμο PageRank -ως μέρος ενός ερευνητικού προγράμματος του Stanford University κατά τη διάρκεια του διδακτορικού τους που κατατάσσει τις ιστοσελίδες το 1997. Ο PageRank αφορά τους συνδέσμους, όσο υψηλότερο είναι το PageRank ενός συνδέσμου τόσο πιο έγκυρος είναι.

Στην παρακάτω *εικόνα 1.2* απεικονίζεται η μορφή του toolbar PageRank, πριν την απόφαση της Google να τον καταργήσει από την οθόνη το 2016, αλλά να τον χρησιμοποιεί παρασκηνιακά, αυτό συνέβη διότι οι SEO -με τον όρο SEO γίνεται αναφορά στις ενέργειες που χρησιμοποιούνται με σκοπό την απόκτηση επισκεψιμότητας από δωρεάν οργανικά αποτελέσματα των μηχανών αναζήτησης- έφτασαν στο σημείο να χειραγωγούν τις κατατάξεις. Το toolbar PageRank ήταν μια γραμμική αναπαράσταση λογαριθμικής κλίμακας μεταξύ 0 και 10, η βαθμολογία 0 αντιστοιχούσε στον ιστότοπο χαμηλής ποιότητας, ενώ η βαθμολογία 10 σε έγκυρους ιστότοπους. [6,7,8]

Εικόνα 1.2 PageRank toolbar. Πηγή: https://www.semrush.com/blog/pagerank/

Μπορεί να θεωρηθεί ως ένας βαθμός μέτρησης της σημαντικότητας μιας ιστοσελίδας, αναλύοντας την ποσότητα και την ποιότητα των συνδέσμων που οδηγούν σ' αυτήν. Με τον όρο ποσότητα γίνεται αναφορά στο πλήθος των υπερσυνδέσμων που οδηγούν σε μια συγκεκριμένη ιστοσελίδα, **υπερσύνδεσμος** *(hyperlink/link),* είναι φράση που βρίσκεται σε μια ιστοσελίδα του παγκόσμιου ιστού, υπογραμμισμένη με μπλε γράμματα, και μεταφέρει τον χρήστη σε μία νέα σχετιζόμενη ιστοσελίδα. Με τον όρο ποιότητα στην ουσία περιγράφεται η βαθμολογία που κατέχει το εκάστοτε link που οδηγεί στην κύρια ιστοσελίδα, διότι οι εισερχόμενοι σύνδεσμοι δεν αντιμετωπίζονται όλοι ισότιμα, αλλιώς είναι να εκφέρει άποψη ένας αρμόδιος επί του θέματος και αλλιώς ένας μη ειδικευμένος. Η βαθμολογία αυτή ονομάζεται **τέχνασμα αυθεντίας** *(authority trick*).[2] Σε υψηλότερη θέση θα είναι η σελίδα που έχει μεγαλύτερο πλήθος ιστοσελίδων που μέσω συνδέσμων οδηγούν προς αυτήν και συνάμα η βαθμολογία των ιστοσελίδων που οδηγούν στην κύρια να έχουν υψηλό βαθμό αυθεντίας. Παράδειγμα συνυπολογισμού του πλήθος των υπερσυνδέσμων και του τεχνάσματος αυθεντίας αποτελεί η *εικόνα 1.3* που δείχνει ότι η web page A τοποθετείται πρώτη στην κατάταξη, διότι οι σύνδεσμοι που οδηγούν προς αυτήν έχουν υψηλή βαθμολογία. Πρέπει να υπογραμμιστεί ότι ο PageRank διαιρείται ισόποσα μεταξύ των υπερσυνδέσμων που εισέρχονται στην εξεταζόμενη ιστοσελίδα.

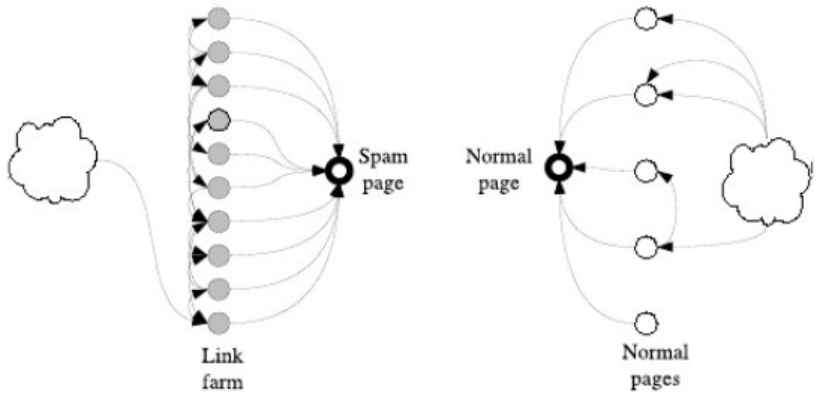
Εικόνα 1.3 Κατάταξη με βάση το πλήθος τον υπερσυνδέσμων και της βαθμολογίας τους. Πήγη: https://ahrefs.com/blog/how-to-improve-seo/

Δεν πρέπει να παραληφθεί ότι υπάρχουν περιπτώσεις όπου τα hyperlinks μπορούν να εκφράζονται με αρνητικό και μη χρηστικό τρόπο για κάποιες ιστοσελίδες στις οποίες καταδεικνύουν. Λόγω της ύπαρξης αυτών των συνδέσμων που επικρίνουν, αντί να συνιστούν μια ιστοσελίδα, η διαδικασία των υπερσυνδέσμων όντως τοποθετεί σελίδες σε υψηλότερη θέση απ' ότι θα τους άξιζε.

Νέα τροχοπέδη αποτελεί ο **κύκλος** *(cycle)*. Για την ανάδειξη της ιστοσελίδας τους οι κάτοχοι καταχράζονται τους υπερσυνδέσμους βελτιώνοντας τη θέση κατάταξης τους. Αυτό επιτυγχάνεται με αυτοματοποιημένα εργαλεία και με τη δημιουργία αναρίθμητων σελίδων που έχουν όλες συνδέσμους προς την ιστοσελίδα του κατόχου, παρεμβάλλοντας και χωρίς προσφέροντας καμία αξία στους χρήστες. Καταλήγοντας, η βαθμολογία της ιστοσελίδας τους να είναι αρκετές φορές μεγαλύτερη από την πραγματική τους αξία εξαπατώντας τους περιηγητές καταφέρνοντας να μένουν πρώτες. Αυτή τη δυσκολία περιγράφει και η *εικόνα 1.4* .

Εικόνα 1.4 Φαύλος κύκλος SEO.

Έτσι δημιουργείται και η **ιστορύπανση** (*web spam*) η οποία φαίνεται στην *εικόνα 1.5.* Στο αριστερό μέρος της εικόνας φαίνεται ότι όλα τα σχετιζόμενα links οδηγούν προς μια μόνο webpage, ενώ στο δεξί μέρος της εικόνας απεικονίζεται η φυσιολογική και μορφή μη-ιστορύπανσης που πρέπει να έχει το διαδίκτυο η οποία οδηγεί τον περιηγητή σε νέες σχετιζόμενες σελίδες προσφέροντας του επιπλέον γνώση.



Εικόνα 1.5 Webspam. Πηγή: Luca Becchetti, Carlos Castillo, Debora Donato, Stefano Leonardi, and Ricardo Baeza-Yates, Web Spam Detection: link-based and content-based technique.

Σύμφωνα με το Google Search Center για την καταπολέμηση του webspam το 2020 βοήθησε η **τεχνητή νοημοσύνη** *(artificial intelligence),* αφού σε συνεργασία με τους κάτοχους ιστότοπων και τους εξειδικευμένους επαγγελματίες της Google το ποσοστό του μειώθηκε σημαντικά.[9,11] Ο χαρακτηρισμός «διαισθητική τεχνολογία» της ταιριάζει εξαιρετικά. Τα φίλτρα *AI* αντιμετωπίζουν το webspam αναγνωρίζοντας τα ανεπιθύμητα μηνύματα και οδηγώντας τα αυτόματα σε έναν ανεπιθύμητο χώρο. Επίσης, η τεχνητή νοημοσύνη ανιχνεύει και το ανεπιθύμητο περιεχόμενο που συνδέεται με απειλές κακόβουλου λογισμικού αποτρέποντας το να εισέλθει στα εισερχόμενά του εκάστοτε χρήστη, αφού τα φίλτρα *AI* σαρώνουν κάθε εισερχόμενο μήνυμα και επισημαίνουν οποιοδήποτε ανεπιθύμητο περιεχόμενο. Όπως ειπώθηκε και άνωθεν υπάρχουν και αρνητικές-κακόβουλες κριτικές οι οποίες είναι μορφή spam.Τα φίλτρα τα αναγνωρίζουν από τη φήμη τους για την αποστολή κακών κριτικών. Τα φίλτρα τεχνητής νοημοσύνης βασίζονται στην συνεισφορά του ανθρώπου, αφού εκείνος αξιολογεί και αποκλείει τα ανεπιθύμητα μηνύματα.

1.3 Κρυπτογράφηση Δημόσιου Κλειδιού

Η **κρυπτογραφία** *(cryptography)* χρησιμοποιείται από τα αρχαία χρόνια, ένα από τα παλαιότερα συστήματα θεωρείται η κρυπτεία σκυτάλη ή «Λακεδαιμονική σκυτάλη» που χρησιμοποιήθηκε στη Σπάρτη.[16] Με την κρυπτογραφία επιτυγχάνεται η μετάδοση μηνυμάτων, αφότου μετασχηματιστούν

σε ακατανόητη μορφή για κάποιον τρίτο που επιχειρεί να τα υποκλέψει, διασφαλίζοντας τη μη διάρρευση των μηνυμάτων που μεταδίδονται. Ο κλάδος της κρυπτογραφίας έχει εξελιχθεί, έχοντας ιδιαίτερη σημασία για την ασφάλεια υπολογιστικών συστημάτων και επικοινωνιών.

Πέντε βασικές παράμετροι εξασφαλίζουν την αποτελεσματικότητα της κρυπτογραφίας αρχίζοντας από την *εμπιστευτικότητα*, καθώς η πληροφορία πρέπει να είναι απόρρητη σε όλους εκτός από τον αποστολέα και τον παραλήπτη. Ταυτόχρονα η *ακεραιότητα* που διασφαλίζει ότι μόνο τα εξουσιοδοτημένα μέλη της επικοινωνίας θα μπορούν να αποκωδικοποιήσουν το μήνυμα που μεταδίδεται. Επόμενοι παράμετροι είναι η *πιστοποίηση ταυτότητας* των μελών που συμμετέχουν στη μετάδοση και η *πιστοποίηση του μηνύματος* προφυλάσσοντας την πηγή και τον προορισμό του μηνύματος. Τελευταία παράμετρος είναι η *εξασφάλιση μη απάρνησης των μελών* που συμμετάσχουν στην μετάδοση πληροφοριών, μη μπορώντας να ισχυριστούν ότι δεν αναλαμβάνουν ευθύνη για κάθε ενέργεια που εκτελέστηκε.[17]

Τα είδη κρυπτοσυστημάτων είναι τα **συμμετρικά** *(symmetric)* και τα **ασσύμετρα** *(asymmetric)*. Στο συμμετρικό χρησιμοποιείται ένα κοινό κλειδί *(key)* για τις διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης έχοντας ως μέσω διασφάλισης της πληροφορίας την μυστικότητα του κλειδιού. Σε αυτό το είδος ανήκει ο πρώτος δημόσια προσιτός αλγόριθμος κρυπτογράφησης ο DES, αλλά λόγου του μικρού μήκους κλειδιού - 56-bit - δεν διακρίνεται για την ασφάλεια μετάδοσης πληροφοριών. Στα ασσύμετρα κρυπτοσυστήματα ή αλλιώς **κρυπτοσυστήματα δημόσιου κλειδιού** *(public key cryptography)* παρέχεται η δυνατότητα δυο κλειδιών, ενός δημοσίου και ενός ιδιωτικού. Το μέγεθος του κλειδιού διασφαλίζει την ισχύ της μυστικότητας του μηνύματος, όσα περισσότερα τα bit τόσο πιο αδιάσπαστο είναι το σύστημα κρυπτογραφίας.

Η κρυπτογραφία δημόσιου κλειδιού βασίζεται στο πρωτόκολλο Diffie-Hellman δίνοντας τη δυνατότητα και στις δυο πλευρές να μην έχουν κάποιο προσυμφωνημένο κλειδί, αλλά να συμφωνήσουν σε ένα ιδιωτικό κλειδί μέσω της ανταλλαγής του από ένα μη ασφαλή δίαυλο επικοινωνίας. Συγκεκριμένα, κατά την επίσκεψη του χρήστη σ' έναν ασφαλή ιστότοπο, ο οποίος αρχίζει με *«https:»*, ο υπολογιστής και ο server με τον οποίο επικοινωνεί δημιουργούν ένα κοινό μυστικό εφαρμόζοντας το πρωτόκολλο Diffie-Hellman κρυπτογραφώντας την επικοινωνία τους.

1.3.1 Διεργασία δημιουργίας κοινού μυστικού

Η μέθοδος δημιουργίας του κοινού μυστικού που θέλουν να ανταλλάξουν οι δύο πλευρές στηρίζεται σε δύο μαθηματικές μεθόδους στη **διακριτή ύψωση σε δύναμη** *(discrete exponentiation)* που αποτελεί μονόδρομη πράξη εξασφαλίζοντας ότι δεν μπορεί κανείς να την αναστρέψει ώστε να εκμαιεύσει τις πληροφορίες και στην **διακριτή λογαρίθμηση** *(discrete*

logarithm). Για την ολοκληρωμένη ανάλυση και επεξήγηση χρειάζεται επιπλέον η αριθμητική ρολογιού. Είναι γνωστό ότι σε ένα αναλογικό ρολόι, κάθε φορά που ο ωροδείκτης περνάει από το 12 ξεκινάει εκ νέου η μέτρηση από το 1. Μια ενέργεια που ξεκινάει στις 11 και ολοκληρώνεται στις 4 διαρκεί 5 ώρες, συνεπώς σε αυτό το δωδεκάωρο σύστημα ρολογιού μπορεί να ειπωθεί ότι 11+4=5. Η αριθμητική του ρολογιού διαφέρει σε δύο σημεία, πρώτον η αρίθμηση αρχίζει από το μηδέν και δεύτερον το μέγεθος του ρολογιού πρέπει να είναι πρώτος αριθμός δηλαδή να διαιρείται μόνο με το 1 και τον εαυτό του.

Εικόνα 1.6 Μέγεθος ρολογιού 11.

Στη *εικόνα 1.6* εμφανίζεται η μορφή του ρολογιού μεγέθους 11. Ο τρόπος λειτουργίας του είναι ο εξής, για να υπολογιστεί η πράξη 12+6 ορίζεται αρχικά η ταύτιση του 12 με κάποια θέση ψηφίου του ρολογιού της εικόνας, αρχίζοντας τη μέτρηση από το 0, με τη φορά του βέλους προς τα δεξιά, προσμετρούνται 12 μονάδες καταλήγοντας ότι ο αριθμός 12 είναι υποθετικά στη θέση του 1. Στην εκτέλεση της πράξης 12+6 λοιπόν το αποτέλεσμα είναι το 7, γιατί ξεκινώντας από το 1 - όπου το 1 και το 12 υποθετικά βρίσκονται στην ίδια θέση- και προσθέτοντας 6 μονάδες κατά τη φορά του βέλους το αποτέλεσμα είναι 7.

Αυτή η διαδικασία θα παρουσιαστεί με τις μαθηματικές πράξεις και κάποιους επιπλέον τύπους. Αρχικά, υπολογίζεται το άθροισμα 12+6 που ισούται με το 18. Το 18 διαιρείται με το 11, το μέγεθος του ρολογιού. Από αυτή την διαίρεση κρατείται μόνο το υπόλοιπο που είναι το 7.

Η μαθηματική πράξη που είναι απαραίτητη για την ορθή διατύπωση λειτουργίας του αλγορίθμου είναι εκείνη της ύψωσης σε δύναμη. Συγκεκριμένα, η πράξη 3*3*3*3 μπορεί να εκφραστεί με την ύψωση της δύναμης ως 3^4=81. Συνδυάζοντας την ύψωση σε δύναμη με την διαδικασία που αναλύθηκε διαιρείται το 81 με το 11, δηλαδή το μεγέθους ρολογιού και το υπόλοιπο είναι το 4. Στον πίνακα 3.1 εμφανίζονται οι αριθμοί 2, 3 και 6 υψωμένοι στις πρώτες 10 δυνάμεις σε αριθμητική ρολογιού μεγέθους 11. Κάθε αριθμός μπορεί να υπολογιστεί από τον παραπάνω του αριθμό. Δηλαδή, στον πίνακα ο αριθμός που συμβολίζει το 6^1 βρίσκεται στην πρώτη γραμμή, τέταρτη στήλη. Παραμένοντας στην ίδια στήλη το 6^2, όπου ισούται με το 36, αντιπροσωπεύεται από το νούμερο 3, αυτό συμβαίνει διότι γίνεται χρήση ρολογιού μεγέθους 11 και το 36 είναι ίσο με

33+3 (το 33 είναι πολλαπλάσιο του 11). Ο τρίτος αριθμός που υπάρχει είναι το 7 και αντικαθιστά το $216=6^3$. Το 7 βρέθηκε με πολύ πιο εύκολες και γρήγορες πράξεις, πολλαπλασιάζοντας το προηγούμενο αποτέλεσμα (το 3) με το 6, 3+6=18 και μετέπειτα διαιρώντας το 18 με το μέγεθος του ρολογιού το 11 , βρίσκοντας έτσι ότι το υπόλοιπο είναι 7. Με αυτό το σκεπτικό συμπληρώνεται και εμφανίζεται ο πίνακας 1.1.

$\mathbb{n}$	2^n	3^n	6^n
1	2	3	6
2	4	9	3
3	8	5	7
4	5	4	9
5	10	1	10
6	9	3	5
7	7	9	8
8	3	5	4
9	6	4	2
10	1	1	1

Πίνακας 1.1 Δέκα πρώτων δυνάμεων των αριθμών 2,3,6 με αριθμητική ρολογιού 11.

Παρουσιάζεται παράδειγμα το οποίο αναλύει την διαδικασία κρυπτογραφίας δημόσιου κλειδιού στην *εικόνα 1.7*. Δύο άτομα θέλουν να ανταλλάξουν μια πληροφορία χωρίς να μπορεί να την αντλήσει κανείς, η πληροφορία είναι ένα νούμερο. Στο χώρο που βρίσκονται υπάρχουν και άλλα άτομα. Κανόνας, αποτελεί ότι κάθε επικοινωνία πρέπει να είναι δημόσια. Για τη δημιουργία του κοινού μυστικού ακολουθούνται τα παρακάτω βήματα. Τα δύο άτομα διαλέγουν από έναν ιδιωτικό αριθμό η κοπέλα διαλέγει ως **ιδιωτικό νούμερο** *(private number)* το 8 και ο φίλος της το 9. Τώρα ορίζουν δύο **δημόσιους αριθμούς** *(public numbers)* τη **βάση** *(base)* που θα είναι το 2 και το **μέγεθος του ρολογιού** (*clock size)* που θα είναι το 11. Υπογραμμίζεται ότι η βάση πρέπει να είναι αρχική ρίζα του μεγέθους του ρολογιού, δηλαδή οι δυνάμεις να διατρέχουν κυκλικά όλες τις πιθανές τιμές του ρολογιού. Επόμενο βήμα είναι ο καθένας από τους συμμετέχοντες στην ανταλλαγή της πληροφορίας να δημιουργήσει τον δικό του ιδιωτικό-δημόσιο νούμερο *(private-public number-PPN)* εφαρμόζοντας την ύψωση σε δύναμη και την αριθμητική ρολογιού. Η σύνθεση των καινούργιων αριθμών θα γίνει με την εφαρμογή των εξής τύπων:

$$\mathbf{PPN=base^{private\ num}\ (clock\ size)}$$

Ως αποτέλεσμα από τον τύπο που διατυπώθηκε και βάση του πίνακα 1.1 οι ιδιωτικοί-δημόσιοι αριθμοί θα είναι:

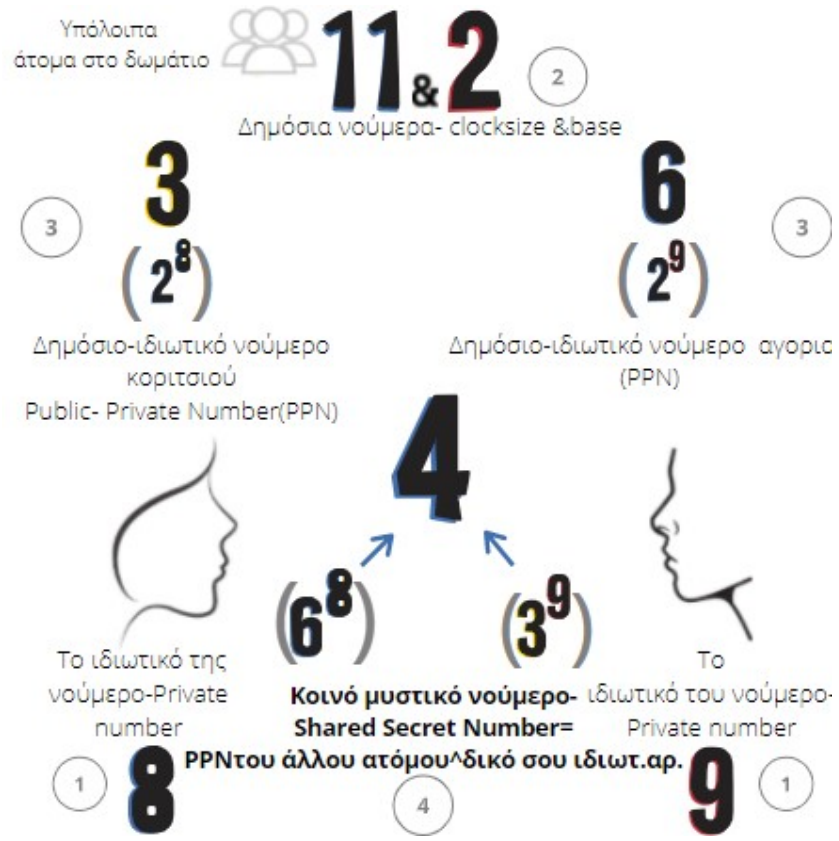
Κοπέλας: PPN= 2^8 =3

Αγοριού: PPN= 2^9=6

Τέταρτο και τελευταίο βήμα, είναι η δημιουργία του κοινού μυστικού αριθμού, που ήταν και ο στόχος εξαρχής και υλοποιείται με το κάτωθι τύπο:

Shared Secret Number = PPNτου άλλου ατόμου $^{\text{private num.}}$

Στην *εικόνα 1.7* φαίνονται τα βήματα της διαδικασίας που αναλύθηκε και τα νούμερα που βρέθηκαν μετά την εφαρμογή των τύπων.



Εικόνα 1.7 Πραγματική διαδικασία.

1.3.2 RSA & ECC

Οι αλγόριθμοι RSA και ECC αποτελούν προσεγγίσεις της κρυπτογραφίας δημόσιου κλειδιού. Η κρυπτογραφική ισχύ και στους δύο αλγορίθμους είναι ίδια, η διαφορά τους έγκειται στο μέγεθος του κλειδιού.

Ξεκινώντας από τον RSA η ασφάλειά του έγκειται σε μεγάλο βαθμό στη δυσκολία εύρεσης των πρώτων παραγόντων μεγάλων ακεραίων, εφόσον δεν έχει ανακαλυφθεί ακόμα ένας αλγόριθμος που να μπορεί να παραγοντοποιεί σε πολυωνυμικό χρόνο έναν ακέραιο. Οι πρώτοι αριθμοί θα πρέπει να είναι αρκετά μεγάλοι, ώστε ο καλύτερος γνωστός αλγόριθμος παραγοντοποίησης να απαιτεί χρόνο μεγαλύτερο από αυτόν με τον οποίο χρειάζονται για να προστατευθούν τα δεδομένα. Μια λανθασμένη του χρήση είναι πιθανόν να οδηγήσει σε μεγάλες αδυναμίες ασφάλειας. Έχει πολλές

εφαρμογές και χρησιμοποιείται σε πολλές συναλλαγές που απαιτούν ασφάλεια στο Internet. Εφαρμόζεται σε εμπορικά προϊόντα λογισμικού, βιομηχανίες για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων αλλά και ως ψηφιακή υπογραφή.[18]

Ο ECC *(Elliptic Curve Cryptography-Κρυπτογράφηση ελλειπτικής καμπύλης)* είναι αλγόριθμος που βασίζεται στις ελλειπτικές καμπύλες σε πεπερασμένα πεδία. Οι μαθηματικές συναρτήσεις στις οποίες βασίζεται είναι απλές στον υπολογισμό ως προς μία κατεύθυνση, αλλά είναι πολύ δύσκολο να αντιστραφούν. Η ασφάλεια βασίζεται στην αδυναμία υπολογισμού του διακριτού λογάριθμου ενός τυχαίου ελλειπτικού στοιχείου καμπύλης σε σχέση με ένα ευρέως γνωστό σημείο βάσης *(ECDLP)*, όπου σημαίνει όσο μικρό είναι το μέγεθος κλειδιού τόσο πιο ασφαλής παραμένει η πληροφορία που μεταφέρεται.[19] Το μικρό μέγεθος των κλειδιών καθιστά το ECC μια ιδανική λύση για συσκευές με περιορισμένο χώρο αποθήκευσης ή πόρους επεξεργασίας δεδομένων, οι οποίες ολοένα αυξάνονται στο πεδίο του IoT *(internet of things),* όπως είναι τα κινητά τηλέφωνα.

1.4 Κώδικες Διόρθωσης Σφαλμάτων

Κατά την μετάδοση πληροφοριών στις τηλεπικοινωνίες τα bits μεταδίδονται μέσω διαφορετικών τύπων καναλιών. Μερικά απ' αυτά είναι μη αξιόπιστα και δημιουργούν θόρυβο, παραδείγματος χάρη, εξαιτίας των γραμμών μεταφορών ή και ελαττωματικών συστημάτων με επακόλουθο να υποβαθμίζεται η ποιότητα της μετάδοσης της πληροφορίας και πιθανόν να καταστρέφονται τα μεταδιδόμενα bits. Οι ακολουθίες bit που υπέστησαν αλλαγές οδηγούν αυτομάτως σε σφάλμα μετάδοσης στον δέκτη. Γι' αυτό το λόγο, ο Αμερικανός μαθηματικός Richard Hamming δημιούργησε τον πρώτο αποτελεσματικό αλγόριθμο εντοπισμού και διόρθωσης σφαλμάτων, τον κώδικα **Hamming (7,4)** το 1950.

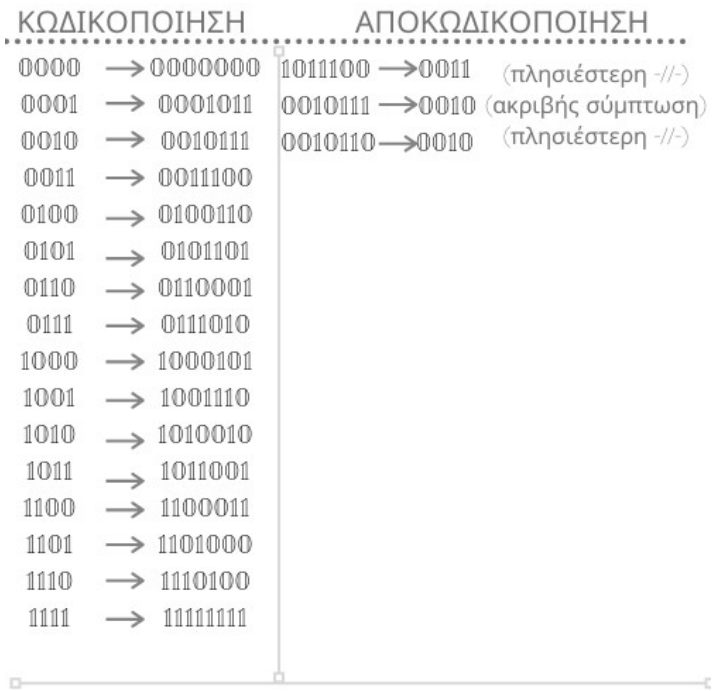
Οι **Error-correcting codes** *(ECC)* μέσω κατάλληλων αλγορίθμων κωδικοποιούν την πληροφορία με προσθήκη επιπλέον πληροφοριών. Στόχος είναι να εντοπίσουν και να διορθώσουν τα σφάλματα. Υπάρχουν δύο είδη ECC οι **κωδικοί τμήματος** *(block code),* που ανήκει και ο κώδικας Hamming (7,4) και οι **συνελικτικοί κώδικες** *(convolutional code*). Στους block codes το μήνυμα χωρίζεται σε τμήματα ή αλλιώς πακέτα συγκεκριμένου μεγέθους στα οποία προστίθενται **bits ισοτημίας** *(parity bits)* για την ανίχνευση και τη διόρθωση σφαλμάτων. Στους convolutional codes το μήνυμα λειτουργεί με ροές bit ή δεδομένων αυθαίρετου μήκους χρησιμοποιώντας συνήθως τον αλγόριθμο Viterbi για αποκωδικοποίηση. [23]

1.4.1 Πλεονασματικότητα & Hamming Code

Οι τρείς ζωτικές εργασίες που εκτελούνται μέσω Η/Υ είναι η εκτέλεση πράξεων, η αποθήκευση και η μετάδοση πληροφοριών. Η ύπαρξη των ηλεκτρονικών υπολογιστών χωρίς αυτές τις

θεμελιώδεις εργασίες θα ήταν ανούσια. Υπογραμμίζεται, ότι αν οι πληροφορίες που αποθηκεύονται και εν τέλει αποστέλλονται έχουν το παραμικρό σφάλμα τότε είναι άχρηστες.

Η βασική αρχή της αξιόπιστης επικοινωνίας δηλώνει ότι μαζί με το μήνυμα που αποστέλλεται μεταδίδεται και κάτι επιπλέον. Ο επιστημονικός όρος για τις επιπλέον πληροφορίες είναι η **πλεονασματικότητα** *(redundant)* και βεβαιώνει την αξιοπιστία του μηνύματος.[2] Ένας τρόπος χρήσης της πλεονασματικότητας είναι η αλλαγή του αρχικού μηνύματος σε ένα καινούργιο, μεγαλύτερο. Στην *εικόνας 1.8* παρουσιάζεται η κωδικοποίηση Hamming(7,4) η οποία κάνει ακριβώς αυτό.



Εικόνα 1.8 Κωδικοποίηση με Hamming (7,4).

Οι συνδυασμοί είναι δεκαέξι, διότι τα στοιχεία εισόδου είναι τέσσερα. Χρησιμοποιείται η πλεονασματικότητα κατά την κωδικοποίηση σε κάθε τετράδα ψηφίων με αποτέλεσμα να εμφανίζεται η κωδικοποιημένη λέξη των επτά ψηφίων που μεταδίδεται. Εξετάζεται αν η κωδικοποιημένη λέξη ταιριάζει με κάποια κωδικολέξη ακριβώς. Στην περίπτωση που δεν συμπίπτει με καμία τότε επιλέγεται η πλησιέστερη. Ο συγκεκριμένος κώδικας είναι σχεδιασμένος με τέτοιο τρόπο ώστε κάθε μεμονωμένο σφάλμα σε κάθε επταψήφια κωδικολέξη να διορθώνεται αποτελεσματικά χωρίς να υπάρχει αμφισημία.

1.4.2 Error correction memory & QR

Ο κώδικας Hamming χρησιμοποιείται στην μνήμη κωδικού διόρθωσης σφάλματος (*error correction memory*). Ο αλγόριθμος λόγω του ότι διορθώνει και εντοπίζει σφάλματα, όπου ο ρυθμός λαθών είναι χαμηλός, χρησιμοποιείται στην error correction memory που το σφάλμα είναι σπάνιο.

Ο κώδικας **Reed-Solomon** χρησιμοποιείται ευρέως και μπορεί να διορθώσει ταυτοχρόνως πολλά σφάλματα ανά κωδικολέξη. Αυτός ο αλγόριθμος βασίζεται στην άλγεβρα πεπερασμένων σωμάτων, δηλαδή είναι ένας συνδυασμός του κλιμακωτού αθροίσματος και της διδιάστατης ισοτιμίας. Χρησιμοποιείται στα CD, DVD, σε τεχνολογίες μεταδόσεις (DSL), σε κωδικούς QR αλλά και σε άλλες ποικίλες εφαρμογές. Τονίζεται, ότι εξαιτίας της πανδημίας COVID-19 μέσω smartphone γίνεται σάρωση του κωδικού QR μετατρέποντας τον αυτόματα σαν ως ένα σύστημα προβολής πληροφοριών «χωρίς άγγιγμα». Σε διάφορες επιχειρήσεις λαμβάνει ο QR τη θέση χαρτιών εμφανίζοντας διαδικτυακή έκδοση των πληροφοριών, αφού μπορεί να αποθηκευτεί ένας σύνδεσμος που να οδηγεί σε μια ιστοσελίδα.[25]

Εικόνα 1.9 Κωδικός QR για Βικιπαίδεια. Πηγή: https://el.wikipedia.org/wiki/%CE%9A%CF%8E%CE%B4%CE%B9%CE%BA%CE%B1%CF%82_QR

1.5 Συμπίεση Δεδομένων

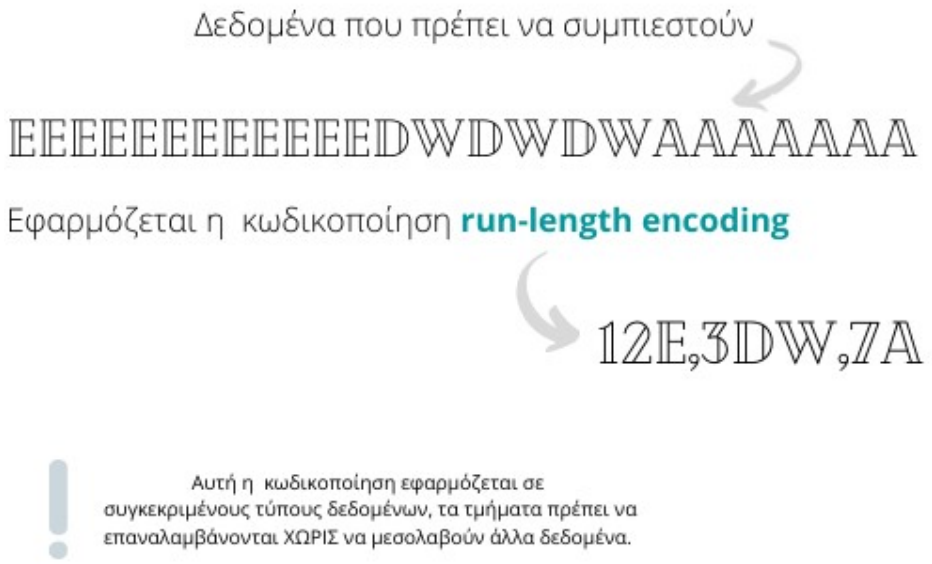
Η **συμπίεση αρχείων** *(data compression)* προσφέρει τη δυνατότητα μείωσης όγκου των αρχείων οποιασδήποτε μορφής έως και 99% του αρχικού μεγέθους, είτε σε αυτόνομα -εικόνα, ήχος, κείμενο- είτε σε συμπιεσμένους φάκελους -ZIP, RAR-. Με αυτή τη μέθοδο επιτυγχάνεται

εξοικονόμηση αποθηκευτικού χώρου και η μεταφορά αρχείων μέσω internet διεξάγεται ταχύτερα Η συμπίεση εξασφαλίζει την δυνατότητα γρήγορης μεταφοράς και λήψης δεδομένων σε λιγότερο χρόνο, στην καλύτερη ποιότητας με την κατάληψη λιγότερου αποθηκευτικού χώρου. [28] Η συμπίεση χρησιμοποιείται και παρασκηνιακά, παραδείγματος χάρη πολλά μηνύματα που στέλνονται μέσω διαδικτύου συμπιέζονται χωρίς να το γνωρίζει ο χρήστης. Το ίδιο συμβαίνει και κατά τη διάρκεια τηλεφωνικών συνομιλιών, γιατί έτσι εξυπηρετούνται πιο ωφέλιμα οι πόροι των τηλεφωνικών υπηρεσιών συμπιέζοντας τα δεδομένα φωνής πριν τη μετάδοση τους. Απαραίτητη προϋπόθεση είναι φυσικά ότι μετά τη συμπίεση θα πρέπει τα αρχεία να επανέλθουν στην αρχική τους μορφή, να αποσυμπιεστούν δηλαδή.

1.5.1 Μορφές συμπίεσης

Υπάρχουν δύο μορφές συμπίεσης, η συμπίεση με απώλειες, **απωλεστική συμπίεση** *(lossy data compression)* και η συμπίεση χωρίς απώλειες, **μη απωλεστική** *(lossless data compression).*Όσον αφορά τη μη απωλεστική εφαρμόζεται σε περιπτώσεις, αρχείων κειμένων ή εφαρμογών, που δεν πρέπει να τροποποιηθούν, διότι η παραμικρή ανεπιθύμητη αλλαγή αποφέρει αρνητικές συνέπειες. Ειδικότερα κατά την εκτέλεση προγράμματος κάθε αλλαγή στον κώδικα μπορεί να οδηγήσει στη μη εκτέλεσή του. Κεντρική ιδέα τη lossless compression αποτελεί ο εντοπισμός τμημάτων δεδομένων που είναι όμοια μεταξύ τους και εφαρμόζοντας κάποιο τέχνασμα περιγράφονται κάθε φορά τα κομμάτια που έχουν επαναληφθεί. Τονίζεται, ότι με την μη απωλεστική μέθοδο δεν πετυχαίνεται μεγάλη εξοικονόμηση χώρου, παρ' όλα αυτά για συγκεκριμένους τύπους αρχείων η μείωση είναι ουσιώδης.[2]

Επί παραδείγματι, πρέπει να συμπιεστεί το ακόλουθο απόσπασμα της *εικόνας 1.10*, χωρίς φυσικά να υπάρξουν απώλειες ώστε να μπορεί μετά να αποσυμπιεστεί ορθά.

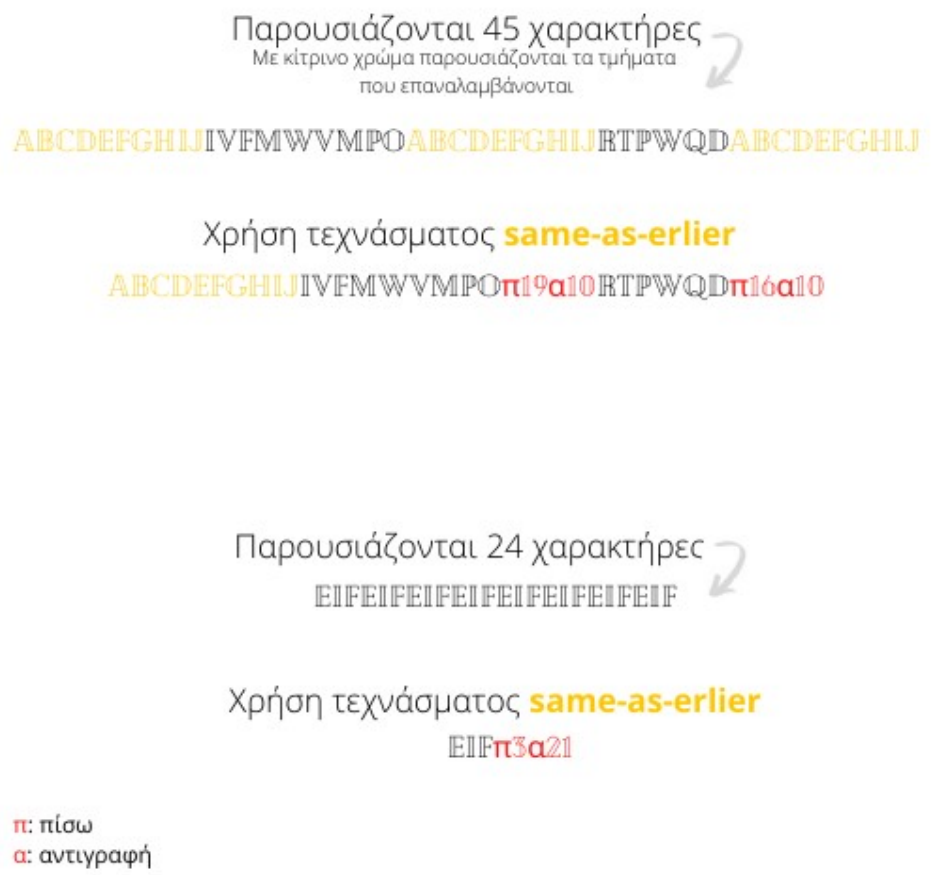


Εικόνα 1.10 Παράδειγμα συμπίεσης, run-length encoding.

Παρατηρείται στην *εικόνα 1.10* ότι επαναλαμβάνονται αλληλουχίες ίδιων στοιχείων οπότε επιλέγεται να εφαρμοστεί η κωδικοποίηση **μακροσειριακή κωδικοποίηση** *(run-length encoding)*. Χρησιμοποιείται σε συγκεκριμένο τύπο δεδομένων μόνο όπου υπάρχουν επαναλαμβανόμενα γειτονικά μοτίβα. Όπως φαίνεται στην απεικόνιση οι χαρακτήρες που κωδικοποιούνται είναι δίπλα ο ένας στον άλλον χωρίς να υπάρχει μεσολάβηση άλλου μοτίβου. Τα μηχανήματα φαξ χρησιμοποιούν αυτή την κωδικοποίηση συνδυαστικά με την κωδικοποίηση Huffman.

1.5.2 Ίδιο με πριν

Ένα πιο σύγχρονο τέχνασμα που χρησιμοποίει παρόμοια λογική με την κωδικοποίηση run-length encoding, δηλαδή τον εντοπισμό επαναλήψεων ίδιων τμημάτων, είναι το τέχνασμα **ίδιο με πριν** *(same as earlier)* με την διαφορά ότι λειτουργεί αποτελεσματικά χωρίς να υπάρχουν γειτονικές επαναλήψεις. Στην ακόλουθη *εικόνα 1.11* παρουσιάζονται δύο παραδείγματα με το εν λόγω τέχνασμα.



Εικόνα 1.11 Παράδειγμα Same as earlier.

Και στις δύο συμβολοσειρές εμφανίζονται τμήματα χαρακτήρων που επαναλαμβάνονται. Για να μειωθεί ο όγκος του αρχείου επιλέγεται τα επαναλαμβανόμενα τμήματα να κωδικοποιηθούν. Για να υπάρχει απόλυτη ακρίβεια κάθε φορά θα αναφέρεται πριν πόσους χαρακτήρες συναντήθηκαν τα όμοια τμήματα. Το σύμβολο «π» δηλώνει το «*πίσω*» και το μήκος του τμήματος που αντιγράφεται συμβολίζεται με το *«α»*. Η διαδικασία μετατροπής αρχείων σε ZIP και RAR αρχίζει με το αρχικό μη συμπιεσμένο αρχείο να μετατρέπεται βάση της μεθόδου **ίδιο με πριν**, για να κωδικοποιηθούν τα επαναλαμβανόμενα τμήματα και να αντικατασταθούν με συντομότερα. Το νέο αρχείο εντοπίζει τους χαρακτήρες που εμφανίζονται συχνότερα και δημιουργεί έναν πίνακα που θα αποδίδει στα συχνότερα γράμματα έναν αριθμητικό κώδικα μικρού μήκους και στα πιο σπάνια μεγαλύτερου μήκους. Τέλος, το αρχείο μετασχηματίζεται ξανά με απευθείας μετάφραση στους νέους κωδικούς. Ο τελικός πίνακας κωδικών αποθηκεύεται στο κοινό αρχείο που βρίσκεται το ZIP, γιατί διαφορετικά θα ήταν αδύνατο να αποκωδικοποιηθεί. Πρέπει να τονιστεί ότι σε κάθε αρχείο υπάρχει και καινούργιος πίνακας που δημιουργείται, στην πραγματικότητα τα αρχεία χωρίζονται σε τμήματα και για το εκάστοτε τμήμα δημιουργείται ο αντίστοιχος πίνακας. [2]

1.5.3 Απωλεστική συμπίεση

Η συγκεκριμένη μορφή χρησιμοποιείται σε αρχεία εικόνων όπου χάνονται οριστικά δεδομένα επιτυγχάνοντας μείωση όγκο. Όσον αφορά τις εικόνες υπάρχει μείωση χρωμάτων. Η διαφορά δε γίνεται αντιληπτή, διότι το ανθρώπινο μάτι δεν αντιλαμβάνεται όλα τα μήκη κύματος που μπορεί παράγει ο υπολογιστής. Με τον περιορισμό των χρωμάτων μειώνεται ο όγκος, αλλά η ποιότητα δεν χάνεται. Υπογραμμίζεται, ότι η αρχική ποιότητα του αρχείου δεν μπορεί να ανακτηθεί ξανά. Η πιο διάσημη απωλεστική συμπίεση εικόνων γίνεται με το ISO/IEC10918-1,το γνωστό δηλαδή JPEG (*Joint Photographic Experts Group*).Αυτό το πρότυπο εκτελεί συμπιέσεις κάθε επιπέδου ανάλογα με το τι ζητά ο χρήστης και πόσο θέλει να μεταβάλει την ποιότητα. Οι αλλοιώσεις που μπορεί να παρατηρηθούν, αν η συμπίεση είναι μεγάλο βαθμού, είναι η αλλαγή χρωμάτων, η ανομοιομορφία που μπορεί να υπάρξουν ανάμεσα στις χρωματικές αποχρώσεις και η ύπαρξη οδοντωτών άκρων. [28] Τα στάδια που ακολουθούνται σε αυτού του είδους συμπίεσης είναι αρχικά ο διαχωρισμός της εικόνας σε μικρά τετράγωνα των 8x8 pixels άρα αναπαριστάται από 64 αριθμούς. Στην περίπτωση που ένα τετράγωνο (8x8) συμβολίζει ένα χρώμα τότε μπορεί να αναπαρασταθεί ολόκληρο από έναν αριθμό με αποτέλεσμα να εξαλείφονται 63 αριθμοί. Ακόμη αν το τετράγωνο αποτελείται από ένα χρώμα, αλλά διαφορετικού τόνου ο υπολογιστής είναι ικανός να δηλώσει το τετράγωνο αυτό με έναν αριθμό, οπότε πάλι προκύπτει καλή συμπίεση και η εικόνα στη τελική μορφή θα έχει ελάχιστα σφάλματα. Αν υπάρχει μεταβολή από ένα χρώμα σε άλλο τότε οι 64 αριθμοί θα μπορούσαν να αναπαρασταθούν μόνο από δύο νούμερα παραλείποντας 62.

Το πρότυπο Mpeg 1 layer III ή πιο διαδεδομένα Mp3 είναι η δημοφιλέστερη μορφή συμπίεσης ήχου. Κωδικοποιεί τον ψηφιακό ήχο αφού μειωθεί το αρχικό αρχείο, ενώ ταυτόχρονα διατηρεί την ποιότητα του. Με βάση το ψυχοακουστικό πρότυπο – δηλαδή κατά πόσο επηρεάζεται η αντίληψη του ανθρώπου σε ένα συγκεκριμένο ήχο- καταργεί συχνότητες που δεν αντιλαμβάνεται ο άνθρωπος κωδικοποιώντας με περισσότερα bit τα σημαντικά τμήματα διατήρησης ποιότητας ήχου, ενώ στην περίπτωση των συχνοτήτων που δεν ακούγονται λόγω ακουστικής συγκάλυψης κωδικοποιούνται με λιγότερα bit.[29]

Η συμπίεση βίντεο συνδυάζει στοιχεία από τους αλγόριθμους που συμπιέζουν την εικόνα και τον ήχο, αφού το βίντεο δημιουργείται από καρέ που συνοδεύονται από ήχο. Η δημοφιλέστερη κωδικοποίηση σήμερα είναι η MPEG4 Part 14 γνωστή ως «.mp4». [28]

Τα GIF έχουν διαδοθεί και χρησιμοποιούνται ευρέως στα μέσα κοινωνικής δικτύωσης. Χρησιμοποιείται ο αλγόριθμος LZW για την συμπίεση των δεδομένων χωρίς να υποβαθμίζεται παραπάνω η ποιότητα τους. Το σημαντικό εδώ είναι ότι η ποιότητα τους εξ αρχής είναι χαμηλή, αφού υποστηρίζουν μονό 8-bit χρωματική παλέτα -256 χρώματα δηλαδή-.

1.6 Βάσεις Δεδομένων

Οι ηλεκτρονικοί υπολογιστές από την πρώτη στιγμή απέδειξαν ότι είναι τα κατάλληλα μέσα αποθήκευσης (*data storage*) και επεξεργασίας δεδομένων. Στις δεκαετίες του ’40 και του ’50 υπήρχαν οι μαγνητικές ταινίες (*magnetic tapes*) αποτελώντας τα μέσα μόνιμης αποθήκευσης, όπου σήμερα χρησιμοποιούνται ως αντίγραφα ασφαλείας (*backup*), κυρίως από εταιρείες. Τότε δεν απέδιδαν στο μέγιστο βαθμό, διότι μειονεκτήματα τους, όπως η ευθραυστότητα ή σειριακή προσπέλαση *(sequential access),* καθιστούσαν χρονοβόρα την ανεύρεση πληροφοριών, προκαλώντας την ανάγκη για δημιουργία νέων μέσων. Έτσι, το 1959 ιδρύθηκε η ομάδα CODASYL με σκοπό την δημιουργία μιας γλώσσας χειρισμού δεδομένων και το ’60 δημιουργηθούν τα πρώτα μέσα αποθήκευσης άμεσης προσπέλασης *(random access)* -drums, hard disk drives- τα οποία βοήθησαν στην εξέλιξη της αποθήκευσης και της διαχείρισης δεδομένων. Εκείνη τη στιγμή γεννήθηκε η ανάγκη για οργάνωση, χειρισμό και αποθήκευση των δεδομένων αυτών. Η έννοια της **βάσης δεδομένων** *(database, DB)* ήρθε στο προσκήνιο το ’62 προσφέροντας στους χρήστες ταυτόχρονη δυνατότητα αλληλεπίδρασης με τα δεδομένα. Μετά από διάφορες διεργασίες και πειραματισμούς δημιουργήθηκε η σημερινή μορφή των databases.

Σήμερα χρησιμοποιούνται ευρέως από την πλοήγηση σε κάποια web page μέχρι τις τραπεζικές δοσοληψίες, σε συνδυασμό φυσικά με το διαδίκτυο και την κρυπτογραφία δημόσιου κλειδιού. Συγκεκριμένα, δίνονται εντολές και με την βοήθεια ενός Συστήματος Διαχείρισης Βάσης Δεδομένων *(DBMS-database management system)* σώζονται τα δεδομένα.[30] Το DBMS είναι η εφαρμογή που αλληλεπιδρά με τους τελικούς χρήστες και τη DB για την εισαγωγή, αποθήκευση ,διαγραφή, επεξεργασία και ανάκτηση πληροφοριών και η διαχείριση των δεδομένων πραγματοποιείται με query languages QL. Η πιο διαδεδομένη γλώσσα προγραμματισμού στις βάσεις δεδομένων είναι η SQL ως γλώσσα σύνταξης ερωτημάτων.[30] Η DB αποτελεί μια οργανωμένη συλλογή μορφοποιημένων σχετιζόμενων δεδομένων. Χωρίς αυτές θα υπήρχε η αδόμητη μορφή πληροφορίας που θα επέφερε πολλές δυσχέρειες.

Οι βασικές αρχές που διέπουν τις βάσεις δεδομένων είναι η **εκ των προτέρων πρακτικογράφηση** *(write-ahead logging,WAL),* η **οριστικοποίηση δύο φάσεων** *(prepare & commit)* και οι **σχεσιακές βάσεις δεδομένων** *(relational database).* Η WAL δημιουργήθηκε για να κρατάει πρακτικά για κάθε ενέργεια που γίνεται και στην περίπτωση που ολοκληρωθούν όλα τα βήματα μόνο διαγράφεται. Στην περίπτωση που ο υπολογιστής καταρρεύσει εν μέσω της συναλλαγής μετά την επανεκκίνηση η βάση ενεργοποιείται ξανά και βρίσκει στο σκληρό δίσκο τις πληροφορίες που έχουν καταγραφεί στη WAL, ο υπολογιστής διακρίνει ότι ίσως βρισκόταν στη μέση της δοσοληψίας, διότι τα πρακτικά έχουν καταγεγραμμένες πληροφορίες. Υπογραμμίζεται,

ότι ο υπολογιστής δεν ενδιαφέρεται για το ποιες διαδικασίες έχουν τελεστεί και ποιες όχι, διότι το σύστημα είναι σχεδιασμένο έτσι ώστε να δίνει το ίδιο αποτέλεσμα ανεξάρτητα από το πόσες φορές θα τις εκτελέσει. Τέλος, μετά την ολοκλήρωση της διαδικασίας διαγράφεται η καταχώρηση των πρακτικών. Έτσι εκτελείται κάθε ενέργεια με ασφάλεια. Όποιο σύνολο πρακτικογραφημένων ενεργειών δεν τελειώνει με τη φράση *«end transaction»* αναιρείται και με αντίστροφη σειρά οι ενέργειες και η βάση επανέρχεται στην κατάσταση στην οποία βρισκόταν αρχικά.

Οι **ομοιοτυπημένες βάσεις** *(replicated databases)* είναι η λύση στο πρόβλημα του πως να μην χαθούν ή αλλοιωθούν τα δεδομένα των πελατών εξαιτίας κάποιας βλάβης σκληρών δίσκων, σφαλμάτων λογισμικού *(software)* είτε αστοχίες υλισμικού *(hardware)*. Όσον αφορά τις τραπεζικές συναλλαγές η απώλεια στοιχείων είναι ανεπίτρεπτη με την τράπεζα να βρίσκεται αντιμέτωπη με σοβαρές νομικές και οικονομικές κυρώσεις αν συμβεί απώλεια δεδομένων, ακόμη και στις διαδικτυακές πωλήσεις δεν τίθεται κανένα περιθώριο λάθους. Γι' αυτό το λόγο εφευρεθεί η ομοιοτυπημένη βάση δεδομένων που απαρτίζει το πλήθος των αντιγράφων της βάσης δεδομένων. Κάθε αντίγραφο αποκαλείται ομοιότυπο διατηρεί όλα τα αντίγραφα ενημερωμένα ανά πάσα στιγμή Υπάρχουν περιπτώσεις που δεν μπορούν να ολοκληρωθούν οι δοσοληψίες οπότε πρέπει να γίνει ανάκληση (*rolling back transactions*)

Η **οριστικοποίηση δύο φάσεων** συμβάλει στην επίλυση της ανάκλησης σε μία ομοιοτυπημένη βάση δεδομένων, διότι ένα από τα ομοιότυπα μπορεί να βρεθεί αντιμέτωπο με ένα πρόβλημα και να πρέπει να εφαρμοστεί ανάκληση ενώ στα υπόλοιπα ομοιότυπα όχι. Η πρώτη φάση ονομάζεται **προετοιμασία** και η δεύτερη **οριστικοποίηση ή ματαίωση** *(prepare & commit)* ανάλογα με την περίσταση.

Οι **σχεσιακές βάσεις** κάνουν πιο εύκολη την διαδικασία συλλογής και πρόσβασης δεδομένων. Στην πραγματικότητα μια βάση δεδομένων αποτελείται από πληθώρα πινάκων. Ο κάθε πίνακας αναφέρεται σε ένα συγκεκριμένο αντικείμενο και περιέχει διάφορα πεδία με σχετιζόμενες πληροφορίες. Ο κάθε πίνακας χαρακτηρίζεται από το **πρωτεύων κλειδί** (*primary key*)**,** δηλαδή από μια μοναδική τιμή που προσδιορίζει κάθε εγγραφή. Το primary key δεν μπορεί να είναι Null. Η τιμή *NULL* δηλώνει απουσία τιμής σε κάποιο πεδίο. Σημαντικό είδος κλειδιού είναι και το **ξένο κλειδί** (*foreign key*) που αποτελεί το πρωτεύον κλειδί κάποιου άλλου πίνακα, δηλαδή αποτελεί τρόπο σύνδεσης πινάκων Με την ύπαρξη των κλειδιών μειώνονται οι αναδιατυπώσεις και ο συνολικός αποθηκευτικός χώρος, αφού δεν επαναλαμβάνονται κοινά δεδομένα. Οι βάσεις έχουν τη δυνατότητα να ανατρέχουν σε αυτά τα κλειδιά με μεγάλη ταχύτητα. Εν ολίγης είναι σαν ένα ψηφιακό λεξικό. Εστιάζει γρήγορα στα δεδομένα που αναζητούνται υπολογίζοντας πόσα πεδία πρέπει να παραλείψει για να εμφανίσει την ορθή απάντηση.

Η SQL αποτελεί την πιο διαδεδομένη γλώσσα χειρισμού βάσεων αναζήτησης. Μέσω του λογισμικού MySQL θα δημιουργηθεί μια βάση δεδομένων και εν συνεχεία θα τεθούν διάφορα ερωτήματα για την διαπίστευση της εύρυθμης λειτουργικότητας της. Μερικές ενδεικτικές εντολές είναι *CREAT DATABASE* για δημιουργία βάσης δεδομένων, για την εμφάνιση όλων των βάσεων *SHOW DATABASES*, για διαγραφή βάσης *DROP DARABASE [όμονα βάσης], η εντολή INSERT* για εισαγωγή στοιχείων, *DELETE* για διαγραφή, *UPDATE* για ενημέρωση στοιχείων, CREATE TABLE για δημιουργία πίνακα, *INSERT VALUES* για εισαγωγή τιμών στους πίνακες. Καθοριστική λειτουργία είναι επίσης η συνένωση πινάκων το λεγόμενο *JOIN* με την οποία δημιουργούνται εικονικοί-προσωρινοί πινάκες (όψη) μονό για να απαντηθούν ερωτήματα που συνδυάζουν στοιχεία από διαφορετικούς πίνακες.

Συγκεκριμένα, θα δημιουργηθεί βάση δεδομένων η οποία θα αφορά την οργάνωση της ετήσιας έκθεσης Θεσσαλονίκης και στην συνέχεια μόλις ολοκληρωθεί θα τεθούν διάφορα ερωτήματα για να διαπιστωθεί αν είναι όλα ορθά.

Πρώτο βήμα είναι η δημιουργία της βάσης στο σύστημα, χρησιμοποιώντας την εντολή *CREATE DATABASE ekthesi_thessalonikis;* και στην συνέχεια χρησιμοποιείται η εντολή *USE ekthesi_thessalonikis;* η οποία επιτρέπει στο χρήστη να κάνει εισαγωγή των πινάκων στη βάση. Οι εντολές που χρησιμοποιούνται για την κατασκευή των πινάκων και την εισαγωγή των εγγραφών φαίνονται στην *εικόνα 7.8.* Έχουν δημιουργηθεί οκτώ πίνακες, ο κάθε πίνακας δημιουργείται με την εντολή CREATE και περιέχει τις στήλες που θα έχει αλλά και το ποιες προδιαγραφές πρέπει να τηρούν ώστε να γίνονται σωστές εισαγωγές. Με την εντολή INSERT VALUES γίνονται οι εγγραφές. Στο αριστερό μέρος της *εικόνας 1.12* βρίσκονται όλοι οι πίνακες και στο δεξί μέρος οι εγγραφές του αντίστοιχου πίνακα.

```
CREATE TABLE ekthesi_skg(
antikeimeno VARCHAR(20) DEFAULT 'unknown' NOT NULL,
onomasia VARCHAR(15)NOT NULL,
hmeres_parousiashs  INT(1) DEFAULT '2' NOT NULL,
CHECK (hmeres_parousiashs>=2 AND hmeres_parousiashs<=9),
PRIMARY KEY(onomasia)
);
CREATE TABLE ekthetis(
afm CHAR(10) NOT NULL,
onoma VARCHAR(30) NOT NULL,
edra_ektheti VARCHAR(20),
typos VARCHAR(10) DEFAULT 'Etaireia' NOT NULL,
CHECK (typos='Etaireia' OR typos='Atomo'),
PRIMARY KEY(afm)
);
CREATE TABLE foreas(
afm CHAR(10) NOT NULL,
eidos VARCHAR(15) DEFAULT'Idiwths' NOT NULL,
CHECK (eidos='Idiwths'OR eidos="Kratikos'),
epwnumia VARCHAR(20),
PRIMARY KEY(afm)
);
```

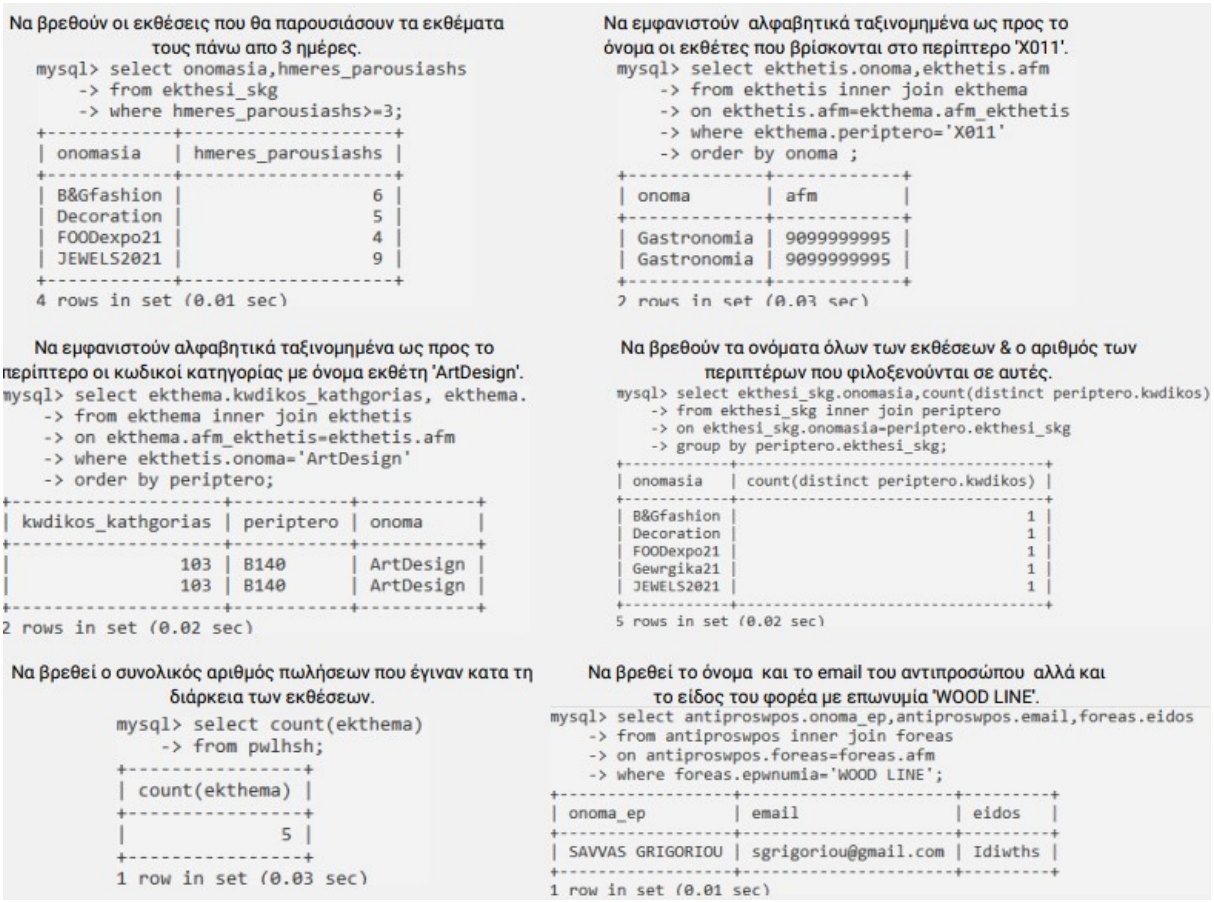
```
INSERT INTO ekthesi_skg VALUES
('food','FOODexpo21','4'),
('house','Decoration','5'),
('gewrgika','Gewrgika21', DEFAULT),
('kosmhmata','JEWELS2021','9'),
('nufika','B&Gfashion','6')
;
INSERT INTO ekthetis VALUES
('1234578908','AGROTICA','THESSALONIKI','Etaireia'),
('9874620230','Bridal Fashion','PATRA','Etaireia'),
('0419632583','ArtDesign','ATHINA','Etaireia'),
('4645552209','GEWRGIA ANASTASIOU','KRHTH','Atomo'),
('3922000003','ALEXANDRA ALEXANDROU','ATHINA','Atomo'),
('9099999995','Gastronomia','THESSALONIKI','Etaireia');
INSERT INTO foreas VALUES
('077753234','Idiwths','Woman'),
('181783239','Idiwths','CARPET'),
('995111139',DEFAULT,'Bride'),
('005111139','Idiwths','Flowers'),
('685221139','Idiwths','WOOD LINE'),
('523045697',DEFAULT,'B&G'),
('185456709',DEFAULT,'HOTELS*'),
('852789321',DEFAULT,'HOME'),
('001258936','Kratikos','NOUNOU');
```

```
CREATE TABLE antiproswpos(
foreas CHAR(10) NOT NULL,
afm_upallhlou CHAR(10),
onoma_ep VARCHAR(30),
email VARCHAR(45),
PRIMARY KEY(afm_upallhlou),
UNIQUE(email),
FOREIGN K                CES foreas(afm)
);
CREATE TABLE organosi(
ekthesi_skg VARCHAR(15) NOT NULL,
foreas CHAR(10) NOT NULL,
atoma INT,
PRIMARY KEY(ekthesi_skg,foreas),
FOREIGN KEY(ekthesi_skg) REFERENCES ekthesi_skg(onomasia
FOREIGN KEY(foreas) REFERENCES foreas(afm)
);
CREATE TABLE periptero(
ekthesi_skg VARCHAR(15) NOT NULL,
kwdikos VARCHAR(4),
thesi VARCHAR(4),
episkepseis INT,
PRIMARY KEY(kwdikos),
FOREIGN KEY(ekthesi_skg) REFERENCES ekthesi_skg(onomasia
);
CREATE TABLE ekthema(
periptero VARCHAR(4) NOT NULL,
kwdikos INT NOT NULL,
titlos_ekthematos VARCHAR(20),
afm_ekthetis CHAR(10),
kwdikos_kathgorias INT(3),
PRIMARY KEY(kwdikos),
UNIQUE (titlos_ekthematos),
FOREIGN KEY(periptero) REFERENCES periptero(kwdikos)
);
CREATE TABLE pwlhsh(
onomatepwnumo_ag VARCHAR(30) NOT NULL,
epaggelma VARCHAR(30),
afm_agorasth CHAR(10),
ekthema INT NOT NULL,
kostos DECIMAL(10,2),
PRIMARY KEY(afm_agorasth,ekthema),
FOREIGN KEY(ekthema) REFERENCES ekthema(kwdikos)
ON DELETE RESTRICT
ON UPDATE CASCADE
);
```

```
INSERT INTO antiproswpos VALUES
('077753234','102345679','ELENI KARRA','elenikarra@gmail.com'),
('181783239','201456987','KOSTAS PANAGIOTOY','kostasnapag@gmail.com'),
('995111139','407584939','GIANNIS MIXALOPOULOS','mixalopoulos@gmail.com')
('005111139','555245216','GRIGORIS ANTONIOU','gr.antoniou@gmail.com'),
('685221139','541364505','SAVVAS GRIGORIOU','sgrigoriou@gmail.com'),
('523045697','887585158','ANNA PETROU','annaperou@gmail.com'),
('185456709','529442855','SOFIA PALIOURA','spalioura@gmail.com'),
('852789321','775822103','MARIA AVGERI','avgeri@gmail.com'),
('001258936','888552552','KOSTAS LIAGAS','kliagas@gmail.com')
;
INSERT INTO organosi VALUES
('B&Gfashion','995111139','3'),
('Decoration','181783239','5'),
('FOODexpo21','001258936','8'),
('Gewrgika21','005111139','7'),
('JEWELS2021','523045697','6'),
('JEWELS2021','077753234','7'),
('Decoration','185456709','2'),
('Decoration','852789321','2'),
('Decoration','685221139','3')
;
INSERT INTO periptero VALUES
('B&Gfashion','B242','EX34','125010'),
('Decoration','B140','EX56','155360'),
('FOODexpo21','X011','EX01','220200'),
('Gewrgika21','A242','EX00','205000'),
('JEWELS2021','A302','EX90','195000')
;
INSERT INTO ekthema VALUES
('A242','1', 'Mhxanima','1234578908','111'),
('A302','2', 'Ring2','3922000003','100'),
('B140', '3','Sofa1','0419632583','103'),
('B242','4','Dress1','4645552209','222'),
('X011','5','SeaFood','9099999995','000'),
('A242','6','Exoplismos','1234578908','111'),
('A302','7','Ring1','3922000003','100'),
('B140','8','Sofa2','0419632583','103'),
('B242','9','Outfit1','4645552209','222'),
('X011','10','MEDITERRANEAN FOOD','9099999995','000')
;
INSERT INTO pwlhsh VALUES
('AGGELOS KWSTANTINOU','HOTEL','211111111','6','29000'),
('MAIRH KWSTANTINOU','OIKOS NYFIKON ','311111231','2','2000'),
('ALEKOS APOSTOLOU','IDIOKTHTHS Restaurant','400111111','10','3000'),
('MIXAHL PAPPAS','GEWRGOS','589441111','7','15000'),
                                                    '611111111','4','1000');
```

Εικόνα 1.12 Δημιουργία πινάκων στη βάση δεδομένων & οι εισαγωγές.

Εφόσον ολοκληρώθηκε η βάση, τίθενται κάποια ερωτήματα και με βάση αυτά γίνεται αντιληπτό πως όλα είναι σωστά, αλλά και ο τρόπος που λειτουργεί το JOIN που δημιουργεί προσωρινούς πίνακες που απατάνε στα ερωτήματα, όπως παρατηρείται στην *εικόνα 1.13*.



Εικόνα 1.13 Ερωτήματα.

Όλα τα ερωτήματα εξάγουν τις σωστές απαντήσεις χωρίς να υπάρχει κάποιο λάθος, συνεπώς όλες οι ενέργειες πραγματοποιήθηκαν με τον κατάλληλο ορθό τρόπο.

1.7 Ψηφιακές υπογραφές

Είναι γενικά γνωστό ότι η ύπαρξη υπογραφής σε ένα έγγραφο εξασφαλίζει την εγκυρότητα του, την αποδοχή του από τον ή τους υπογράφοντες και επισφραγίζει την δέσμευση και την τήρηση των όρων της συναλλαγής-συμφωνίας από τους συμμετέχοντες, ενώ στη περίπτωση μη τήρησης των όρων υπάρχουν νομικές συνέπειες. Επί του παρόντος, η τεχνολογία καλπάζει και για να παρέχει μια κάλυψη, εφόσον μέσω διαδικτύου γίνεται διακίνηση πληθώρας πληροφοριών και επειδή πολλές δραστηριότητες απαιτούν κάποιου είδους επιβεβαίωσης της μιας πλευράς προς στην άλλη,

δημιουργήθηκαν **οι ψηφιακές υπογραφές** *(digital signatures)* ή αλλιώς σχήματα ψηφιακών υπογραφών *(digital signature schemes)* που προσφέρουν φερεγγυότητα σε κάθε συναλλαγή, εγγύτητα σε κάθε λήψη προγράμματος ελέγχοντας αυτόματα αν οι ψηφιακές υπογραφές των προγραμμάτων είναι έγκυρες.

Οι digital signatures χρησιμοποιούν την κρυπτογραφία δημόσιου κλειδιού, έτσι διασφαλίζουν το περιεχόμενο που αποστέλλεται να παραμένει αμετάβλητο. Στηρίζονται σε τρείς βασικές αρχές στον **έλεγχο ταυτότητας** προσδιορίζοντας έτσι τον κάτοχο του ιδιωτικού κλειδιού που χρησιμοποιείται για την υπογραφή των δεδομένων, στην **ακεραιτότητα** κάνοντας χρήση αλγορίθμου κατακερματισμού διασφαλίζοντας ότι το μήνυμα θα ληφθεί και στη **μη απόρριψη** εξασφαλίζοντας ότι ο αποστολέας δεν μπορεί να αρνηθεί ότι το υπόγραψε.

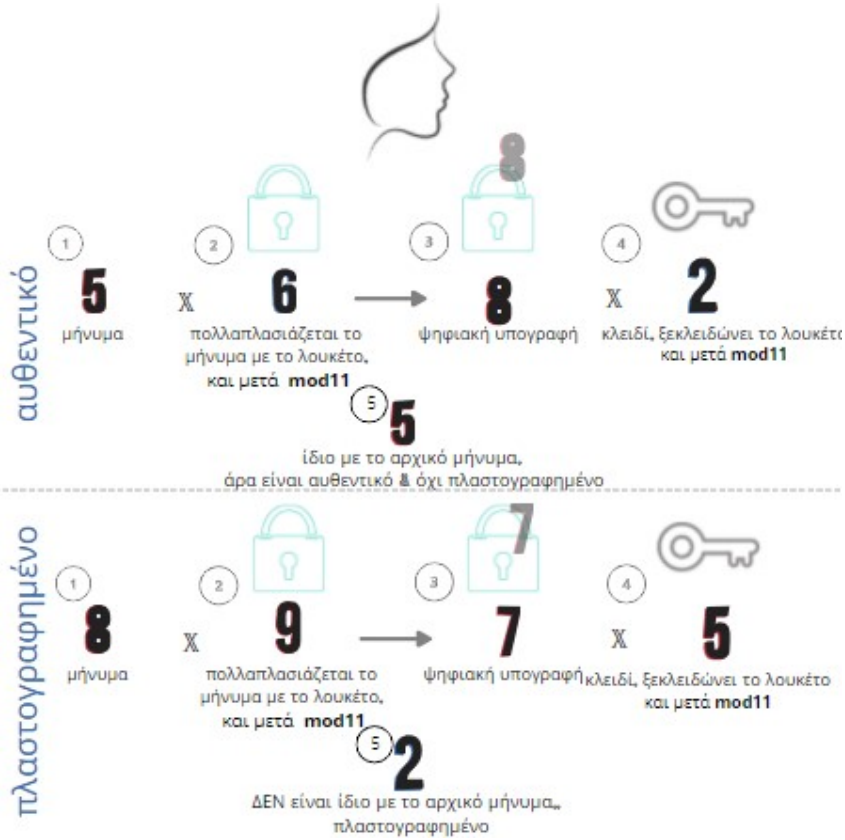
Πριν την ανάλυση για το ποια είναι η διαδικασία δημιουργίας ψηφιακών υπογραφών πρέπει να διαχωριστεί η digital signature από την e-signature. Η ψηφιακή υπογραφή αποτελεί τεχνικό όρο, αφού είναι το επακόλουθο μιας κρυπτογραφικής διαδικασίας που χρησιμοποιείται για την πιστοποίηση εγγύτητας των δεδομένων. Αντιθέτως, η ηλεκτρονική υπογραφή αποτελεί νομικό όρο. Αυτό σημαίνει ότι η digital signature μπορεί να εκφράζεται ψηφιακά σε ηλεκτρονική μορφή και να συσχετιστεί με την αναπαράσταση μιας εγγραφής. Γενικότερα η e-signature μπορεί να είναι τόσο απλή όσο το όνομα του υπογράφοντος που εισάγεται σε μια φόρμα. Οι ψηφιακές υπογραφές χρησιμοποιούν την κρυπτογραφία δημοσίου κλειδιού

Επαναφέροντας το ρολόι μεγέθους 11 και παρουσιάζεται ολοκληρωμένος ο πίνακα που χρησιμοποιήθηκε σε προηγούμενο κεφάλαιο στον πίνακα 1.2.

	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

Πίνακας 1.2 για ρολόι μεγέθους 11.

Όπως είναι γνωστό ο υπολογιστής μετατρέπει κάθε χαρακτήρα σε αριθμό γι' αυτό στο παράδειγμα που θα παρατεθεί η ψηφιακή υπογραφή θα αναπαριστάται με αριθμούς. Η κοπέλα της *εικόνας 1.14* επιθυμεί να στείλει ένα σύντομο μήνυμα, τον αριθμό 5. Αυτό θα συμβεί με την τεχνική του πολλαπλασιαστικού λουκέτου, δηλαδή χρειάζεται ένα «λουκέτο» για να διασφαλιστεί η μυστικότητα του μηνύματος και ένα κλειδί για να το ξεκλειδώσει ο αποστολέας του. Το λουκέτο ορίζεται αφότου έχει επιλεγεί το μέγεθος του ρολογιού λόγω του ότι οφείλεται να είναι μικρότερος αριθμός από το μέγεθος του ρολογιού –στην προκειμένη περίπτωση το 11- και το λουκέτο επιλέγεται να είναι ο αριθμός 6. Για να κλειδωθεί, δηλαδή ασφαλιστεί το μήνυμα, χρησιμοποιείται ο πολλαπλασιασμός και το γινόμενο *(μήνυμα*λουκέτου) mod11* θα είναι η ψηφιακή υπογραφή. Για να ξεκλειδωθεί το μήνυμα εφαρμόζεται ξανά η πράξη του πολλαπλασιασμού, δηλαδή *(ψηφιακή υπογραφή*κλειδί) mod11*. Αν προκύψει ο αριθμός 5 ο οποίος ταυτίζεται με το αρχικό το μήνυμα είναι αυθεντικό. Υπάρχει όμως και η περίπτωση που ο αποστολές ξεκλειδώνει την υπογραφή και να είναι πλαστογραφημένη μην υπάρχοντας ταύτιση με το αρχικό μήνυμα, όπως γίνεται στη δεύτερη περίπτωση της *εικόνας 1.14*.



Εικόνα 1.14 Αυθεντικό & πλαστογραφημένο με μέθοδο πολλαπλασιαστικού λουκέτου.

Τονίζεται ότι δημόσια μπορεί να ανακοινωθούν το μέγεθος του ρολογιού και το κλειδί, ενώ μυστικό πρέπει να παραμείνει το αριθμητικό λουκέτο. Για την εύρεση του κλειδιού ο υπολογιστής

βασισμένος στον αλγόριθμο του Ευκλείδη όπου βρίσκει αυτομάτως την τιμή του κλειδιού. Η μέθοδος του πολλαπλασιαστικού λουκέτου βοηθάει να προσεγγιστεί και να κατανοηθεί η σκέψη της αληθινής μεθόδου των ψηφιακών υπογραφών. Η πολλαπλασιαστική μέθοδος έχει ελαττώματα επειδή οι τιμές λουκέτων είναι γνωστές και οι τιμές λουκέτου μπορούν να υπολογιστούν με βάση τον αλγόριθμο ενώ επιβάλλεται να είναι μυστικοί, οπότε μπορούν να πλαστογραφηθούν οι ψηφιακές υπογραφές.[2]

1.7.1 RSA

Ο αλγόριθμος RSA αναφέρθηκε στην υποενότητα της κρυπτογραφίας δημόσιου κλειδιού, είναι το πρώτο και πιο διαδεδομένο δημόσιο κρυπτοσύστημα, παρέχει απόρρητο και ψηφιακή υπογραφή. Γενικά τα σχήματα ψηφιακής υπογραφής απαρτίζονται από έναν αλγόριθμο υπογραφής και έναν επαλήθευσης. Υπάρχουν δύο κύριες κατηγορίες digital signatures, οι ψηφιακές υπογραφές με παράρτημα *(digital signature schemes with appendix)* και οι ψηφιακές υπογραφές με την δυνατότητα ανάκτησης μηνύματος *(digital signature schemes with message recovery)*. Ο αλγόριθμος RSA ανήκει στη δεύτερη κατηγορία. Χρησιμοποιείται σε πολλές συναλλαγές που απαιτούν ασφάλεια στο διαδίκτυο παρέχοντας ασφαλή κρυπτογράφηση, δημιουργία ψηφιακών υπογραφών και δίνοντας την δυνατότητα για να μεταβιβάζει σύντομα κλειδιά.

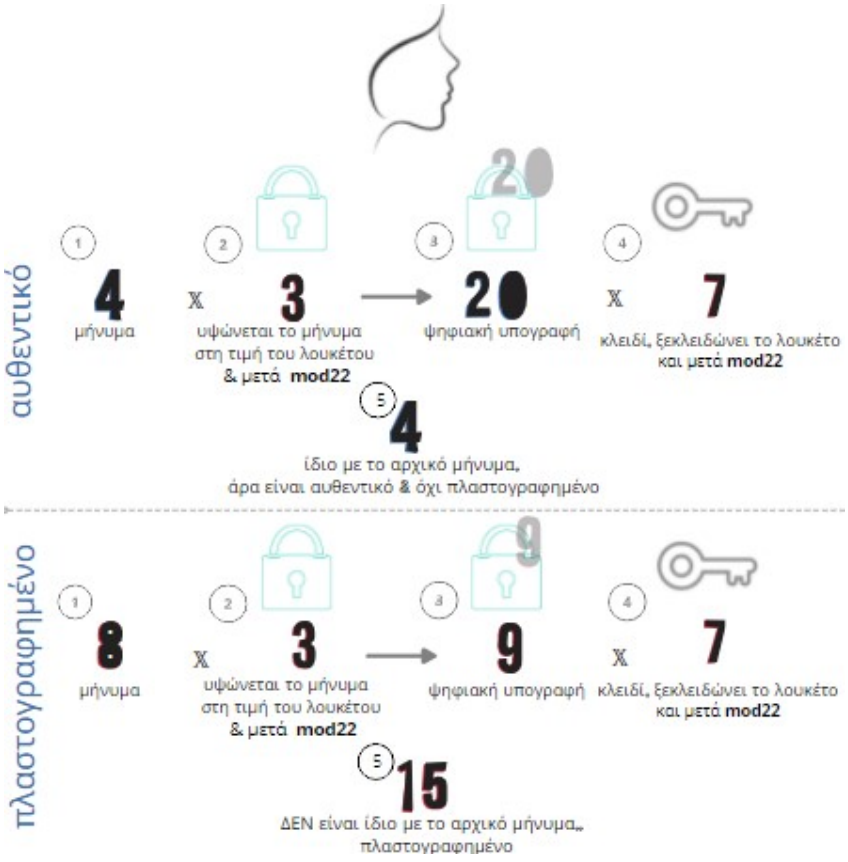
Ακολούθως παρουσιάζεται η διαδικασία δημιουργίας ψηφιακής υπογραφής με μικρούς πρώτους αριθμούς. Θα χρησιμοποιηθεί η ύψωση σε δύναμη και θα συνδυαστεί με την αριθμητική ρολογιού, όπου το ρολόι θα είναι μεγέθους 22. Στον παρακάτω πίνακα 1.3 παρουσιάζονται οι εκθέτες 3 και 7 που θα χρησιμοποιηθούν.

n	n^3	n^7
1	1	1
2	8	18
3	5	9
4	20	16
5	15	3
6	18	8
7	13	17
8	6	2
9	3	15
10	10	10
11	11	11
12	12	12
13	19	7
14	16	20
15	9	5
16	4	14
17	7	19
18	2	6
19	17	13
20	14	4

Πίνακας 1.3 με εκθέτης το 3 και το 7.

Αφού επιλεγεί και δημοσιευθεί το μέγεθος του ρολογιού, δηλαδή το 22 επιλέγεται και η μυστική τιμή λουκέτου η οποία θα είναι τιμή μικρότερη του. Ο υπολογιστής με το μέγεθος του ρολογιού και τη μυστική τιμή υπολογίζει εύκολα τη τιμή του κλειδιού. Σ' αυτή την περίπτωση, είναι απαραίτητη η μεσολάβηση μίας **έμπιστης αρχής** *(trusted third party -TTP),* η οποία συνδέει την ταυτότητα κάθε χρήστη με το εκάστοτε δημόσιο κλειδί. Με αυτόν τον τρόπο πιστοποιείται η γνησιότητα του δημοσίου κλειδιού χωρίς τη βοήθεια της TTP, αφού υπογράφει ψηφιακά ακολουθίες δεδομένων της μορφής (χρήστης, δημόσιο κλειδί του χρήστη). Η TTP υπογράφει αυτά τα δεδομένα με την προϋπόθεση ότι το δημόσιο κλειδί ανήκει όντως στον συγκεκριμένο χρήστη.[2]

Η διαδικασία που ακολουθείται για να διαπιστωθεί η αυθεντικότητα ή μη του μηνύματος βρίσκεται στην *εικόνα 1.15.* Η τιμή του μηνύματος υψώνεται στην τιμή του λουκέτου και λαμβάνοντας υπόψη το μέγεθος του ρολογιού εκτελείται η πράξη mod22 και η τιμή που προκύπτει είναι το 20, που είναι η ψηφιακή υπογραφή. Για την επαλήθευση της υψώνεται στη τιμή του κλειδιού και εφαρμόζεται το μέγεθος ρολογιού. Αν το αποτέλεσμα ταυτίζεται με το αρχικό η υπογραφή είναι αυθεντική και όχι πλαστογραφημένη. Υπογραμμίζεται ότι δεν μπορεί μέσω της γνώσης του κλειδιού και του μεγέθους του ρολογιού να υπολογιστεί η τιμή λουκέτου.



Εικόνα 1.15 Παράδειγμα αυθεντικό και πλαστογραφημένο.

Όσον αφορά την παραγωγή κλειδιού το παράδειγμα της *εικόνας 1.16* συμβάλει στην κατανόηση του. Ο χρήστης επιλέγει δύο πρώτους αριθμούς, το 11 και το 17, στην πραγματικότητα οι αριθμοί δεν είναι τόσο μικροί, αλλά απαρτίζονται από εκατό ψηφία. Έπειτα, υπολογίζεται το γινόμενο τους που είναι ίσο με 187 και το μήκος που είναι L=(11-1)(17-1)=160. Ο εκθέτης-κλειδί κρυπτογράφησης e είναι αριθμός ανάμεσα στο 1 και το L και πρέπει να είναι coprime αριθμός με τους L και N, δηλαδή σχετικά πρώτος ή πρώτος προς αλλήλους ή μεταξύ τους πρώτοι αν ο μέγιστος κοινός διαιρέτης τους είναι η μονάδα, στην συγκεκριμένη περίπτωση επιλέγεται να είναι το 3. Ο εκθέτης-κλειδί αποκρυπτογράφησης d επιλέγεται έτσι ώστε να ικανοποιείται η συνθήκη edmodL=1 -> 7*23mod160=1. Το κρυπτογραφημένο μήνυμα προκύπτει ως εξής 3^7mod187=130 και το αποκρυπτογραφημένο 130^{23}mod187=3. Είναι εμφανές ότι είναι γνήσιο αφού ταυτίζονται. Το ιδιωτικό κλειδί είναι (e,N) και το δημόσιο (d,N).

Εικόνα 1.16 Αναλυτικά η διαδικασία.

Αναλύοντας εκτενέστερα τη διαδικασία δημιουργίας ψηφιακών υπογραφών, για να αποσταλεί ένα μήνυμα χρησιμοποιείται και η κρυπτογραφική συνάρτηση κατακερματισμού *(cryptographic hash function)*. Είναι μια μαθηματική συνάρτηση που σαν έξοδο δίνει ένα καθορισμένο μέγεθος στοιχείων. Είναι σημαντικό να ειπωθεί ότι δεν γίνεται με αντιστροφή της διαδικασίας να αποκαλυφθεί το αρχικό μήνυμα -one-way function-. Η έξοδος είναι μικρότερου μήκους τους αρχικού μηνύματος και ονομάζεται σύνοψη *(message digest),* ή αποτύπωμα *(fingerprint),* ή τιμή κατακερματισμού *(hash value),* και είναι μοναδική. Μετά την σύνοψη γίνεται η κρυπτογράφηση με το ιδιωτικό κλειδί και κατάλληλο μυστικό αλγόριθμο υπογραφής και δημιουργείται η ψηφιακή υπογραφή. Είναι σημαντικό να ειπωθεί ότι οποιαδήποτε αλλαγή συμβεί σημαίνει και αλλαγή στη σύνοψη. Είναι προτιμότερο οι κρυπτογραφικές διαδικασίες να εφαρμόζονται στη σύνοψη του μηνύματος για να υπάρχει καλύτερη διαχείριση χώρου και χρόνου, αφού είναι πιο μικρή και πιο εύκολη στη διαχείριση. Συνεπώς, ενισχύεται η αποδοτικότητα των αλγόριθμων υπογραφής και επαλήθευσης και διαφυλάσσεται η ακεραιότητα των δεδομένων. Τέλος, οι hash συναρτήσεις αποτελούν μια αξιόπιστη λύση έναντι των πλαστογραφήσεων.

1.8 Συμπεράσματα κεφαλαίου

Οι μηχανές αναζήτησης για να εξασφαλίσουν στους περιηγητές τον εντοπισμό της καταλληλότερης απάντησης, μετά την ιστοαναζήτηση, συνδυάζουν αρκετές διεργασίες την ανίχνευση, την ευρετηρίαση, τον εντοπισμό και την κατάταξη.

Ο PageRank είναι ο λόγος εκτόξευσης της Google ως την κυρίαρχη μηχανή αναζήτησης. Όσο υψηλότερο είναι το PageRank τόσο υψηλός και ο βαθμός σημαντικότητας της ιστοσελίδας. Η

σημαντικότητα της εκάστοτε web page εξαρτάται από την ποιότητα και την ποσότητα των εισερχόμενων συνδέσμων Το ποσοστό του Webspam μειώνεται σημαντικά με την συνεισφορά της AI.

Η κρυπτογραφία δημόσιου κλειδιού που χρησιμοποιεί δυο κλειδιά και η μυστικότητα του μηνύματος εξαρτάται από το μέγεθος του κλειδιού και στηρίζεται στο πρωτόκολλο Diffie-Hellman. Τα θετικά σ' αυτό το είδος κρυπτογραφίας είναι ότι επιτρέπει και στις δύο πλευρές να διεξάγουν ασφαλές ανταλλαγές πληροφοριών χωρίς να έχουν προσυμφωνήσει κάποιο κρυφό κλειδί. Το αρνητικό βρίσκεται στο ότι οι αλγόριθμοι δημοσίου κλειδιού είναι λιγότερο αποτελεσματικοί με μεγάλο μήκος κλειδιού. Επίσης συγκριτικά με την συμμετρική κρυπτογραφία είναι πιο αργή και χρησιμοποιεί περισσότερους υπολογιστικούς πόρους.

Οι κώδικες σφαλμάτων χωρίζονται σε δύο κατηγορίες στους κώδικες τμήματος και στους συνδυαστικούς κώδικες. Στην πρώτη κατηγορία συγκαταλέγεται ο Hamming (7,4) που αποτελεί τον πρώτο αποτελεσματικό κώδικα εντοπισμού και διόρθωσης σφαλμάτων. Μέθοδος εντοπισμού λάθους είναι η πλεονασματικότητα, δηλαδή μαζί με το μήνυμα να στέλνεται και κάτι επιπλέον ώστε να εντοπίζεται εύκολα η εκάστοτε αλλοίωση.

Η συμπίεση δεδομένων χρησιμοποιείται για παροχή ταχύτερων αποστολών και λήψεων δεδομένων μέσω διαδικτύου με προϋπόθεση η ποιότητα τους να παραμένει αμετάβλητη καταλαμβάνοντας λιγότερο αποθηκευτικό χώρο. Χρησιμοποιείται και παρασκηνιακά χωρίς ο χρήστης να το αντιλαμβάνεται. Χωρίζεται σε απωλεστική και μη απωλεστική. Πλέον χρησιμοποιείται ιδιαίτερα η μέθοδος JPEG για τις εικόνες, το MP3 για την συμπίεση ηχητικών και το MPEG για συμπίεση βίντεο.

Οι βάσεις δεδομένων προσφέρουν οργάνωση, γρήγορο και εύκολο χειρισμό. Είναι αποδοτικές και αξιόπιστες. Η DBMS αλληλεπιδρά με τους τελικού χρήστες και στη DB πραγματοποιείται διαγραφή, εισαγωγή και επεξεργασία των δεδομένων. Η δοσοληψία εκτελείται με βάση την WAL. Το πρωτόκολλο οριστικοποίησης 2 φάσεων συμβάλει στο ζήτημα της ανάκλασης.

Οι ψηφιακές υπογραφές προσφέρουν εγκυρότητα, φερεγγυότητα, διασφαλίζοντας το περιεχόμενο τους στις διαδικτυακές συναλλαγές. Ο RSA είναι το πιο διαδεδομένο δημόσιο σχήμα υπογραφής. Χρησιμοποιεί κρυπτογραφία δημόσιου κλειδιού. Επίσης, χρησιμοποιεί την τεχνική του πολλαπλασιαστικού λουκέτου για την επισφράγιση μυστικότητας. Η έμπιστη αρχή (TTP) συνδέει την ταυτότητα του χρήστη με το κλειδί που του αντιστοιχεί.

2 ΚΕΦΑΛΑΙΟ 2ο: Αναγνώριση προτύπων

Η **τεχνητή νοημοσύνη** *(artificial intelligence-AI)* είναι πιθανόν η πιο αντιπροσωπευτική τεχνολογία των τελευταίων ετών και σίγουρα των ερχόμενων. Η συμβολή της στο πεδίο της επιστήμης έχει βελτιώσει τομείς της καθημερινότητας. Συγκεκριμένα αντιγράφει την ανθρώπινη φύση, αφού ασχολείται με την αναπαραγωγή γνωστικών λειτουργιών του ανθρώπινου εγκεφάλου. Έτσι, η AI περιλαμβάνει μηχανές που τεχνητά αντικατοπτρίζουν την ανθρώπινη νοημοσύνη και βοηθούν στην διαχείριση και στην μοντελοποίηση πολύπλοκων συστημάτων. Τα υπολογιστικά συστήματα, με την συμβολή της artificial intelligence, λαμβάνοντας δεδομένα -από κάμερες, αισθητήρες- τα επεξεργάζονται και εκτελούν εργασίες βάσει αυτών. Η AI βοηθάει συνεπώς τα υπολογιστικά συστήματα να κατανοήσουν το περιβάλλον τους λαμβάνοντας δράση, ως ένα βαθμό αυτονομίας, προς επίτευξη του εκάστοτε στόχου.

Υποσύνολο της τεχνητής νοημοσύνης είναι η **μηχανική μάθηση** (*machine learning*), είναι ουσιαστικά ένα δομικό στοιχείο για την τεχνητή νοημοσύνη. Με τη μηχανική εκμάθηση, διδάσκετε μια μηχανή για να μάθει την διαδικασία εκτέλεσης μιας εργασίας, αφορά δηλαδή την μελέτη αλγόριθμων οι οποίοι βελτιώνονται αυτόματα μέσω εμπειρίας με αποτέλεσμα να αυτοματοποιούν τους κανόνες δημιουργίας αντλώντας στοιχεία από τα εκπαιδευτικά δεδομένα που έχουν δοθεί στο δίκτυο. Μερικοί τύποι αλγορίθμων μηχανικής μάθησης είναι τα *Dicision Trees, Linear Regression, Support Vector Machines*. Η ουσία της συνοψίζεται στη χρήση αλγορίθμων που μπορούν και αναγνωρίζουν διαφορετικά πρότυπα και λαμβάνουν τις ορθές αποφάσεις σε συνεργασία με την βελτιστοποίηση, την στατιστική και τη θεωρία των πιθανοτήτων.

Υποσύνολο την μηχανικής μάθησης είναι η **βαθιά μάθηση** (*deep lerning)* που είναι μορφή machine learning που μιμείται την λειτουργία του ανθρώπινου εγκεφάλου. Υλοποιεί ένα τεχνητό νευρικό δίκτυο (ANN), το οποίο έχει πολλαπλά επίπεδα επιτρέποντας έτσι την επεξεργασία κάθε βαθμού δυσκολίας που πραγματοποιείται μεταξύ της εισόδου και της εξόδου. Εκεί ανήκει και η **αναγνώριση προτύπων** *(pattern recognition)*.

Όλα τα επίπεδα συνδέονται με την επιστήμη δεδομένων *(data science)* η οποία είναι υπεύθυνη για την διαχείριση πολλών δεδομένων περιλαμβάνοντας τον καθορισμό, την προετοιμασία, την ανάλυση και όλα αυτά γίνονται με μαθηματικές εφαρμογές όπως η στατιστική και η γραμμική άλγεβρα. Ενσωματώνει όλους τους παραπάνω όρους για να εξαγάγει πληροφορίες από τα δεδομένα και να είναι ικανό να κάνει προβλέψεις. Στην *εικόνα 2.1* απεικονίζεται η σύνδεση των παραπάνω όρων.

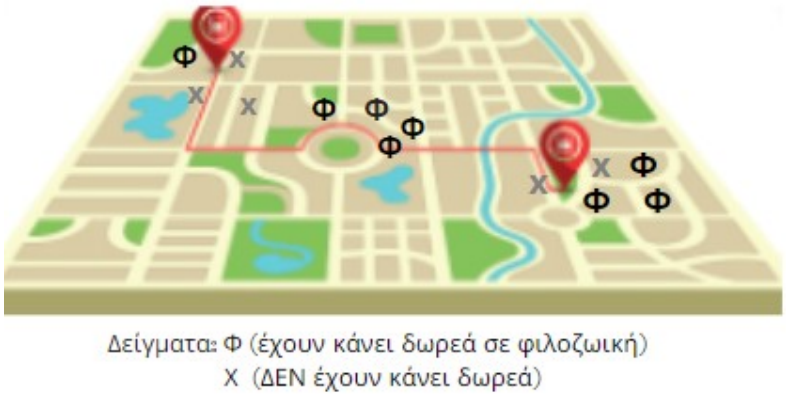
Εικόνα 2.1 Τεχνητή νοημοσύνη και τα υποσύνολά της.

Στην αναγνώριση προτύπων συμπεριλαμβάνεται η ανάγνωση κειμένων, αντικειμένων, προσώπων, φωνής. Οι υπολογιστές εκπαιδεύονται κατάλληλα μέσω τροφοδότησης δειγμάτων να αναγνωρίζουν πρότυπα ώστε στην πορεία όταν υπάρξει η εισαγωγή νέων δειγμάτων να τα κατατάσσουν στις κλάσεις που ανήκουν μέσω των αλγορίθμων ταξινόμησης. Οι άνθρωποι μέσω εκπαίδευσης και βιωματικής μάθησης είναι σε θέση να αναγνωρίζουν γρήγορα κάθε πρότυπο είτε χειρόγραφο χαρακτήρα είτε πρόσωπο είτε αντικείμενο.

Με αυτόν τον τρόπο εκπαιδεύεται το σύστημα και μπορεί να λάβει νέα δεδομένα χωρίς να χρειάζεται πλέον η επιγραφή -δηλαδή η κλάση-, τα προσδιορίζει συγκρίνοντας τα με τα ήδη ταξινομημένα, και καταλλήλως τα τοποθετεί στην κλάση που τους ταιριάζει.

2.1 Τέχνασμα πλησιέστερου γείτονα

Το τέχνασμα του **πλησιέστερου γείτονα** *(nearest neighbor)* αποτελεί μία τεχνική ταξινόμησης. Επί παραδείγματι, σε μία γειτονία των Αθηνών θα γίνει πρόβλεψη για το αν οι κάτοικοι πρόκειται να δωρίσουν χρήματα σε φιλοζωική εταιρεία βασισμένο σε μια υποθετική καταγραφή που είχε γίνει στην ίδια γειτονία πριν από πέντε έτη. Ακολούθως στην *εικόνα 2.2* εμφανίζεται το υποθετικό πρότυπο κατοίκων που προσέφεραν οικονομική ενίσχυση σε φιλοζωικές. Με ‘Φ’ δηλώνονται οι κάτοικοι που έχουν δωρίσει χρήματα, ενώ με ‘Χ’ η μη δωρεά. Το ‘Φ’ και το ‘Χ’ είναι τα δείγματα και οι κλάσεις, τα οποία αποτελούν και τα εκπαιδευτικά δεδομένα για την πρόβλεψη που θα πραγματοποιηθεί.



Εικόνα 2.2 Εκπαιδευτικά δεδομένα για μελλοντική πρόβλεψη χορήγησης ή μη σε φιλοζωικές.

Εφόσον δοθήκαν τα εκπαιδευτικά δεδομένα, προστίθενται νέα δείγματα, που δηλώνονται με ερωτηματικό στην *εικόνα 2.3* και πρέπει να ταξινομηθούν με χρήση του τεχνάσματος του πλησιέστερου γείτονα.

Εικόνα 2.3 Εφαρμογή τεχνάσματος πλησιέστερου γείτονα.

Για να παρθεί απόφαση σε ποια κλάση ανήκουν τα καινούργια δείγματα της *εικόνας 2.3* βρίσκεται ο πλησιέστερος γείτονας του ζητούμενου δείγματος και έπειτα χρησιμοποιείται ως πρόβλεψη σε ποια κλάση ανήκει το νέο δείγμα. Αυτή η μέθοδος χρησιμοποιείται για το ερωτηματικό κόκκινου χρώματος. Μια πιο σύγχρονη μορφή της τεχνικής αυτή είναι η οι ***K-***

πλησιέστεροι γείτονες. Το *K* λαμβάνει μικρές τιμές, παραδείγματος χάρη τον αριθμό 3, και το δείγμα λαμβάνει την κλάση στην οποία θα ανήκει ανάλογα με τους *K* γείτονες που εμφανίζονται πλειοψηφικά γύρω του. Ανάλογα με το πρόβλημα επιλέγεται και η τιμή του *K*. Αυτή η τεχνική χρησιμοποιείται στο ερωτηματικό κίτρινου χρώματος. Μπορεί εύκολα να ειπωθεί ότι οι προβλέψεις, που αφορούν τα νέα δείγματα, γίνονται με βάση την απόσταση που έχουν από τα ήδη υπάρχοντα. Πρέπει να τονιστεί, ότι η εργασία ταξινόμησης είναι αδύνατον να γίνει με απόλυτη ακρίβεια, αλλά ο στόχος είναι η εκπαίδευση του συστήματος για πρόβλεψη αναλύοντας τις θέσεις των δειγμάτων συγκριτικά με τις προτιμήσεις των κατοίκων.

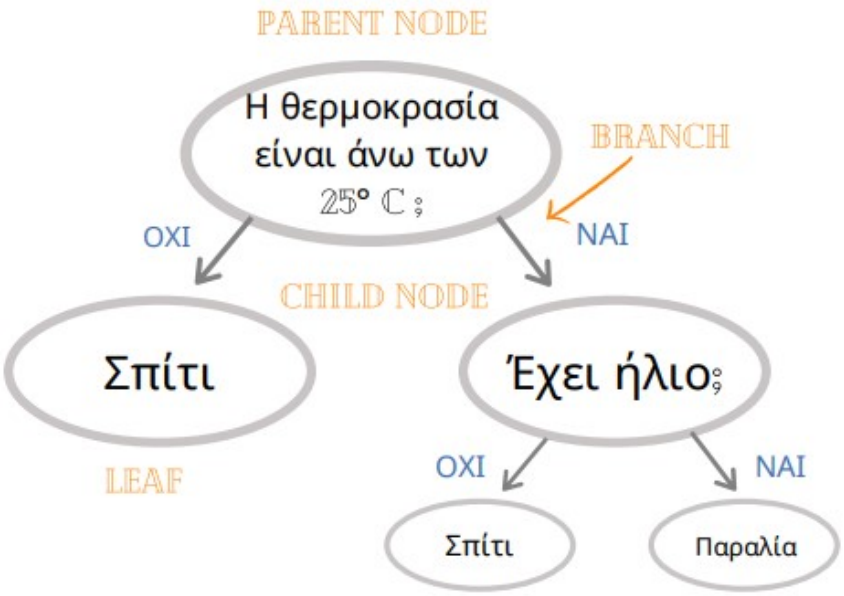
Η ταξινόμηση του πλησιέστερου γείτονα εφαρμόζεται και στην εύρεση διαφοράς ή ταύτισης χειρόγραφων ψηφίων συμβόλων. Η διαφορά εκφράζεται σαν ποσοστό. Το μικρό ποσοστό εκφράζει ότι είναι κοντινοί γείτονες, δηλαδή την ομοιότητα τους, ενώ το μεγάλο ποσοστό εκφράζει τη διαφορά των χαρακτήρων. Όσο το ποσοστό να είναι όσο μικρότερο για να ανήκουν τα δεδομένα στην ίδια κλάση.

2.2 Δέντρα αποφάσεων

Τα **δέντρα αποφάσεων** *(decision trees)* αποτελούν είδος προγνωστικών μοντέλων και μέρος της μηχανικής μάθησης. Χρησιμοποιούνται για ταξινόμηση και εκφράζονται ως αναδρομική διχοτόμηση του χώρου γεγονότων. Είναι επιθυμητά λόγω της απλότητας και της διαφάνειας που προσφέρουν. Κάθε δέντρο απαρτίζεται από τη ρίζα *(root/parent node),* στην οποία δεν εισέρχεται καμία εισερχόμενη ακμή. Οι κόμβοι έχουν ακριβώς μια εισερχόμενη ακμή, χωρίζονται στους εσωτερικούς (*children nodes),* δηλαδή εκείνους που έχουν εξερχόμενη άκρη και στους τερματικούς ή αλλιώς φύλλα *(leaves).* Κάθε κόμβος αντιστοιχίζεται σε ένα συγκεκριμένο χαρακτηριστικό και κάθε εσωτερικός κόμβος διαιρεί τις καταστάσεις σε μια ή περισσότερες. Τα φύλλα υποδεικνύουν μια κατηγορία που αναπαριστά την επιθυμητή αξία του στόχου. Υπογραμμίζεται, ότι κάθε διαδρομή *(branch)* από τη ρίζα προς τα φύλλα είναι ένας κανόνας που δημιουργείται εφόσον συνενωθούν όλα τα χαρακτηριστικά.

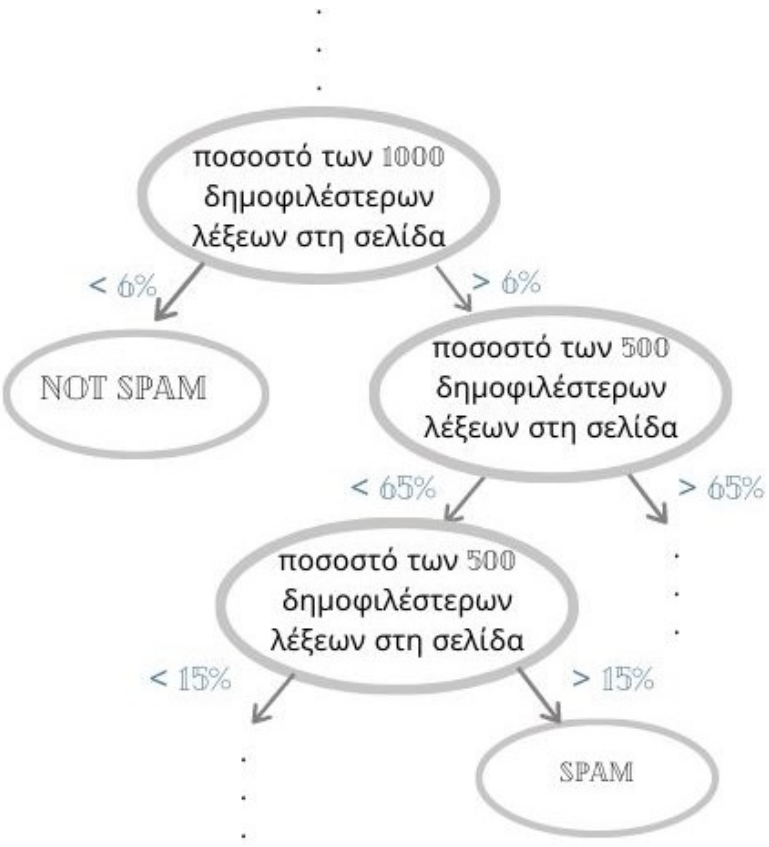
Μέσω των δέντρων απόφασης και με επαρκή εκπαιδευτικά δεδομένα μπορεί να κατασκευάσει μέσω μάθησης ένα δέντρο αποφάσεων που θα εκτελεί ακριβείς ταξινομήσεις. Η φάση μάθησης είναι αυτόματη και χρειάζεται να γίνει μόνο μία φορά, κάνοντας την μέθοδο ταξινόμησης να φαίνεται μια διασκεδαστική διαδικασία.

Στην *εικόνα 2.4* έχει δημιουργηθεί δέντρο απόφασης το οποίο εξάγει την ιδανική απόφαση για το αν είναι κατάλληλο κάποιος να πάει στην παραλία για κολύμπι ή όχι μέσω εύστοχων ερωτημάτων.



Εικόνα 2.4 Δέντρο απόφασης.

Επιπροσθέτως τα δέντρα απόφασης χρησιμοποιούνται και για την καταπολέμηση της ιστορύπανσης *(web spam)*, που παρουσιάστηκε στην *υποενότητα 1.2 PageRank*, επιλύοντας την κατά 90%. Η ιστορύπανση συμβαίνει όταν οι κάτοχοι των ιστοσελίδων θέλουν να βελτιώσουν την κατάταξη της σελίδας τους χρησιμοποιώντας δημοφιλείς όρους, χωρίς ουσιαστικά να παρέχουν καμία χρήσιμη πληροφορία. Με τα decision trees καταβάλλεται μεγάλη προσπάθεια για επίλυση τέτοιων φαινομένων. Το web spam αναγνωρίζεται από την τοποθέτηση πολλών άσχετων μεταξύ τους λέξεων κλειδιών και συνδέσμων. Επίσης, από την επιλογή λέξεων κλειδί στη διεύθυνση URL και από την ένταξη απόκρυφου κειμένου το οποίο γράφεται στο ίδιο χρώμα με το φόντο της σελίδας. Μέρος του δέντρο απόφασης για την καταπολέμηση ιστορύπανσης παρουσιάζεται την *εικόνα 2.5*.



Εικόνα 2.5 Μέρος δέντρου απόφασης Webspam.

Τα δέντρα απόφασης που δημιουργούνται για να καταπολεμήσουν την ιστορύπανση επικεντρώνονται συνήθως στο ποσοστό δημοφιλίας των λέξεων. Αν το ποσοστό είναι μικρό η ιστοσελίδα δεν αποτελεί δείγμα web spam, ενώ αν είναι μεγάλο θεωρείται ότι είναι φαινόμενο ιστορύπανσης.

Η διαδικασία που ακολουθείται για την οποιαδήποτε διαδικασία δημιουργίας δέντρων απόφασης είναι η διατύπωση ορθών και αποδοτικών ερωτήσεων για να δίνεται η καταλληλότερη απάντηση στην εκάστοτε ερώτηση. Οι ερωτήσεις σταματούν όταν ο υπολογιστής δε θα δημιουργεί ερωτήσεις. Η διαδικασία αυτή εκτελείται μια φορά και μετά είναι σε θέση να χρησιμοποιηθεί και σε οποιαδήποτε σχετιζόμενη περίπτωση για υπολογιστικά μοντέλα αφού έχουν εκπαιδευτεί στο να «κατανοούν» και να διαχωρίζουν συγκεκριμένα πρότυπα και έπειτα να τα ταξινομούν τα καινούργια.

2.3 Τεχνητά νευρωνικά δίκτυα

Τα **τεχνητά νευρωνικά δίκτυα** *(artificial neural networks)* διερευνήθηκαν από τον Alan Turing, που ήταν από τους πρώτους που ασχολήθηκαν με αυτόν τον τομέα. Ο ίδιος υποστήριζε ότι θα μπορούσε να δημιουργήσει προσομοίωση του ανθρώπινου εγκεφάλου μέσω υπολογιστή, με την διαφορά όμως ότι δεν είχε αντιληφθεί πλήρως την δυσκολία αυτού του εγχειρήματος. Λόγω αυτής

της προσπάθειας δημιουργήθηκαν τα νευρωνικά δίκτυα. Τα artificial neural networks είναι συστήματα επεξεργασίας δεδομένων μεγάλης υπολογιστικής ικανότητας. Είναι αποτέλεσμα σύνδεσης των τεχνητών νευρώνων, οι οποίοι είναι δημιουργημένοι σε δομές παρόμοιες με εκείνες του ανθρώπινου εγκεφάλου, αφού η διαδικασία της μάθησης τους είναι εμπνευσμένη από τον τρόπο μάθησης που έχουν οι άνθρωποι -αλλά και τα ζώα- κατά την διάρκεια προσαρμογής και εξερεύνησης του περιβάλλοντος τους. Τονίζεται ότι οι τεχνητοί νευρώνες λειτουργούν σε παράλληλη διάταξη.

Η τεχνητή νοημοσύνη και τα νευρωνικά δίκτυα έχουν απογειώσει τον κλάδο της επιστήμης των υπολογιστών και της πληροφορίας. Τα **τεχνητά νευρωνικά δίκτυα** *(artificial neural network, ANNs)* αντιγράφουν τους νευρώνες που συναντώνται στον ανθρώπινο εγκέφαλο. Πρόκειται για δίκτυα που είναι αλγοριθμικά κατασκευασμένα και εστιάζουν στην εύρεση λύσης του εκάστοτε υπολογιστικού ζητήματος. Μιμούνται με τον καλύτερο δυνατό τρόπο τα βιολογικά νευρωνικά δίκτυα. Οι εγκέφαλοι αποτελούνται από κύτταρα, τους λεγόμενους νευρώνες, ο κάθε νευρώνας συνδέεται με πολλούς επιπλέον. Μέσω της σύνδεσης τους στέλνουν ηλεκτροχημικά σήματα, κάποιες συνδέσεις λαμβάνουν ερεθίσματα και άλλες στέλνουν. Για το αν θα στείλουν ερεθίσματα εξαρτάται από την ισχύ των εισερχόμενων νευρώνων, δηλαδή αθροίζονται όλα τα σήματα που δέχεται και αν είναι αρκετά μεγάλο το άθροισμα στέλνεται το ερέθισμα. Υπάρχουν δύο είδη εισερχόμενων σημάτων τα ανασταλτικά και τα διεγερτικά. Στα διεγερτικά αθροίζεται κάθε φορά η ισχύς, ενώ στα ανασταλτικά αφαιρείται.

Το ακόλουθο παράδειγμα θα οδηγήσει στην κατανόηση της λειτουργίας. Συγκεκριμένα θα παρουσιαστεί ένα νευρωνικό δίκτυο για το θέμα που τέθηκε στην *εικόνα 2.4* σχετικά με το ποια είναι κατάλληλη η απάντηση όταν τίθεται το ερώτημα αν μπορεί να πάει κάποιος παραλία για κολύμπι. Το νευρωνικό δίκτυο εμφανίζεται στην *εικόνα 2.6*.

Εικόνα 2.6 Νευρωνικό δίκτυο.

Κάθε νευρώνας θα προσδιορίζεται από έναν αριθμό, το λεγόμενο κατώφλι. Όταν θα βρίσκεται σε λειτουργία ο νευρώνας θα αθροίζει τα ερεθίσματα που δέχεται και αν ο αριθμός είναι ίσος με το κατώφλι, τότε θα υπάρχει ενεργοποίηση του νευρώνα διαφορετικά θα βρίσκεται σε αδράνεια. Στο παράδειγμα της *εικόνας 2.7* και οι τρείς νευρώνες είναι διεγερτικοί. Η κάθε είσοδος μεταδίδει σήμα με ισχύ +1 αν η συνθήκη που περιγράφεται είναι αληθής, αλλιώς δε αποστέλλεται τίποτα.

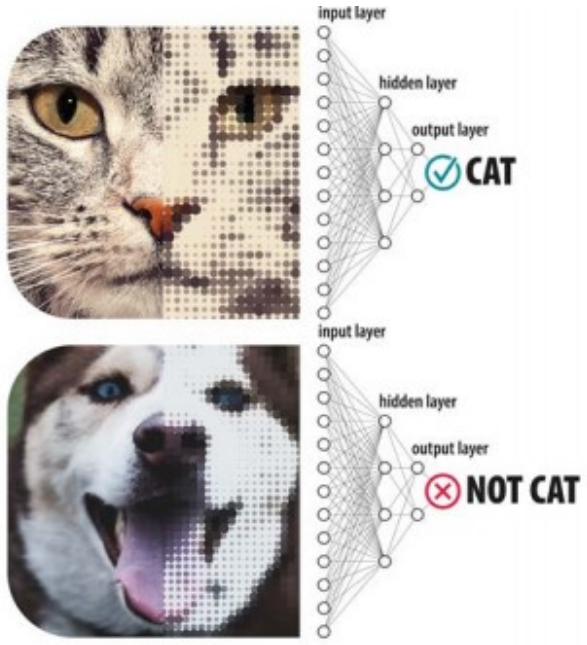
Εικόνα 2.7 Νευρωνικό δίκτυο αποτελέσματα.

Τα ANNs εμπνέονται από τη λειτουργικότητα του ηλεκτροχημικών νευρωνικών δικτύων που βρίσκονται σε ανθρώπινους –και ζωικούς- εγκεφάλους μεταδίδοντας σήματα μέσω ενός σύνθετου

δικτύου νευρώνων. Με αυτόν τον τρόπο τόσο η δομή του όσο και τα σήματα που δέχεται σε κάθε περίπτωση παρουσιάζονται στην *εικόνας 2.7*.

Τα δεδομένα εισόδου λοιπόν είναι εκείνα που μεταφράζονται σε σήματα και είναι υπεύθυνα για τα αποτελέσματα που παράγονται. Στα τεχνητά νευρωνικά δίκτυα υπάρχουν διάφορα επίπεδα ανάμεσα στην είσοδο και στη έξοδο, υπάρχουν ενδιάμεσα επίπεδα ανάλογα με τον όγκο δεδομένων τα οποία μπορεί να είναι ένα ή περισσότερα. Όσο περισσότερα είναι τα επίπεδα τόσο πιο διεξοδική ανάλυση εκτελούν τα ANNs, αφού υποδιαιρούν κάθε ζήτημα που προκύπτει ώστε να ληφθεί η πιο εύστοχη απάντηση.

Στην περίπτωση της *εικόνα 2.8* που ακολουθεί το ANNs θα μαντεύει αν πρόκειται για γάτα. Αρχικά, η εικόνα χωρίζεται σε εικονοστοιχεία *(pixels)* και στέλνονται στους νευρώνες της εισόδου. Έπειτα, οδηγούνται ως σήμα στο πρώτο κρυφό επίπεδο. Κάθε νευρώνας στο κρυφό επίπεδο λαμβάνει πολλαπλά σήματα τα οποία αθροίζονται και είναι υπεύθυνα για την αναπαραγωγή του εξωτερικού σήματος.



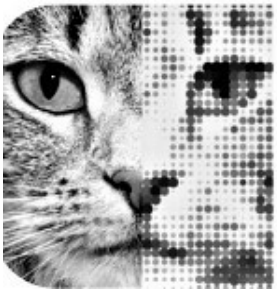
Εικόνα 2.8 Πηγή:Philip Boucher,Artificial intelligence: How does it work, why does it matter, and what can we do about it?

Στην *εικόνα 2.8* εμφανίζεται μόνο ένα κρυμμένο επίπεδο, διότι το διάγραμμα είναι σχηματικό. Στο αριστερό μέρος της εικόνας εμφανίζεται το περίπλοκο μέρος, επειδή εκεί βρίσκονται οι συνδέσεις από την εικόνα εισόδου προς τους κεντρικούς νευρώνες. Τα ANNs δεν είναι σε θέση να γνωρίζουν τι είναι γάτα, αλλά μέσω της εκπαίδευσης και της τροφοδότηση παραδειγμάτων -από φωτογραφίες που απεικονίζουν γάτες- μπορεί να αποφανθεί την παρουσία ή μη γάτας. Για την ορθή παραγωγή αποτελεσμάτων πρώτο βήμα είναι η δημιουργία δομής και μετά ως δεύτερο στάδιο

έρχεται η εκπαίδευση. Θεωρητικά θα μπορούσε να γίνει από έναν έμπειρο επιστήμονα με το χέρι, ο οποίος θα προσάρμοζε καταλλήλως τους νευρώνες ώστε να αντικατοπτρίζουν τους δική του εμπειρία για τον τρόπο ταυτοποίησης των γάτων. Αντ' αυτού, λόγω των πολύπλοκων συνδέσεων των νευρώνων εφαρμόζεται ένας αλγόριθμος ML *(machine learning)* για την αυτοματοποίηση της διαδικασίας. Τέλος, υπογραμμίζεται ότι η δομή του εκάστοτε νευρωνικού δικτύου διαφέρει, καθώς η επιλογή της δομής του εξαρτάται από την πρότερη εμπειρία, την διορατικότητα και την διαισθητικότητα του επαγγελματία. [26]

Αναφερόμενοι στην πιο καταξιωμένη μηχανή αναζήτησης, την Google, οι ταξινομητές εικόνων της χρησιμοποιούν έως και 30 κρυμμένα στρώματα. Τα πρώτα στρώματα αναζητούν γραμμές που μπορούν να αναγνωριστούν ως άκρες ή γωνίες, τα μεσαία στρώματα εντοπίζουν σχήματα σε αυτές τις γραμμές και τα τελικά στρώματα συνδέουν αυτά τα σχήματα για να ερμηνεύσουν την εικόνα.[26]

Εμβαθύνοντας τον τομέα της τεχνητής νοημοσύνης θα αναφερθούν κάποιες επιπλέον λεπτομέρειες που αντικατοπτρίζουν την πραγματική λειτουργία. Αρχικά πρέπει να διατυπωθεί ότι μέρος της *εικόνας 2.9* μετατρέπεται σε ασπρόμαυρη για λόγους απλοποίησης.

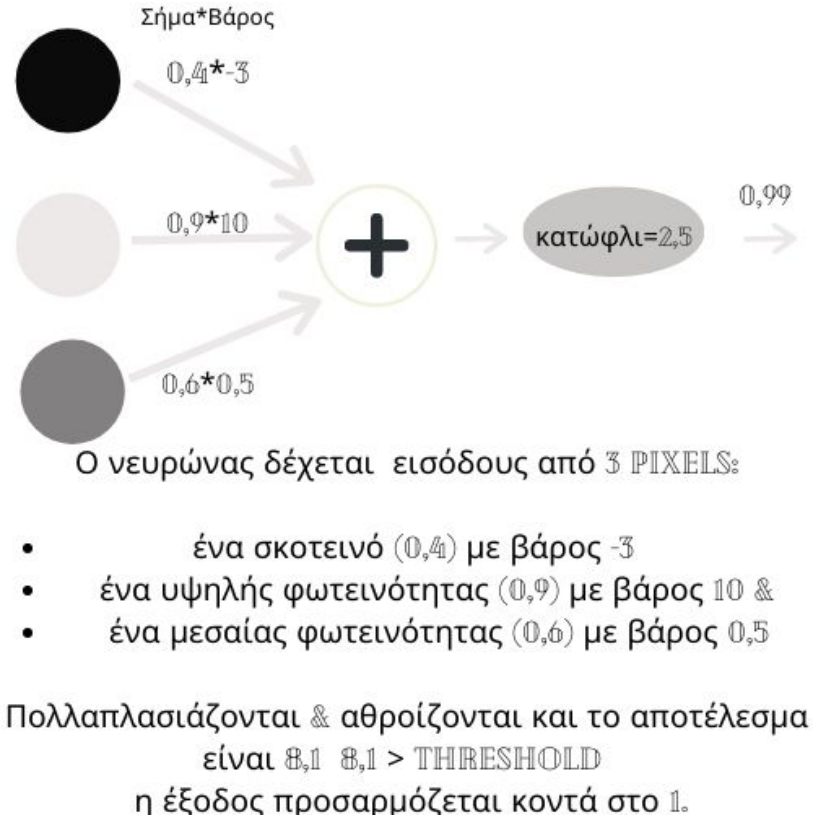


Εικόνα 2.9 Ασπρόμαυρη. Πηγή: Philip Boucher, Artificial intelligence: How does it work, why does it matter, and what can we do about it?

Σε σχέση με την *εικόνα 2.8* εδώ τα σήματα μπορούν να λάβουν και ενδιάμεσες τιμές μεταξύ του 0 και του 1. Με τιμή 1 χαρακτηρίζονται τα pixels που είναι λευκά, με 0 τα μαύρα και οι υπόλοιπες ενδιάμεσες τιμές δηλώνουν τις διάφορες αποχρώσεις του γκρι. Τη θέση της ισχύς πλέον παίρνουν τα **βάρη** *(weight).* Η συνολική τιμή της εισόδου προκύπτει μετά την άθροιση των βαρών. Το βάρος μπορεί να έχει αρνητική ή θετική τιμή. Τα θετικά βάρη αναπαριστούν διεγερτικά σήματα, ενώ τα αρνητικά ανασταλτικές συνδέσεις. Οι συνδέσεις με μικρά βάρη επηρεάζουν ελάχιστα το αν θα υπάρξει ή όχι ενεργοποίηση νευρώνων, αντιστοίχως τα μεγάλα βάρη που δηλώνουν ισχυρές συνδέσεις μπορούν να καθορίσουν το αποτέλεσμα.

Ο νευρώνας υπολογίζει το σύνολο των εισόδων πολλαπλασιάζοντας με το βάρος της σύνδεσης πριν αθροιστεί στο σύνολο. Όσον αφορά το κατώφλι η επίδραση του είναι πιο ήπια. Το κατώφλι δεν αναγκάζει την έξοδο να πάρει τιμές μόνο το 0 και το 1 αλλά δίνεται η δυνατότητα να ληφθούν

και ενδιάμεσες τιμές. Στην περίπτωση που η συνολική είσοδος είναι μικρότερη από το κατώφλι τότε παίρνει τιμές κοντά στο 0, ενώ όταν είναι μεγαλύτερη από το κατώφλι λαμβάνει τιμές κοντά στο 1.Όταν η συνολική είσοδος πάρει τιμές κοντά στο κατώφλι λαμβάνει τιμή περίπου ίση με 0,5. Συνεπώς, οι τιμές στην διαπίστωση απεικόνισης γάτας είναι τιμές εξόδου κοντά στο 1, σε περίπτωση που οι τιμές εξόδου είναι κοντά στο μηδέν αποτελούν ένδειξη μη απεικόνισης γάτας. Οι πληροφορίες που δίνονται από τον άνθρωπο είναι τα εκπαιδευτικά δεδομένα, πληθώρα εικόνων καταταγμένες στην κλάση τους αναγράφοντας αν δείχνουν γάτα ή όχι. Με την επαναλαμβανόμενη προσαρμογή των βαρών κατά τη φάση μάθησης προκύπτει και η απάντηση ύπαρξης της γάτας. Παράδειγμα πρόσθεσης των βαρών εμφανίζεται στην *εικόνα 2.10* το βάρος εξαρτάται από την φωτεινότητα του pixel.



Εικόνα 2.10 Σήματα πολλαπλασιάζονται με το βάρος & μετά αθροίζονται.

2.4 Που χρησιμοποιείται η αναγνώριση προτύπων.

Το pattern recognition αποτελεί υποσύνολο της AI. Η συνεισφορά της είναι μεγάλη σε ποικίλες εφαρμογές κάποιες από τις οποίες αναφέρονται ακολούθως. Στην ταξινόμηση εικόνων αναγνωρίζοντας διάφορα πρόσωπα και ταξινομώντας τα στη κατάλληλη κλάση. Επίσης, στην μηχανική όραση που εξετάζει και περιγράφει τα τεχνητά συστήματα όρασης -που βρίσκουν

εφαρμογή σε λογισμικά- που συμπεριλαμβάνει αλγόριθμους οι οποίοι δέχονται εικόνες και ως έξοδο παράγουν συμβολικές περιγραφές των εν λόγω οπτικών σκηνών, όπως στην βιοϊατρική. Επιπροσθέτως στις σεισμικές αναλύσεις για ανίχνευση φυσικών ανωμαλιών και αναγνώριση των δομικών σεισμικών μοτίβων σε δισδιάστατα σεισμογραφήματα. Σε ακόμη έναν τομέα που χρησιμοποιείται, είναι εκείνου του χρηματιστήριου για ανάλυση αγορών, μπορεί να χαρακτηρίζεται μεταβλητός τομέας όμως υπάρχουν αλγόριθμοι που βασίζονται στην artificial intelligence όπως ο Blumberg, ο Tinkoff, και ο αλγίριθμος Sofi. Οι επιστήμονες αφουγκράζονται τις τρέχουσες ανάγκες της κοινωνίας και η αναγνώριση προτύπων περνάει και στον τομές της υγείας. Συγκεκριμένα συμβάλει στην αποτελεσματική διάγνωση του κορωνοϊού μέσω της χρήσης αλγορίθμων που μελετούν τομογραφίες θώρακα. Αξιοσημείωτη επίσης είναι η συμβολή της και στην αναγνώριση ομιλίας. Οι εφαρμογές, γνωστές σε όλους πλέον Siri, Alexa, Cortona, ανήκουν στο pattern recognition.Οι αλγόριθμοι ομιλίας ακολουθούν συγκεκριμένες οδηγίες που έχουν καθοριστεί με το χέρι για την εύρεση μοτίβων ηχητικών κυμάτων ομιλίας τα οποία τα χαρακτηρίζουν ως «φωνητικές μονάδες» και καθορίζουν το εύρος ομιλίας πριν από τη μετάφρασή τους σε ουσιαστικούς συνδυασμούς γραμμάτων και τελικά λέξεων. [27]

2.5 Συμπεράσματα κεφαλαίου

Η αναγνώριση προτύπων μέσω υπολογιστών αποτελεί μεγάλη εφεύρεση. Το τέχνασμα του πλησιέστερου γείτονα και η μετεξέλιξη του σε Κ-πλησιέστερους γείτονες είναι τεχνική ταξινόμησης που χρησιμοποιείται ακόμα και σε χειρόγραφους χαρακτήρες και προϋποθέτει σύγκριση κάθε δείγματος με τις υπάρχουσες κλάσεις. Τα δέντρα αποφάσεων είναι είδος προγνωστικών μοντέλων, ανήκουν στην μηχανική μάθηση και συμβάλλουν στη καταπολέμηση της ιστορύπανσης και η διαδικασία ταξινόμησης τους είναι αυτόματη και πραγματοποιείται μόνο μια φορά. Τα νευρωνικά δίκτυα προσομοιώνουν τον ανθρώπινο εγκέφαλο και ανήκουν στην βαθιά μάθηση. Κάθε νευρώνας του δικτύου δέχεται στοιχεία εισόδου τα οποία πολλαπλασιάζονται με το αντίστοιχο βάρος και αθροίζονται. Μόλις αθροιστούν όλοι οι παράγοντες θα προκύψει η ενεργοποίηση ή μη του νευρώνα. Επόμενο επίπεδο είναι το κρυφό επίπεδο *(hidden layer)*.Οι αποκρίσεις κάθε επιπέδου μπορεί να αποτελούν την έξοδο του νευρωνικού δικτύου ή μπορεί και να συνδέονται με νέο κρυφό επίπεδο.

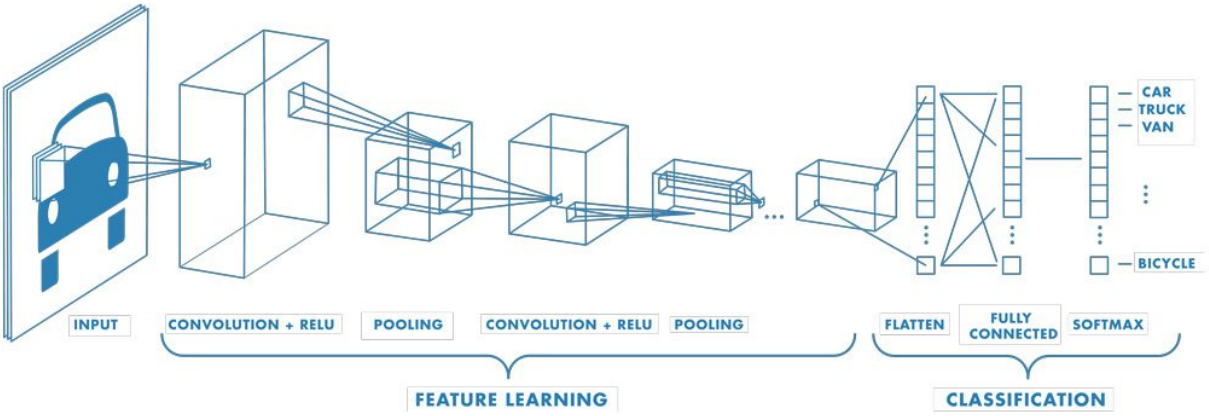
3 ΚΕΦΑΛΑΙΟ 3ο:Εφαρμογές στην αναγνώριση προτύπων.

Το παρόν κεφάλαιο εστιάζει στα **συνελικτικά νευρωνικά δίκτυα** *(convolutional neural networks, CNNs, ConvNets)* και συγκεκριμένα στην συνεισφορά τους στην **αναγνώριση προτύπων**. Είναι κατηγορία νευρωνικών δικτύων (*neural networks*) και έχουν αποδειχθεί πολύ αποτελεσματικά στην αναγνώριση, επεξεργασία και ταξινόμηση εικόνων. Είναι γνωστά ως *«η εφαρμογή της νευροεπιστήμης (neuroscience) στη μηχανική μάθηση»*. Χρησιμοποιούν την **συνέλιξη** *(convolution)* που είναι εξειδικευμένο είδος γραμμικής λειτουργίας. Θα παρουσιαστεί η λειτουργία τους τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο.

Αναλυτικότερα σκοπός του εν λόγω κεφαλαίου είναι με την βοήθεια του Matlab και του πακέτου AlexNet, που αποτελεί μορφή προ-εκπαιδευμένου συνελικτικού νευρωνικού δικτύου και με κώδικα που θα δημιουργηθεί από την αρχή να γίνει πετυχημένη αναγνώριση οκτώ ατόμων μετά από επιλογή προσωπικής αρεσκείας. Πρώτα θα παρουσιαστεί η υλοποίηση κώδικα στο Matlab που θα λαμβάνει εικόνες μέσω κάμερας, που έχουν επιλεγεί από τον χρήστη, και με αυτό το μέρος του κώδικα να δημιουργηθεί από το μηδέν μια βάση δεδομένων από φωτογραφίες των οκτώ διάσημων πρόσωπων Jennifer Aniston, Courteney Cox, Lisa Kudrow, Matt LeBlanc, Matthew Perry, David Schwimmer, Λευτέρης Πετρούνιας και η Μαρία Σάκκαρη και αυτό αποτελεί το διαδραστικό μέρος του κώδικα, αφού ο χρήστης επιλέγει τις φωτογραφίες που θα δείχνει στην κάμερα μέσω του κινητού τηλεφώνου του και τις παρουσιάζει έτσι ώστε να λάβει στιγμιότυπα το σύστημα να τα αποθηκεύσει και με αυτή την διαδικασία να φτιάξει την βάση δεδομένων. Οι φωτογραφίες που θα αποτελέσουν την βάση δεδομένων πρέπει να ποικίλουν και να παρουσιάζουν τους εικονιζόμενους σε διαφορετικές ηλικίες και με διάφορα αξεσουάρ (π.χ καπέλο) για να είναι όσο πιο ακριβής η ταυτοποίηση από το σύστημα. Δεύτερον γράφεται καινούργιο κομμάτι κώδικα το οποίο θα εκπαιδεύει το συνελικτικό δίκτυο με στόχο να μάθει να αναγνωρίζει τα άνωθεν άτομα και τα αποτελέσματα αυτού -για τα χαρακτηριστικά προσώπου του κάθε ατόμου- θα αποθηκεύονται ώστε να είναι ικανό το σύστημα στο τρίτο μέρος κώδικα που δημιουργείται να τα χρησιμοποιήσει για την αναγνώριση. Κατά τον ίδιο τρόπο ο χρήστης στον τρίτο και τελευταίο μέρος κώδικά επιλέγει νέες εικόνες των οκτώ προσώπων τις δείχνει στην κάμερα του υπολογιστή και αναμένει για το αν θα γίνει η ορθή ή μη ταυτοποίηση.

Θεωρητικά τώρα η αρχιτεκτονική των ConvNets έχει σχεδιαστεί έτσι ώστε να εκμεταλλεύεται τη δισδιάστατη δομή εικόνων ή των σημάτων ήχου που λαμβάνονται ως είσοδοι. Αυτό εξασφαλίζεται με την ύπαρξη των τοπικών συνδέσεων *(local connections)* και των βαρών *(weight)* ακολουθούμενα από τα επίπεδα συγκέντρωσης *(pooling layers)* με αποτέλεσμα να δημιουργούνται τα χαρακτηριστικά αμετάβλητων μετατοπίσεων *(translation invariant),* δηλαδή τα χαρακτηριστικά

που δίνουν τη δυνατότητα αναγνώρισης πρόσωπων, αντικείμενων ακόμα και όταν η εμφάνισή τους ποικίλλει με κάποιο τρόπο. Επίσης με τις τοπικές συνδέσεις επιλύεται και το θέμα της πολυπλοκότητας που συναντάται κατά την εκπαίδευση του δικτύου, διότι περιορίζονται οι συνδέσεις των νευρώνων στην είσοδο αλλά και των νευρώνων του κρυφού επιπέδου με απόρροια κάθε κρυφός νευρώνας να συνδέεται μόνο με ένα μικρό μέρος νευρώνων εισόδου. Τονίζεται ότι τα ConvNets διαθέτουν λιγότερες προϋποθέσεις και εκπαιδεύονται πιο εύκολα απ' ότι πλήρως συνδεδεμένα νευρωνικά δίκτυα *(fully connected)* με τον ίδιο πλήθος κρυφών επιπέδων.[36]



Εικόνα 3.1 Δομή CNNs. Πηγή: https://ch.mathworks.com/discovery/convolutional-neural-network-matlab.html

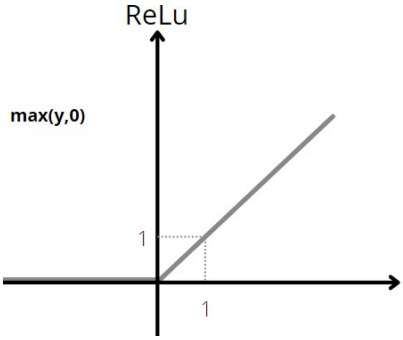
Στην *εικόνα 3.1* το CNN λαμβάνει ως είσοδο εικόνες με χαρακτηριστικά $m \times m \times r$, το m αντιπροσωπεύει το ύψος *(height)* και το πλάτος *(width)* της εικόνας, ενώ το r το πλήθος των καναλιών. Αποδίδεται εικονικά η αρχιτεκτονική των συνελικτικών νευρωνικών δικτύων. Υπάρχουν τέσσερις κύριες λειτουργίες η **συνέλιξη** *(convolution),* η **μη-γραμμικότητα** *(non linearity),* η **συγκέντρωση** *(pooling)* και το **πλήρως συνδεδεμένο επίπεδο** *(fully connected layer).* Τα στρώματα συνέλιξης και συγκέντρωσης εξάγουν χαρακτηριστικά από τις εικόνες που εισάγονται, ενώ το πλήρως συνδεδεμένο επίπεδο λειτουργεί ως ταξινομητής των εικόνων.

Πιο συγκεκριμένα, το πρώτο επίπεδο που συναντάται είναι εκείνο της συνέλιξης που συμπεριλαμβάνει τα φίλτρα kernels με χαρακτηριστικά $n \times n \times q$, το n δηλώνει τις νέες, μικρότερες διαστάσεις των εικόνων και το q το κανάλι που μπορεί να είναι μικρότερο ίσο του αρχικού. Δημιουργείται μια τοπική συνδεδεμένη δομή και το εκάστοτε φίλτρο, το οποίο έχει προκύψει μετά από διαδικασία εκμάθησης, πραγματοποιεί συνέλιξη με την εκάστοτε εικόνα με αποτέλεσμα να δημιουργούνται k χάρτες χαρακτηριστικών *(feature maps)* μεγέθους $m\text{-}n+1$.[36] Μέσω αυτών των διεργασιών προκύπτει η συνάρτηση ενεργοποίησης κάθε νευρώνα. Η συνάρτηση της οποίας αποτυπώνεται στην *εικόνα 3.2.*

$$y=\sum_{i=1}^{n} W_i X_i + b_i$$

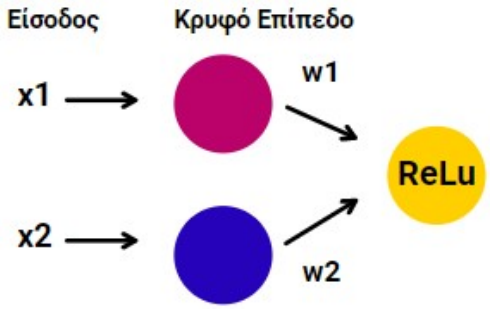
Εικόνα 3.2 Συνάρτηση ενεργοποίησης.

Το W δηλώνει το βάρος, το X τα χαρακτηριστικά της εικόνας εισόδου και το b την σταθερά bias. Η **bias** είναι πολύ σημαντική και ο κάθε νευρώνας έχει διαφορετική τιμή σταθεράς, οι τιμές προσαρμόζονται και βελτιώνονται αυτόματα μέσω εμπειρίας. Είναι εκείνη η οποία λαμβάνει την απόφαση για το αν θα ενεργοποιηθεί ή όχι ο εκάστοτε νευρώνας ή κατά πόσο ισχυρός θα είναι και ταυτόχρονα είναι εκείνη που δηλώνει πόσο ικανό είναι το δίκτυο να αντιλαμβάνεται διαφορετικά δεδομένα. Δεύτερο στάδιο είναι η εφαρμογή **μη γραμμικότητας** *(non-linearity)* που αποτελεί μεγάλο πλεονέκτημα, διότι οι γραμμικές μέθοδοι αδυνατούν να δώσουν ακριβή αποτελέσματα, ειδικότερα αν το σύστημα εμφανίζει χαοτική συμπεριφορά. Η πιο διαδεδομένη μέθοδος είναι η **Rectified Linear Unit** *(ReLU)* που παρουσιάζεται το διάγραμμα της στην *εικόνα 3.3.*



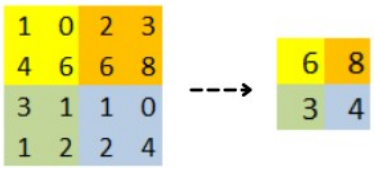
Εικόνα 3.3 Διάγραμμα ReLu.

Λαμβάνει την συνάρτηση ενεργοποίησης από την *εικόνας 3.2* και την περνάει από την ReLu εφαρμόζοντας μια απλή φόρμουλα την max(y,0) που φαίνεται στην *εικόνα 3.3*. Όταν το y είναι αρνητικό τότε η έξοδος είναι μηδέν, ενώ στην περίπτωση που το y είναι θετικό η έξοδος είναι θετική και λαμβάνει την ίδια τιμή με το y. Συνδυάζοντας τα δύο πρώτα στάδια των *εικόνων 3.2* και *3.3* προκύπτει η παρακάτω απεικόνιση της *εικόνας 3.4*:



Εικόνα 3.4 Συνδυασμός δύο πρώτων σταδίων.

Στο τρίτο στάδιο συναντάται το επίπεδο **pooling**, όπου μειώνει την κατανάλωση μνήμης και ταυτόχρονα την μείωση των χωρικών διαστάσεων διατηρώντας τις πιο σημαντικές πληροφορίες, δηλαδή τις μέγιστες τιμές του πίνακα εξόδου του συνελικτικού επιπέδου. Παράδειγμα της διαδικασίας συγκέντρωσης φαίνεται *εικόνα 3.5*. Κάθε χαρακτηριστικό ουσιαστικά υπο-δειγματοληπτείται σε συνεχείς περιοχές μεγέθους *pxp,* στην εν λόγω περίπτωση 2x2, κρατώντας κάθε φορά τη μέγιστη τιμή. Με αυτή τη μέθοδο ελαττώνεται σημαντικά η πολυπλοκότητα, αφού μειώνονται τα δεδομένα κι σαφώς ο αριθμός των πράξεων που θα πραγματοποιηθούν αποτελώντας σημαντικό βήμα για τη μετατροπή των χωρικών πληροφοριών σε χαρακτηριστικά.

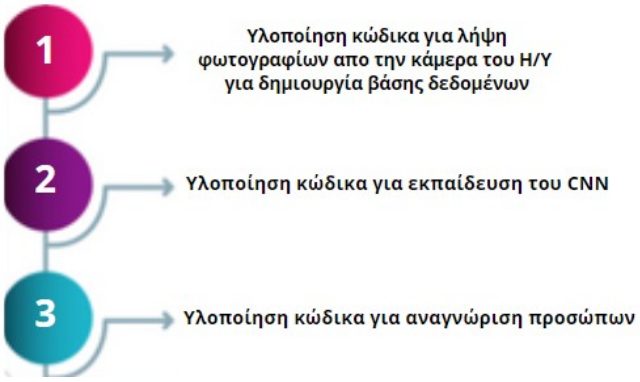


Εικόνα 3.5 Διαδικασία pooling.

Οι περιοχές που υπέστησαν την διαδικασία συγκέντρωσης μπορούν πλέον να χρησιμοποιηθούν για ταξινόμηση, ενώ τέταρτο και τελευταίο στάδιο είναι η **κανονικοποίηση** *(normalization).*

3.1 AlexNet

Στην πράξη τώρα με χρήση του προγραμματιστικού και αριθμητικής υπολογιστικής περιβάλλοντος MATLAB θα παρουσιαστούν τα στάδια που θα οδηγήσουν στην επίτευξη του στόχου, δηλαδή στην αναγνώριση προσώπων.

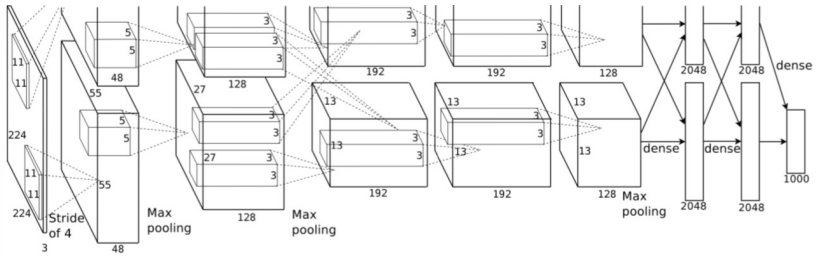


Εικόνα 3.6 Στάδια για την επίτευξη αναγνώρισης.

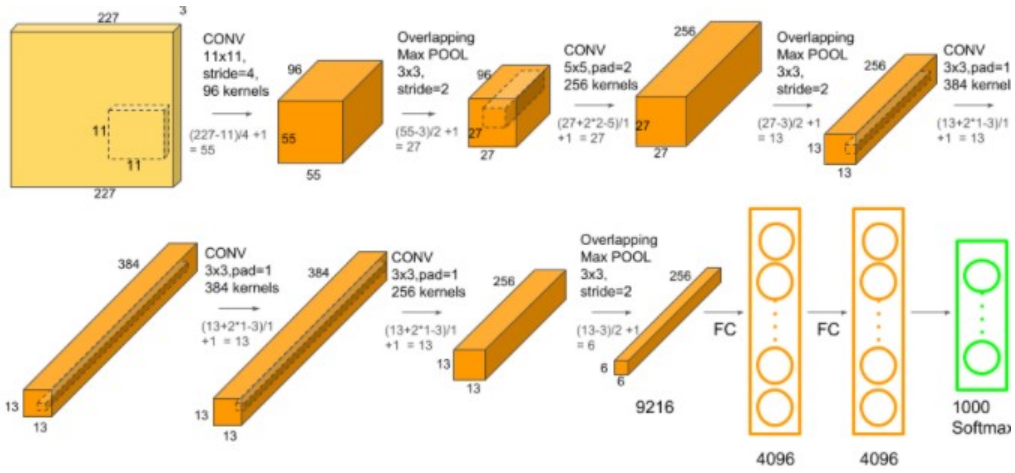
Στην *εικόνα 3.6* φαίνονται τα στάδια που θα ακολουθήσουν. Πρώτο στάδιο είναι η δημιουργία κώδικα που λαμβάνει δεδομένα από την κάμερα του υπολογιστή δημιουργώντας ουσιαστικά την

βάση δεδομένων. Η βάση αποτελείται από οκτώ άτομα, τον ολυμπιονίκη Λευτέρη Πετρούνια, την αθλήτρια Μαρία Σάκκαρη, και τους ηθοποιούς Jennifer Aniston, Courteney Cox, Lisa Kudrow, Matt LeBlanc, Matthew Perry και David Schwimmer, δηλαδή οκτώ κλάσεις. Στο δεύτερο στάδιο γράφεται κώδικας με τον οποίο γίνεται η εκπαίδευση του συνελικτικού δικτύου και η αποθήκευση του. Στο τρίτο και τελευταίο στάδιο υλοποιείται καινούργιος κώδικας ο οποίος καλεί το συνελικτικό εκπαιδευμένο δίκτυο και ενεργοποιεί τη κάμερα του υπολογιστή και δίνοντας του καινούργιες εικόνες των οκτώ προσώπων είναι σε θέση να τις ταυτοποιήσει.

Πρώτο βήμα είναι η εγκατάσταση του ConvNet AlexNet στο Matlab, το οποίο αποτελεί ένα ισχυρό μοντέλο ανάλυσης και υψηλής ακρίβειας. Για να συμβεί η εγκατάσταση θα χρειαστεί η έκδοση του Matlab να είναι του 2018 και μετά, γιατί αυτό το πακέτο δεν είχε κυκλοφορήσει μέχρι το R2016b και στην έκδοση του 2017 δεν εξάγονται αποτελέσματα για το CNN. Η αρχιτεκτονική του AlexNet προβάλλεται στην παρακάτω *εικόνα 3.7*.



Εικόνα 3.7 Αρχιτεκτονική AlexNet. Πηγή: Krizhevsky, A., Sutskever, I., & Hinton, G. E. H. (2012). *ImageNet Classification with Deep Convolutional Neural Networks*. University of Toronto.
https://papers.nips.cc/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf



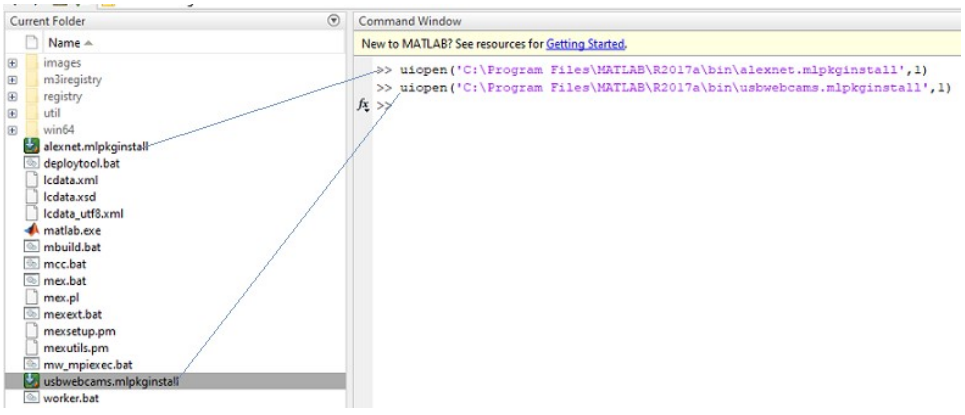
Εικόνα 3.8 Πηγή: Nayak, S. (2021, May 5). Understanding AlexNet | Learn OpenCV. Learn OpenCV | OpenCV, PyTorch, Keras, Tensorflow Examples and Tutorials. https://learnopencv.com/understanding-alexnet/

Στην *εικόνα 3.8* αποκαλύπτονται τα οκτώ επίπεδα που χρησιμοποιεί, πέντε **συνελικτικά στρώματα** *(convolution layers)* και τρία πλήρως **συνδεδεμένα επίπεδα** *(fully connected layers)*. Οι

εικόνες που επεξεργάζεται πρέπει να είναι μεγέθους 227x227x3, οι τιμές δηλώνουν αντίστοιχα το ύψος *(height),* το πλάτος *(width*) και το RBG channel. Κάθε εικόνα που αναλύει περνάει από διάφορα επίπεδα. Το πρώτο επίπεδο είναι εκείνο της συμπίεσης με τα *kernels* να είναι 96 σε αριθμό και τα χαρακτηριστικά του να είναι *f=11*11*, *stride=4*, κάθε φορά εφαρμόζεται ο τύπος **(n+2p-f)/s+1**. Το n ισούται με το 227, το p δηλώνει το γέμισμα (*padding*) που διασφαλίζει να μην χαθούν τα αρχικά εικονοστοιχεία *(pixels)* δίνοντας περισσότερες ακμές και εξασφαλίζοντας ότι όταν συμβούν συμπιέσεις δε θα χαθούν τα αρχικά στοιχεία. Το s είναι το stride που δηλώνει την μετακίνηση ανά pixel και είναι ίσο με τέσσερα, δηλαδή προσπερνάει τέσσερα εικονοστοιχεία. Το αποτέλεσμα του τύπου είναι το 55, που δηλώνει τα χαρακτηριστικά της εξερχόμενης εικόνας η οποία θα είναι η είσοδος στο επόμενο επίπεδο το οποίο ταυτίζεται με εκείνο της *εικόνας 3.8* (55x55x96).

Ακολουθεί το επίπεδο μέγιστης συγκέντρωσης που χρησιμοποιείται για μείωση του πλάτους και του ύψους διατηρώντας το βάθος, δηλαδή τα ενενήντα έξι φίλτρα. Η εικόνα περνάει από επιπλέον φίλτρα συμπίεσης όπως φαίνεται στην *εικόνα 3.8* που στο τέλος συνδέονται στο fully connected layer εξάγοντας 1.000 κλάσεις. Ως έξοδο λαμβάνονται χίλια αποτελέσματα, διότι η αρχιτεκτονική του βασίζεται στο ImageNet.Το ImageNet είναι μια βάση δεδομένων ταξινόμησης εικόνων και υπάρχουν χίλιες διαφορετικές κατηγορίες. Η δημιουργία του έχει συνεισφέρει στην εξέλιξη της υπολογιστικής όρασης *(computer vision)* και της έρευνας της βαθιάς μάθησης.

Δεύτερο βήμα είναι η εγκατάσταση της λειτουργίας webcam για σύνδεση της κάμερας με το πρόγραμμά. Τα πακέτα AlexNet και webcam θα τοποθετηθούν στο φάκελο του bin του Matlab. Η ενεργοποίηση τους γίνεται με την διαδικασία drag and prop στο command window, *εικόνα 3.9* όπου εμφανίζονται δύο ξεχωριστά αναδυόμενα παράθυρα για το καθένα με την ονομασία «*installing support packages»* και πραγματοποιείται η εγκατάσταση τους.



Εικόνα 3.9 Διαδικασία εγκατάστασης.

Τα συστήματα αναγνώρισης προτύπων χρειάζονται δείγματα για να εκπαιδευτούν, στην συγκεκριμένη περίπτωση το σύστημα έλαβε τριακόσιες πενήντα λήψεις του εκάστοτε προσώπου από διαφορετικές ηλικίες οι οποίες ταξινομούνται στην κλάση που τους αναλογεί. Συνολικά το σύστημα εκπαιδεύεται με 2.800 πλήθος εικόνων. Στην *εικόνα 3.10* που ακολουθεί εμφανίζεται το πρόγραμμα που χρησιμοποιείται για. τη λήψη των εικόνων μέσω της κάμερας του υπολογιστή ώστε να δημιουργηθεί η βάση.

```
1  clear all; close all; clc;                % καθαρισμός του command window & επανεκκίνηση κάμερας
2  image=webcam;
3  faceDetector=vision.CascadeObjectDetector;%αλγόριθμος που εντοπίζει το πρόσωπο,τη μύτη, τα μάτια, το στόμα
4  c=350; num_of_image=0;                    %αρχικοποίηση τιμών
5  for num_of_image=0:c                      %βρόχος επανάληψης για την λήψη & αποθήκευση φωτογραφιών
6      i=image.snapshot;
7      bboxes=step(faceDetector,i); %οριοθετεί σε ποια περιοχή βρίσκεται το πρόσωπο
8      if(sum(sum(bboxes))~=0)      %δεν εντόπιστηκε πρόσωπο
9      if(num_of_image>=c)          %ολοκλήρωση των 350 εικόνων
10         break;
11     else
12     new_i=imcrop(i,bboxes(1,:));     %περικοπή εικόνας χρησιμοποιώντας το bbox
13     new_i=imresize(new_i,[227 227]); %ρυθμίζονται οι διαστάσεις 227x227
14     file=strcat(num2str(num_of_image),'.jpg');
15     imwrite(new_i,file); %αποθηκεύονται οι εικόνες
16     imshow(new_i);       %εμφανίζεται η εικόνα που αποθηκεύεται
17     drawnow;
18     end
19     else
20         imshow(i);%εμφανίζεται η εικόνα που δεν ανίχνευσε πρόσωπο
21         drawnow;
22     end
23 end
```

Εικόνα 3.10 Συλλογή εικόνων.

Στην *εικόνα 3.10* εμφανίζεται ο αλγόριθμος οποίος έχει προσαρμοστεί ώστε να αποθηκεύει τις λήψεις στην περίπτωση που μόνο εντοπίζονται πρόσωπα στην οθόνη και αυτό επιτυγχάνεται με τον αλγόριθμο Violas-Jones που είναι προσαρμοσμένος να εντοπίζει τα όρια του προσώπου, τα μάτια, τα χείλη και τη μύτη του εικονιζόμενου. Το εκάστοτε πρόσωπο είναι μοναδικό με εκατομμύρια μικροσκοπικά χαρακτηριστικά που το διαφοροποιούν από κάποιο άλλο, αξιολογώντας κάθε μικρό κομμάτι δεδομένων. Υπάρχουν δύο στάδια στον αλγόριθμο Viola-Jones η εκπαίδευση και η ανίχνευση. Η εκπαίδευση έχει προέλθει μετά από την τροφοδότηση δεδομένων και στη συνέχεια εκπαιδεύεται για να μπορέσει να προβλέψει. Η εικόνα μετατρέπεται σε κλίμακα του γκρι, καθώς είναι πιο εύκολο να επεξεργαστεί αφού υπάρχουν λιγότερα δεδομένα και εκείνη τη στιγμή ανιχνεύει το πρόσωπο και στο τέλος εντοπίζει τη θέση του στην έγχρωμη εικόνα. Πιο αποτελεσματική είναι η ανίχνευση όταν τα πρόσωπα που κοιτάζουν ευθεία και όχι πλάγια, πάνω ή κάτω.

Στην *εικόνα 3.10* συμβαίνουν τα εξής:

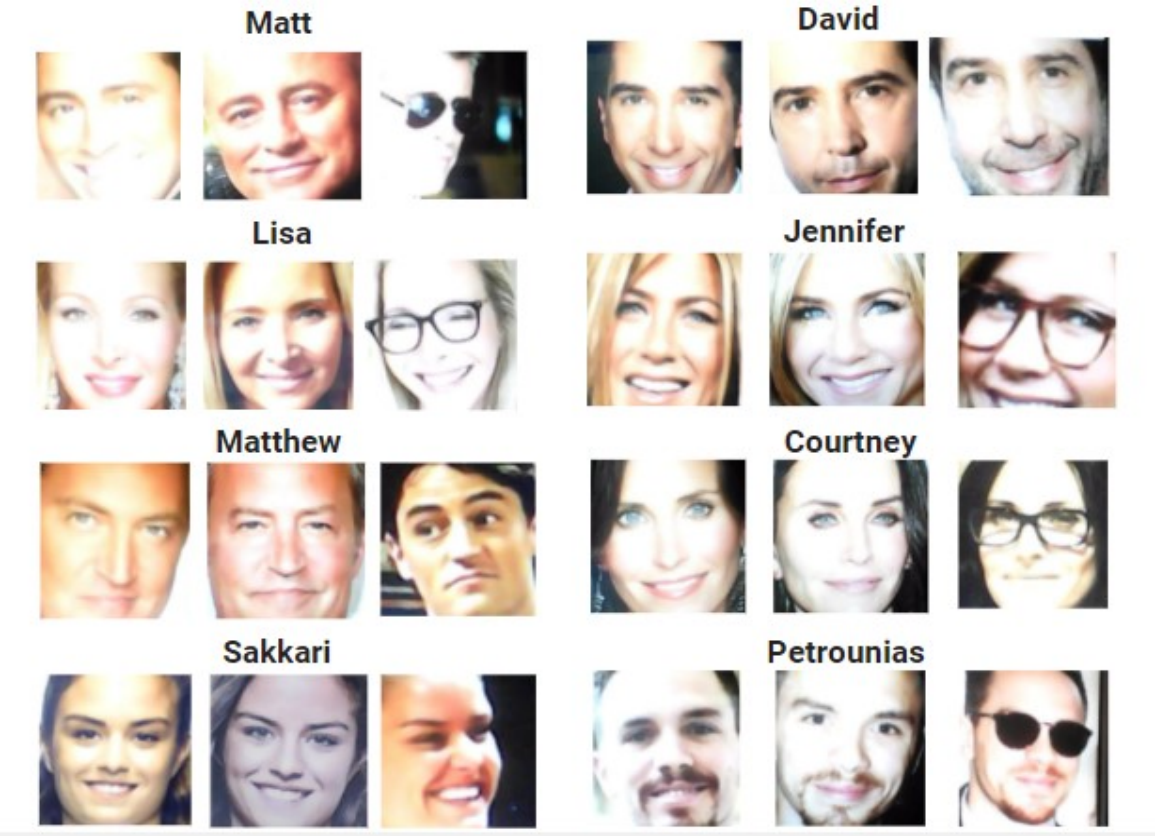
- Στην **γραμμή 2** του κώδικα ενεργοποιείται η κάμερα του υπολογιστή.

- Στην **γραμμή 3** γίνεται εντοπισμός του προσώπου με χρήση τον αλγορίθμου Violas-Jones
- Στην **γραμμή 4** γίνεται η αρχικοποίηση των τιμών πριν εισέλθει στο βρόχο επανάληψης
- Στην **γραμμή 5** αρχίζει ο βρόχος επανάληψης for
- Στην **γραμμή 6** λαμβάνεται στιγμιότυπο
- Στην **γραμμή 7** με την βοήθεια του bbox οριοθετείται η περιοχή του προσώπου και σε συνεργασία με την συνάρτηση step που ανιχνεύει τα στοιχεία του προσώπου επιστρέφεται πίνακας που αναφέρει το πλάτος και το μήκος για το εκάστοτε στοιχείο του προσώπου.
- Στη **γραμμή 8** ουσιαστικά αν οι τιμές του πίνακα είναι κοντά στο μηδέν δηλώνεται ότι δεν υπάρχει πρόσωπο και πηγαίνει στην **γραμμή 20** δείχνοντας σε πραγματικό χρόνο το τι λαμβάνει η κάμερα μη λαμβάνοντας κάποιο στιγμιότυπο
- Στην **γραμμή 9** όταν ολοκληρώνεται το πλήθος τερματίζεται η διαδικασία μέσω break
- Στην **γραμμή 12** εφόσον έχει εντοπιστεί πρόσωπο γίνεται περικοπή της εικόνας χρησιμοποιώντας τα όρια που είχαν εντοπιστεί μέσω της **γραμμής 7**
- Στην **γραμμή 13** επιστρέφεται η εικόνα η οποία πρόκειται να αποθηκευτεί με τις διαστάσεις που λαμβάνει ως είσοδο το AlexNet *227x227*
- Στην **γραμμή 14** μετατρέπεται ο αριθμός i σε συμβολοσειρά και αποθηκεύεται με την κατάληψη «.jpg», στην ουσία επεξεργάζεται τις λήψεις που είναι αριθμημένες σε μορφή 1,2,3…. και γι' αυτό χρησιμοποιείται η num2str.
- Στην **γραμμή 15** δημιουργείται ένας καινούργιος φάκελος για την αποθήκευση των εικόνων.
- Η **γραμμή 16** δείχνει κάθε φορά την λήψη της εικόνας με τις καινούργιες της διαστάσεις.

Μόλις ολοκληρωθούν οι λήψεις για όλα τα άτομα που επιλέχτηκαν ώστε να ταυτοποιεί το δίκτυο και με τον καθένα τους να αποτελεί μία κλάση, δημιουργούνται οκτώ ξεχωριστοί φάκελοι *(folders)* με τα ονόματά τους και οι φωτογραφίες τοποθετούνται στο φάκελο που τους αναλογεί. Όλοι οι φάκελοι συγκεντρώνονται και τοποθετούνται στον κύριο πλέον φάκελο που ονομάζεται «collect», αποτελώντας πλέων υποφακέλους όπως φαίνεται και στην *εικόνα 3.11.*

Εικόνα 3.11 Οι οκτώ κλάσεις.

Δείγμα των εικόνων που λήφθηκαν από την κάμερα φαίνεται στην *εικόνα 3.12.*



Εικόνα 3.12 Δείγματα.

Δεύτερο στάδιο αποτελεί η εκπαίδευση του δικτύου. Στην *εικόνα 3.13* φαίνεται ο κώδικας.

```
1 -    clc;close all;
2 -    cnn=alexnet;                        %φορτώνεται το pre-trained net
3 -    layers=cnn.Layers;                  %καθορίζονται τα επίπεδα του alexnet
4 -    layers(23)=fullyConnectedLayer(8);% τροποποίηση επιπέδων για 8 κλάσεις
5 -    layers(25)=classificationLayer
6 -    images=imageDatastore('collect', 'IncludeSubfolders', true,...
7          'LabelSource', 'foldernames');%φάκελος&υποφάκελοι που λαμβάνονται οι εικόνες
8 -    opts=trainingOptions('sgdm','MiniBatchSize',64,'MaxEpochs',20,...
9          'InitialLearnRate',0.001);     %ποσοστά εκμάθησης
10 -   Cnetwork2=trainNetwork(images,layers,opts);%εκπαίδευση δικτύου
11 -   save ('cnn.mat','Cnetwork2');       %αποθήκευση
```

Εικόνα 3.13 Μέρος εκπαίδευσης.

Η εξήγηση του κώδικά της *εικόνας 3.13* δίνεται παρακάτω:

- Στην **γραμμή 2** φορτώνεται το προ-εκπαιδευμένο συνελικτικό δίκτυο AlexNet
- Στην **γραμμή 3** καθορίζονται τα επίπεδα του AlexNet

- Στην **γραμμή 4** και **5** γίνεται τροποποίηση των εξόδων και αναδιαμορφώνονται τα επίπεδά του, διότι το AlexNet είναι προσαρμοσμένο να αναγνωρίζει 1000 τάξεις, ενώ στόχος του παραδείγματος αυτού είναι να αναγνωρίζονται μόνο οκτώ
- Στην **γραμμή 7** λαμβάνει τα εκπαιδευτικά δεδομένα από κύριο φάκελο «collect» και των υποφακέλων του
- Στην **γραμμή 8** τίθενται οι τιμές των παραμέτρων της εκπαίδευσης του
- Στην **γραμμή 10** γίνεται η διαδικασία εκπαίδευσης και
- Στην **γραμμή 11** η αποθήκευσή του για να χρησιμοποιηθούν τα αποτελέσματα μετά στο τρίτο μέρος του κώδικα όπου θα συμβεί η αναγνώριση.

Στην *εικόνα 3.14* φαίνεται η ώρα που χρειάστηκε για να εκπαιδευτεί το δίκτυο, οι πληροφορίες αυτές εμφανίζονται στο command window του MATLAB. Η πρώτη στήλη **epoch** πρόκειται για μια αριθμητική τιμή που υποδεικνύει σε πόσα σύνολά διαχώρισε το δίκτυο τα δεδομένα. Η δεύτερη στήλη **iteration** δηλώνει πόσα εκπαιδευτικά δεδομένα έχει κάθε epoch. Η τρίτη στήλη **time elapsed** δηλώνει τον χρόνο που χρειάστηκε κάθε διεργασία ώστε να ολοκληρωθεί. Η τέταρτη στήλη **mini-batch accuracy** δηλώνει τα ποσοστά ακρίβειας για κάθε σύνολο και η πέμπτη στήλη **mini-batch loss** το ποσοστό των στοιχείων που χάθηκαν και η τελευταία στήλη **base learning rate** τον ρυθμό μάθησης που επιλέχτηκε από την γραμμή του κώδικά 8 στην *εικόνα 3.13*.

```
Training on single CPU.
Initializing image normalization.
|=========================================================================================|
|  Epoch  |  Iteration  |  Time Elapsed  |  Mini-batch  |  Mini-batch  |  Base Learning  |
|         |             |   (hh:mm:ss)   |   Accuracy   |     Loss     |      Rate       |
|=========================================================================================|
|       1 |           1 |       00:00:09 |       21.88% |       2.8825 |          0.0010 |
|       3 |          50 |       00:10:08 |      100.00% |       0.0005 |          0.0010 |
|       6 |         100 |       00:18:09 |      100.00% |   9.7235e-05 |          0.0010 |
|       8 |         150 |       00:25:32 |      100.00% |       0.0001 |          0.0010 |
|      11 |         200 |       00:31:37 |      100.00% |       0.0002 |          0.0010 |
|      14 |         250 |       00:37:24 |      100.00% |   7.5365e-05 |          0.0010 |
|      16 |         300 |       00:43:07 |      100.00% |   1.8931e-05 |          0.0010 |
|      19 |         350 |       00:48:52 |      100.00% |   6.1171e-05 |          0.0010 |
|      20 |         380 |       00:52:18 |      100.00% |       0.0001 |          0.0010 |
|=========================================================================================|
```

Εικόνα 3.14 Ολοκλήρωση εκπαίδευσης CNN.

Τελευταίο κομμάτι, για να ολοκληρωθεί η διαδικασία, αποτελεί η εκτέλεση και η διαπίστευση λειτουργικότητας του κώδικα για την αναγνώριση προσώπων που λαμβάνονται από την κάμερα. Ο κώδικας εμφανίζεται στην *εικόνα 3.15.*

```
1  clc; close all; clear all;
2  c=webcam;                          %ενεργοποίηση κάμερας
3  loaded_Network = load('cnn.mat');%φόρτωση νευρωνικού δικτύου
4  net = loaded_Network.Cnetwork2;
5  faceDetector=vision.CascadeObjectDetector;
6  while true        %όσο είναι αληθής ταυτοποιεί τα πρόσωπα
7      e=c.snapshot; %λήψη στιγμιότυπου
8      bboxes =step(faceDetector,e);
9      if(sum(sum(bboxes))~=0)
10     es=imcrop(e,bboxes(1,:));
11     es=imresize(es,[227 227]);
12     [label, Probability] = classify(net, es); %κλάση
13     image(e);
14     title({char(label), num2str(max(Probability)*100, 2)}); %ποσοστό ακριβείας χρησιμοποιώντας 2 ψηφία
15     drawnow;
16     else
17         image(e);
18         title('Not a match'); %όταν δεν αναγνωρίζει κάποιο απο τα προσωπα της βάσης
19     end
20 end
```

Εικόνα 3.15 Στην πράξη.

Η εξήγηση του κώδικα της *εικόνας 3.15* είναι η εξής:

- Στην **γραμμή 2** ενεργοποιείται η κάμερα
- Στην **γραμμή 3** φορτώνεται το δίκτυο που εκπαιδεύτηκε στο προηγούμενο μέρος του κώδικα στην *εικόνα 3.13*
- Στην **γραμμή 4** το δίκτυο αντιστοιχείται με την μεταβλητή net
- Στην **γραμμή 5** εφαρμόζεται ο αλγόριθμος Viola-Jones
- Στην **γραμμή 6** χρησιμοποιείται βρόχος επανάληψης που δηλώνει όσο είναι η συνθήκη είναι αληθής να συνεχίσει την ταυτοποίηση
- Στην **γραμμή 7** λαμβάνεται στιγμιότυπο
- Στην **γραμμή 8** οριοθετείται η θέση του προσώπου
- Στην **γραμμή 9** αν δεν εντοπιστεί πρόσωπο ο κώδικας πηγαίνει στην **γραμμή 17** ώστε να δείξει στον χρήστη τι εντοπίζει και να βγάλει ειδοποίηση *«Not a match»*
- Στην **γραμμή 10** εφόσον έχει εντοπιστεί πρόσωπο γίνεται περικοπή της εικόνας χρησιμοποιώντας τα όρια που είχαν εντοπιστεί μέσω της **γραμμής 7**
- Στην **γραμμή 11** αναδιαμορφώνεται η εικόνα η οποία πρόκειται να αποθηκευτεί με τις διαστάσεις *227x227*
- Στην **γραμμή 12** καθορίζεται η πιθανότητα της εκάστοτε εικόνας και σε ποια κλάση θα ανήκει

- Στην **γραμμή 14** ορίζεται η επιγραφή, ο τίτλος που θα εμφανίζεται σε κάθε αναγνώριση με την ονομασία και το ποσοστό ακριβείας

Δίνοντας νέα δείγματα εξετάζεται η αποτελεσματικότητα του δικτύου. Τα αποτελέσματα δίνονται ακολούθως.

Εικόνα 3.16 Ποσοστά ακριβείας Matthew.

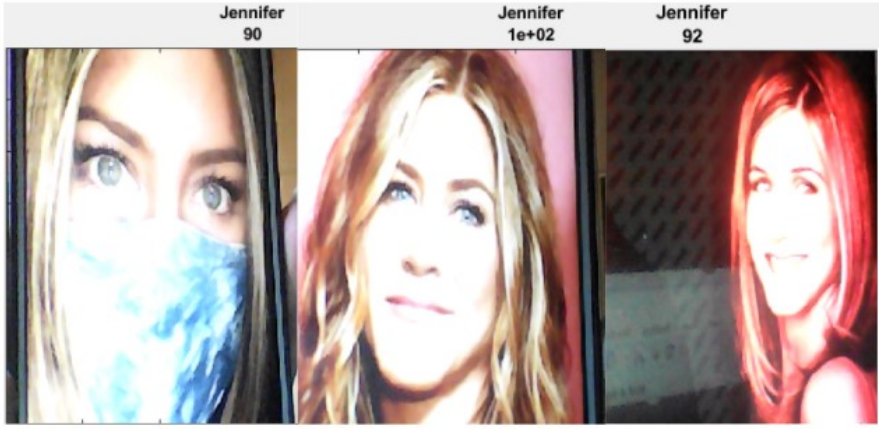
Στην *εικόνα 3.16* παρουσιάζονται οι νέες εικόνες του ηθοποιού Matthew που τίθεται το δίκτυο να αναγνωρίσει. Όλες αναγνωρίζονται επιτυχώς το μόνο χαμηλό ποσοστό ακριβείας βρίσκεται στην πρώτη εικόνα με 45% ακρίβεια, εκεί όπου ο εικονιζόμενος εμφανίζεται με γυαλιά μυωπίας, το ποσοστό είναι τόσο χαμηλό διότι δεν δόθηκαν πολλές εικόνες στο δίκτυο όπου ο εικονιζόμενος να εμφανίζεται με γυαλιά. Η δεύτερη φωτογραφία παρουσιάζει τον ηθοποιό με καπέλο και το ποσοστό ταύτισης είναι αρκετά υψηλό της τάξης του 79% και στην τελευταία εικόνα είναι 100% ακριβές.

Εικόνα 3.17 Ποσοστά ακριβείας Courtney.

Στην *εικόνα 3.17* παρουσιάζεται η ηθοποιός Courtney Cox όλες οι καινούργιες εικόνες που δόθηκαν ταυτοποιήθηκαν με ποσοστό ακρίβειας 100%.

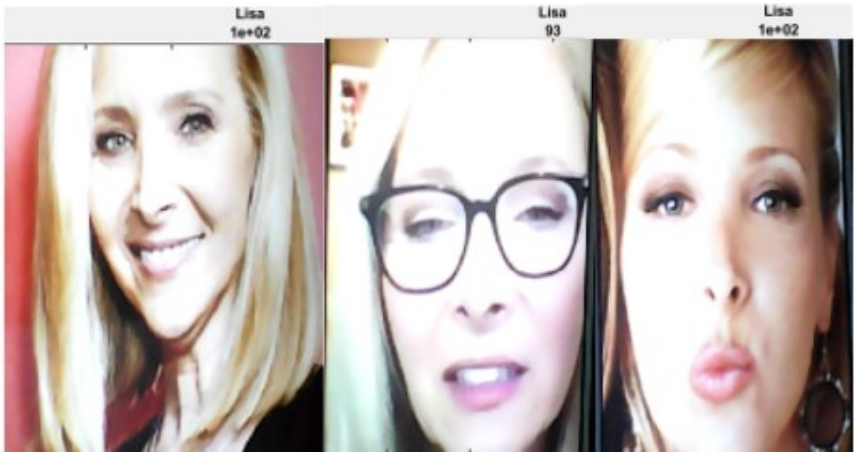
Εικόνα 3.18 Ποσοστά ακριβείας David.

Στην *εικόνα 3.18* φαίνονται οι τρείς διαφορετικές, νέες φωτογραφίες του ηθοποιού David που δόθηκαν ώστε να αναγνωριστούν και οι τρείς φέρουν ποσοστά ακριβείας του μέγιστου βαθμού, δηλαδή 100%.



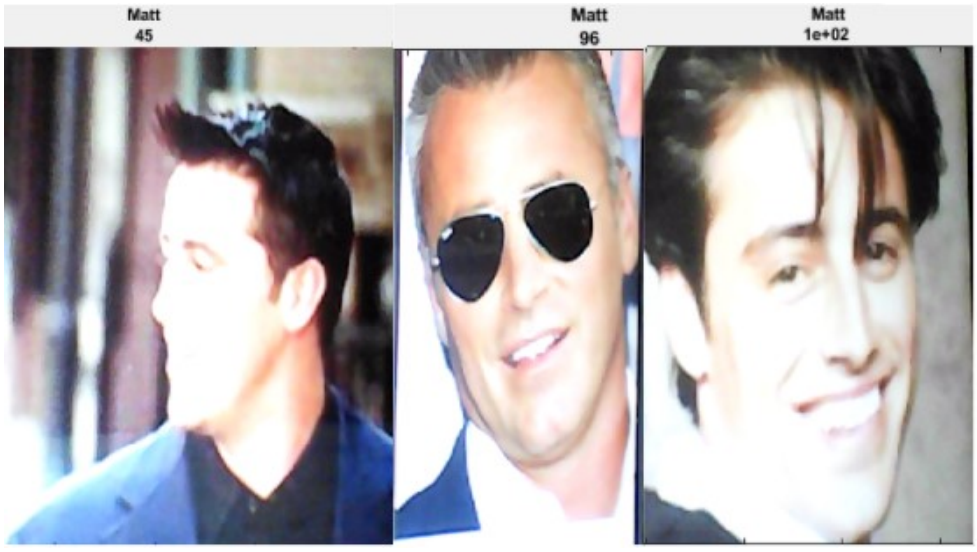
Εικόνα 3.19 Ποσοστά ακριβείας Jennifer.

Στη *εικόνα 3.19* εξήχθησαν πολύ υψηλά ποσοστά και για την ηθοποιό Jennifer Aniston. Υπογραμμίζεται συγκεκριμένα η πρώτη φωτογραφία στην οποία η εικονιζόμενη φοράει μάσκα καλύπτοντας σημαντικό μέρος του προσώπου της και το ποσοστό ακριβείας είναι 90%, ποσοστό που αποδεικνύει τη λειτουργικότητα του δικτύου ακόμα και σε περιπτώσεις που διαφέρει η εμφάνιση. Στην δεύτερη εικόνα το ποσοστό ακριβείας είναι 100% και η τρίτη φωτογραφία έχει ποσοστό 92% το οποίο είναι πλήρως ικανοποιητικό.



Εικόνα 3.20 Ποσοστά ακριβείας Lisa.

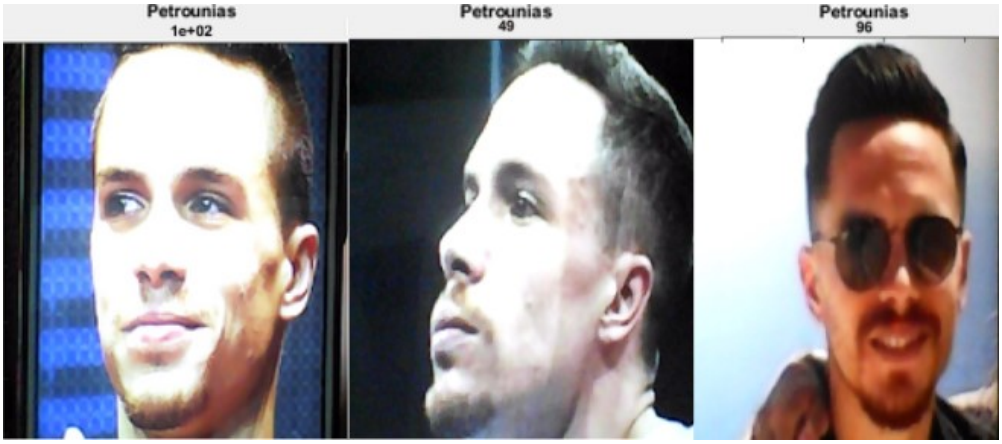
Στην περίπτωση της *εικόνας 3.20* η ταυτοποίηση είναι και εδώ επιτυχημένη. Η πρώτη και η τρίτη φωτογραφία έχουν ποσοστά ακριβείας 100% με το δίκτυο να αναγνωρίζει την ηθοποιό επιτυχημένα σε διαφορετικές ηλικίες και με διαφορετική έκφραση, όπως προβάλλεται στην τρίτη φωτογραφία. Στη μεσαία φωτογραφία παρουσιάζεται με γυαλιά μυωπίας και με μεγάλο ποσοστό ακρίβειας 93% που είναι εξίσου υψηλό και ικανοποιητικό και είναι τόσο επιτυχημένο, διότι στο δίκτυο δόθηκαν ως εκπαιδευτικά δεδομένα ποικίλες εικόνες της ηθοποιοί οι οποία εμφανιζόταν με γυαλιά σε αντίθεση με την περίπτωση του ηθοποιού στην *εικόνα 3.16* που δεν είχαν δοθεί τόσες εικόνες στο δίκτυο φορώντας γυαλιά.



Εικόνα 3.21 Ποσοστά ακριβείας Matt.

Στην *εικόνα 3.21* παρατηρείται ότι ο ηθοποιός στην πρώτη φωτογραφία δεν κοιτάει το φακό αλλά

παρόλα αυτά ταυτοποιήθηκε επιτυχώς με χαμηλό ποσοστό ακρίβειας της τάξης του 45%. Στις επόμενες δύο εικόνες εμφανίζεται αρχικά με γυαλιά ηλίου και ταυτοποιείται ορθώς με ποσοστό 96% και είναι τόσο ακριβές, διότι δόθηκαν πολλές διαφορετικές εικόνες του ηθοποιού με γυαλιά και στην τελευταία παρουσιάζεται μια φωτογραφία σε αρκετά νεότερη ηλικία και το ποσοστό ακρίβειας φτάνει το μέγιστο, 100%.



Εικόνα 3.22 Ποσοστά ακριβείας Petrounias.

Στην *εικόνα 3.22* ο ολυμπιονίκης Λευτέρης Πετρούνιας ταυτοποιείται επιτυχώς στην πρώτη εικόνα με ποσοστό 100%, στην δεύτερη ταυτοποιείται με 49% ακρίβεια, διότι εμφανίζεται μόνο το προφίλ του και στην τρίτη εικόνα που εμφανίζεται με γυαλιά ηλίου το ποσοστό ακριβείας αγγίζει το 96%.

Εικόνα 3.23 Ποσοστά ακριβείας Sakkari.

Στην *εικόνα 3.23* ταυτοποιείται επιτυχώς η αθλήτρια Μαρία Σάκκαρη, η πρώτη εικόνα φτάνει το 98% ποσοστό ακριβείας ενώ η δεύτερη το 86%, εξίσου υψηλό ποσοστό ακρίβειας, και η τρίτη φωτογραφία το ποσοστό 52% λόγω του ότι φαίνεται σε πλάγια όψη προσώπου *(profil)* και όχι ανφάς.

Όλες οι εικόνες των προσώπων ταυτοποιήθηκαν επιτυχώς. Έγινε αναγνώριση των ατόμων όταν φορούσαν διάφορα αξεσουάρ -όπως γυαλιά, καπέλο ακόμα και μάσκα-, όταν δεν κοιτούσαν τον φακό αλλά είχαν γυρισμένο το πρόσωπο τους, όταν σχηματιζόντουσαν διάφορες εκφράσεις στα πρόσωπα τους και σε διαφορετικές ηλικίες. Υπογραμμίζεται ότι στη περίπτωση της *εικόνα 3.16* ο ηθοποιός Matthew είχε 45% ποσοστό ακριβείας και αυτό γιατί δεν είχαν δοθεί επαρκή εκπαιδευτικά δεδομένα στο δίκτυο με τον εικονιζόμενο να φοράει γυαλιά, ενώ στις περιπτώσεις των *εικόνων 3.21* και *3.20* που είχαν δοθεί με τα ποσοστά να ξεπερνούν το 90%.

Στην *εικόνα 3.24* το σύστημα αναγνωρίζει ορθώς ότι δεν πρόκειται για κάποιο από τα πρόσωπα που μπορεί να αναγνωρίσει και βγάζει σχετική ειδοποίηση. Ειδικότερα στο κάτω μέρος της *εικόνα 3.24* που του δόθηκαν δύο διάσημα πρόσωπα, η Ελένη Μενεγάκη και ο Σάκης Ρουβάς, αναγνωρίζει επιτυχώς ότι δεν πρόκειται για κάποιο από τα οκτώ άτομα και εμφανίζει σχετικό μήνυμα.

Εικόνα 3.24 Νέα δείγματα.

Ακολούθως εμφανίζεται ο συγκεντρωτικός πίνακας 3.1 με τα ποσοστά ακριβείας γι' όλες τις εικόνες που εξετάστηκαν. Είκοσι οκτώ φωτογραφίες ταυτοποιήθηκαν επιτυχώς από το σύστημα αποδεικνύοντας την αποτελεσματικότητα του.

Matthew1	45%	
Matthew2	79%	
Matthew3	100%	
Courtney1	100%	
Courtney2	100%	
David1	100%	
David2	100%	
David3	100%	
Courtney3	100%	
Jennifer1	90%	
Jennifer2	100%	
Jennifer3	92%	
Lisa1	100%	
Lisa2	93%	
Lisa3	100%	
Matt1	45%	
Matt2	96%	
Matt3	100%	
Petrounias1	100%	
Petrounias2	49%	
Petrounias3	96%	
Sakkari1	98%	
Sakkari2	86%	
Sakkari3	52%	
Γάτα	Not a match	Ορθή ειδοποίηση
Πίθινος	Not a match	Ορθή ειδοποίηση
Ελένη Μεναγάκη	Not a match	Ορθή ειδοποίηση
Σάκης Ρουβάς	Not a match	Ορθή ειδοποίηση

Πίνακας 3.1 Πίνακας ποσοστών.

Τέλος, αν υπήρχε η επιθυμία για αναγνώριση περισσότερων ατόμων θα ανέβαινε το πλήθος των κλάσεων και θα έπρεπε να ληφθούν περισσότερες από τριακόσια πενήντα φωτογραφίες για να εξάγει το δίκτυο ορθά αποτελέσματα.

3.2 Συμπεράσματα κεφαλαίου

Τα συνελικτικά δίκτυα πραγματοποιούν επιτυχημένα ταυτοποιήσεις προτύπων. Χρησιμοποιούνται ειδικά για αναγνώριση προτύπων μέσω εικόνων ή μέσω frame που έχουν λάβει από κάποιο βίντεο. Για την αποτελεσματικότητα του δίκτυο ώστε να εξάγει υψηλά ποσοστά ακριβείας πρέπει να δίνονται πολλά και ποικίλα δείγματα. Στην εν λόγω περίπτωση ταυτοποίησε ορθώς εικοσιοκτώ διαφορετικές φωτογραφίες με μεγάλα ποσοστά ακριβείας. Η αποτελεσματικότητα του είναι έγκυρη και σε περιπτώσεις όπου τα άτομα φορούν γυαλιά μυωπίας ή ηλίου, φορώντας μάσκα ή έχοντας καπέλου, δηλαδή όταν έχουν καλυφθεί κάποια από τα χαρακτηριστικά του προσώπου τους. Το AlexNet αποδίδει μέγιστα.

4 ΚΕΦΑΛΑΙΟ 4ο: Συμπεράσματα

Αλγόριθμος έννοια που δημιουργήθηκε από μαθηματικούς για μαθηματικούς και με την πάροδο των χρόνων έγινε αναπόσπαστο κομμάτι της καθημερινότητας. Θα μπορούσε να χαρακτηριστεί σαν το «θεμέλιο» της ανάπτυξης λογισμικού, ένα ισχυρό εργαλείο για τους προγραμματιστές, αφού με τα κατάλληλα βήματα επιλύουν προβλήματα κάθε πολυπλοκότητας.

Βρίσκονται παντού στα έξυπνα κινητά (*smart phones*), στα βιντεοπαιχνίδια (*video games*), στα συστήματα των αυτοκινήτων, στις διαδικτυακές συναλλαγές, στη συμπίεση αρχείων, στην εκκίνηση του υπολογιστή όπου εκεί υπάρχει το λογισμικό -το οποίο είναι η υπολογιστική μετάφραση ενός αλγόριθμου- είναι υπεύθυνο για τον έλεγχο όλων των στοιχείων του υπολογιστή ώστε να διαπιστωθεί η εύρυθμη λειτουργία και μετέπειτα να αναζητηθεί το λειτουργικό σύστημα (*operating system*) -Microsoft windows,Unix- στο δίσκο για να φορτωθεί. Υπάρχουν αναρίθμητοι αλγόριθμοι διαφορετικής ιδιότητας και δυσκολίας. Τα πάντα στον υπολογιστή μπορούν να μεταφραστούν σε αλγόριθμο χωρίς υπερβολή.

Οι αλγόριθμοι αποτελούν ακούραστο σύμμαχο της ανθρωπότητας, αφού επεξεργάζονται χιλιάδες δεδομένα σε ελάχιστο χρόνο, παρακολουθώντας και διαχωρίζοντας άλλα δεδομένα συγχρόνως. Ανταποκρίνονται γρήγορα και δεν λειτουργούν με βάση τα συναισθήματα, κάτι το οποίο τους επιτρέπει να επιτυγχάνουν καλύτερες επιδόσεις και να μειώνουν το ρίσκο ύπαρξης λάθους. Ένας τέτοιου είδους αλγόριθμος δημιουργήθηκε στο κεφάλαιο τρία. Ο αλγόριθμος μπορεί να αναγνωρίσει οκτώ άτομα. Στην σημερινή κοινωνία η αναγνώριση προτύπων βρίσκεται στην παλάμη των χεριών των ανθρώπων κυριολεκτικά, κάνοντας την κοινωνία πιο ασφαλή, βολική και δίνοντας της το έναυσμα για περεταίρω εξέλιξη. Μετεξελίσσοντας τον θα μπορούσε να μετατραπεί και να χρησιμοποιηθεί από τα άτομα χωρίς όραση ώστε να τα βοηθάει να ειδοποιούνται για τα συναισθήματα του συνομιλητή τους εξετάζοντας κάθε φορά την έκφραση του και μετέπειτα να ειδοποιεί τον χρήστη μέσω ενός ηχητικού ή μέσω δόνησης για το συναίσθημα. Επίσης, είναι εξαιρετικό εργαλείο για παροχή ασφάλειας όπως για την διασφάλιση προσωπικών δεδομένων στο κινητό ή ακόμα και σε χώρους όπου η πρόσβαση πρέπει να είναι επιλεγμένη -εργαστήριο- και μόνο σε εξουσιοδοτημένα άτομα να δίνεται η δυνατότητα εισόδου. Επίσης για την εύρεση αγνοούμενων ατόμων. Ταυτόχρονα, θα μπορούσε να εφαρμοστεί και ως σύστημα ασφάλειας στα αυτοκίνητα, ταυτοποιώντας τους ιδιοκτήτες του αυτοκινήτου και μόνο τότε να ενεργοποιεί την μηχανή. Σε ακόμα έναν τομέα που θα μπορούσε να χρησιμοποιηθεί είναι στις ηλεκτρονικές συναλλαγές επιτρέποντας μόνο μετά από ταυτοποίηση του χρήστη της ηλεκτρονικής κάρτας να εκτελέσει τις συναλλαγές του. Αυτοί είναι κάποιοι ενδεικτικοί τομείς που θα μπορούσε να χρησιμοποιηθεί ο εν λόγω αλγόριθμος του κεφαλαίου 3 με κάποιες μικρές μετατροπές.

Οι αλγόριθμοι ήρθαν για να μείνουν και προσαρμόζονται ανάλογα με την εποχή και τις ανάγκες των ανθρώπων. Τρανό παράδειγμα είναι η δημιουργία αλγορίθμων σχετικά με την πανδημία που χτύπησε το 2020 -έως και σήμερα που γράφεται η εν λόγω διπλωματική- τον κορωνοϊό. Η δημιουργία εφαρμογής που θα ιχνηλατεί τις επαφές μέσω εφαρμογής ενημερώνοντας τον κόσμο για το αν βρέθηκαν σε κοντινή απόσταση με κάποιο κρούσμα τις προηγούμενες δεκατέσσερις ημέρες είναι ήδη εν εξελίξει. Πρόκειται για εφαρμογή εντοπισμού (*tracing app*), η οποία θα είναι διαθέσιμη σε smartphone λογισμικού IOS ή Android και θα λειτουργεί αποκλειστικά με την τεχνολογία Bluetooth.[37]

Επιπροσθέτως, ερευνητές του MIT έχουν ξεκινήσει την διαδικασία με τη βοήθεια στατιστικών αλγορίθμων ώστε να εντοπιστούν φάρμακα που είναι ήδη διαθέσιμα στην αγορά για καταπολέμηση του κορωνοϊού σε ηλικιωμένους ασθενείς. Η έρευνα αυτή βασίζεται στην μηχανική μάθηση και ονομάζεται αυτόματος κωδικοποιητής.[38] Παραμένοντας στο χώρο της υγείας άλλη ομάδα του MIT και συγκεκριμένα η ομάδα του εργαστηρίου «*Επιστήμης Υπολογιστών και Τεχνητής Νοημοσύνης*» σε συνεργασία με την κλινική *Jameel* δημιούργησαν ένα σύστημα μάθησης που θα προβλέπει τον κινδύνου καρκίνου χρησιμοποιώντας μια μαστογραφία του ασθενούς. Ο αλγόριθμος ονομάζεται *«Mirai»* καταγράφει τις απαιτήσεις της μοντελοποίησης κινδύνου, δημιουργεί στατιστικά λαμβάνοντας πληροφορίες αναφορικά με την ηλικία, το φύλλο, το οικογενειακό ιστορικό προβλέποντας συγχρόνως τον κίνδυνο σε όλα τα χρονικά σημεία χρησιμοποιώντας ένα εργαλείο που ονομάζεται «στρώμα πρόσθετου κινδύνου» για το αν ένας ασθενής έχει κίνδυνο να νοσήσει. Το σύνολο των εκπαιδευτικών δεδομένων που διατέθηκε ήταν 200.000 εξετάσεις. Χρησιμοποιείται ήδη στο Γενικό Νοσοκομείο της Μασαχουσέτης.[41]

Ένας άλλος τομέας που βελτιώνεται και εξελίσσεται εκπλήσσοντας με τις αλλαγές που πραγματοποιεί είναι ο κλάδος της αυτοκινητοβιομηχανίας. Αποτελεί σκοπό το 2030 να είναι πλήρως αυτοματοποιημένα τα αυτοκίνητα, *βαθμού 5* δηλαδή. Συγκεκριμένα η αυτονομία κατατάσσεται σε 6 επίπεδα. Το *επίπεδο 0* προειδοποιεί τον οδηγό με ηχητική ή οπτική προειδοποίηση, αλλά δεν επεμβαίνει. Στο *επίπεδο 1* ο οδηγός έχει τον πλήρη έλεγχο στην οδήγηση και τα συστήματα λειτουργούν εντελώς βοηθητικά, παραδείγματος χάρη ειδοποιεί τον οδηγό αν δεν έχει προειδοποιήσει με φλας τους υπόλοιπους οδηγούς με για την αλλαγή λωρίδας *(lane assist)*. Στο *επίπεδο 2* το αυτοκίνητο εξοπλίζεται με περισσότερα είδη αυτόματων συστημάτων. Το ραντάρ, οι κάμερες και η δυνατότητα επικοινωνίας με άλλα οχημάτων μέσω δορυφόρου ανήκουν στο επίπεδο 2. Στο *επίπεδο 3* το όχημα λαμβάνει επιπρόσθετες πρωτοβουλίες εν ώρα οδήγησης, όπως το αυτόματο φρενάρισμα για αποφυγή σύγκρουσης και το αυτόματο παρκάρισμα. Στο *επίπεδο 4* υπάρχει η πλήρης αυτονομία του αυτοκινήτου για μικρό εύρος διαδρομών. Στο *επίπεδο 5* γίνεται εξολοκλήρου η χρήση της πλήρους αυτονομίας σε όλο το δίκτυο.[39] Η πρώτη ελληνική προσπάθεια

αυτόνομων αυτοκίνητων έγινε το 2013 στη περιοχή των Τρικάλων και αφορούσε το μικρό αυτόνομο λεωφορείο το οποίο διέθετε από 9 έως 11 θέσεις. Κινούνταν αυτόνομα, με χαμηλή ταχύτητα των 20 χλμ/ώρα, διανύοντας 2,4 χλμ με οκτώ στάσεις. Συγχρόνως ομάδα του MIT επενδύει στον τομές αυτόματης οδήγησης δημιουργώντας την MIT Driverless το 2018 να κατασκευάσει ένα αγωνιστικό αυτοκίνητο με ταχύτητες έως και 120 μίλια την ώρα. Συμπεριλαμβάνει καινοτόμους αλγόριθμους και συστήματα που βασίζονται στη μηχανική μάθηση. Όσο πιο γρήγορα εκτελούνται οι αλγόριθμοι τόσο ασφαλέστερα θα κινείται το αυτοκίνητο. Συνάμα υπολογίζει τις πιθανές διαδρομές και στη συνέχεια επιλέγει την καλύτερη που πρέπει να ακολουθήσει το αυτοκίνητο με βάση το συνολικό χρόνο και τα εμπόδια που μπορεί να υπάρξουν.[40]

Ολοκληρώνοντας, οι αλγόριθμοι βρίσκονται παντού εξάπτοντας το ενδιαφέρον για εξερεύνηση και επιπλέον μάθηση. Αυτό που πρέπει να υπογραμμιστεί, είναι το τι μπορεί να συμβεί στη περίπτωση που ο αλγόριθμος κάνει λάθος. Σύμφωνα με ανάλυση που είχε κάνει το 2017 το Pew Research Center, μια λανθασμένη χρήση του αλγόριθμου μπορεί να δώσει τη δυνατότητα σε κάποια κυβέρνηση είτε σε μεγάλες εταιρείες να αποκτήσουν τον έλεγχο της ζωής των χρηστών. Σύμφωνα με την καθηγήτρια Meredith Broussard, για περισσότερα από 20 χρόνια υπήρχε η άποψη ότι οι αλγόριθμοι είναι καλύτεροι από τον άνθρωπο, όμως κάτι τέτοιο δεν υφίσταται. Πλέον υπάρχει μια νέα κατηγορία επαγγελματιών που εργάζονται στο να προβλέπουν και να αποκλείουν τυχόν τεχνολογικά λάθη. Στόχος είναι η διαφάνεια και η ακρίβεια του λογισμικού. Ολοένα και περισσότερες εταιρείες επικεντρώνονται σε αυτόν τον τομέα, όπως για παράδειγμα η Deloitte, που επενδύει στον περιορισμό προβλημάτων που ελλοχεύουν προκαλούμενα από αλγόριθμους.[42]

Βιβλιογραφία – Αναφορές - Διαδικτυακές Πηγές

1. *Αλγόριθμος—Βικιπαίδεια*. (n.d.). Retrieved from https://el.wikipedia.org/wiki/%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CF%82
2. John MacCormick. (2012). *Nine algorithms that changed the future: The ingenious ideas that drive today's computers* (Vol. 49). Retrieved from http://choicereviews.org/review/10.5860/CHOICE.49-5106
3. How Search Engines Work: Crawling, Indexing, and Ranking | Beginner's Guide to SEO - Moz. (n.d.). Retrieved May 31, 2021, from https://moz.com/beginners-guide-to-seo/how-search-engines-operate
4. SEO, M. the S. (2021, January 7). 210 Παράγοντες κατάταξης Google (Αναλυτική λίστα—2021). Retrieved May 31, 2021, from Mind The SEO website: https://mindtheseo.com/paragontes-katataksis-google/
5. The Anatomy of a Search Engine. (n.d.). Retrieved May 31, 2021, from http://infolab.stanford.edu/~backrub/google.html
6. Everything You Need to Know about Google PageRank in 2021. (n.d.). Retrieved May 31, 2021, from https://www.semrush.com/blog/pagerank/
7. Google PageRank is NOT Dead: Why It Still Matters. (n.d.). Retrieved May 31, 2021, from https://ahrefs.com/blog/google-pagerank/
8. Why we shouldn't forget about PageRank in 2019. (n.d.). Retrieved May 31, 2021, from https://searchengineland.com/why-we-shouldnt-forget-about-pagerank-in-2019-315443
9. How we fought Search spam on Google in 2020. (n.d.). Retrieved May 31, 2021, from Google Developers website: https://developers.google.com/search/blog/2021/04/how-we-fought-search-spam-2020
10. How we fought Search spam on Google—Webspam Report 2019. (n.d.). Retrieved May 31, 2021, from https://developers.google.com/search/blog/2020/06/how-we-fought-search-spam-on-google?hl=en
11. The Importance of AI Spam Filtering. (2019, June 21). Retrieved May 31, 2021, from Cii website: https://ciinc.com/the-importance-of-ai-spam-filtering/
12. This year in Search Spam—Webspam report 2018. (n.d.). Retrieved May 31, 2021, from https://developers.google.com/search/blog/2019/03/this-year-in-search-spam-webspam-report
13. *MpatsariMsc2006.pdf*. (n.d.). Retrieved from https://dspace.lib.uom.gr/bitstream/2159/2503/2/MpatsariMsc2006.pdf

14. Becchetti, L., Luca, Castillo, C., Carlos, Donato, D., Debora, … EITO-BRUN, R. (2008, February 1). *Web Spam Detection: Link-based and Content-based Techniques*.
15. Spam statistics: Spam e-mail traffic share 2019. (n.d.). Retrieved May 31, 2021, from Statista website: https://www.statista.com/statistics/420391/spam-email-traffic-share/
16. Κρυπτογραφία: Όλα όσα χρειάζεται να ξέρεις για να μην είσαι πια αρχάριος! - Frapress. (n.d.). Retrieved May 31, 2021, from https://frapress.gr/2016/12/kriptografia-ola-osa-chriazete-na-xeris-gia-na-min-ise-pia-archarios/
17. Κρυπτογραφία. (2021). In *Βικιπαίδεια*. Retrieved from https://el.wikipedia.org/w/index.php?title=%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%B1%CF%86%CE%AF%CE%B1&oldid=8626574
18. Τμήμα Εφαρμοσμένης Πληροφορικής Πανεπιστήμιο Μακεδονίας Θεσσαλονίκης. (2006, June). *Η ΕΠΙΣΤΗΜΗ ΤΗΣ ΚΡΥΠΤΟΓΡΑΦΙΑΣ ΚΑΙ Ο ΚΡΥΠΤΟΑΛΓΟΡΙΘΜΟΣ RSA*. ΠΑΣΧΑΛΗΣ Δ. ΜΠΑΤΣΑΡΗΣ. https://dspace.lib.uom.gr/bitstream/2159/2503/2/MpatsariMsc2006.pdf
19. L. (2016, March 21). *Τι είναι το ECC και γιατί πρέπει να το χρησιμοποιείτε*. LeaderTelecom. https://www.leaderssl.gr/articles/345-ecc
20. *STE_MHP_00038_Medium.pdf*. (n.d.). Retrieved from http://nestor.teipel.gr/xmlui/bitstream/handle/123456789/13283/STE_MHP_00038_Medium.pdf?sequence=1
21. Cryptographic hash function. (2021). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Cryptographic_hash_function&oldid=1021301526
22. Alimohammadi, M., & Pouyan, A. A. (n.d.). *Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET*.
23. Pamuditha, I. (2020, May 12). Hamming Code Generation & Correction (with explanations using C codes). Retrieved May 31, 2021, from Medium website: https://medium.com/swlh/hamming-code-generation-correction-with-explanations-using-c-codes-38e700493280
24. Hamming Code: Construction, encoding & decoding. Retrieved May 31, 2021, from GaussianWaves website: https://www.gaussianwaves.com/2008/05/hamming-codes-how-it-works/
25. QR code. (2021). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=QR_code&oldid=1025335320
26. Scientific Foresight Unit (STOA), within the Directorate-General for Parliamentary Research Services (EPRS) of the Secretariat of the European Parliament, & Philip Boucher. (2020, June). *Artificial intelligence: How does it work, why does it matter, and what can we do about it?* Scientific Foresight Unit (STOA).

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf

27. S. (2020, December 18). *An Overview of Neural Approach on Pattern Recognition*. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2020/12/an-overview-of-neural-approach-on-pattern-recognition/
28. Συμπίεση Δεδομένων: Τι Είναι και Πώς Λειτουργεί. (2016, June 16). Retrieved May 31, 2021, from PCsteps.gr website: https://www.pcsteps.gr/104540-συμπίεση-δεδομένων-πώς-λειτουργεί/
29. Τι είναι το Mp3, Πώς λειτουργεί, και Πώς Δημιουργήθηκε. (2016, April 4). Retrieved May 31, 2021, from PCsteps.gr website: https://www.pcsteps.gr/98136-τι-είναι-το-mp3-πώς-λειτουργεί/
30. Database. In *Wikipedia*. https://en.wikipedia.org/wiki/Database
31. Menezes, A. J., Oorschot, P. V. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography (Discrete Mathematics and Its Applications)* (1st ed.). CRC Press. https://doc.lagout.org/network/3_Cryptography/CRC%20Press%20-%20Handbook%20of%20applied%20Cryptography.pdf
32. *Chatzic_digital.pdf*. (n.d.). Retrieved from http://dspace.lib.ntua.gr:8080/xmlui/bitstream/handle/123456789/38783/chatzic_digital.pdf?sequence=1&isAllowed=y
33. What are Digital Signatures and How do They Work? | by Code Notary | FAUN. (n.d.). Retrieved May 31, 2021, from https://faun.pub/what-are-digital-signatures-and-how-do-they-work-195b18c4f42c
34. What is a Digital Signature? (n.d.). Retrieved May 31, 2021, from Search Security website: https://searchsecurity.techtarget.com/definition/digital-signature
35. A. (2017, February 24). *Deep Learning: Transfer Learning in 10 lines of MATLAB Code*. File Exchange Pick of the Week. https://blogs.mathworks.com/pick/2017/02/24/deep-learning-transfer-learning-in-10-lines-of-matlab-code/
36. ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ - ΤΜΗΜΑ ΦΥΣΙΚΗΣ - Δ.Π.Μ.Σ. (2016). *Συνελικτικά Ναυρωνικά Δίκτυα Στην Υπολογιστική Όραση*. ΠΑΠΑΔΟΠΟΥΛΟΣ ΑΘΑΝΑΣΙΟΣ. https://nemertes.lis.upatras.gr/jspui/bitstream/10889/9623/3/PapadopoulosAth%28phys%29.pdf
37. Tracing app: Η εφαρμογή για κινητά που θα ιχνηλατεί τον κορονοϊό έρχεται και στην Ελλάδα - Πώς θα λειτουργεί. (n.d.). Retrieved May 31, 2021, from http://www.enikonomia.gr/technology/245505,tracing-app-i-efarmogi-gia-kinita-pou-tha-ichnilatei-ton-koronoio.html
38. A machine-learning approach to finding treatment options for Covid-19. (n.d.). Retrieved May 31, 2021, from MIT News | Massachusetts Institute of Technology website: https://news.mit.edu/2021/machine-learning-treatment-covid-19-0216

39. Όσα πρέπει να ξέρετε για τα αυτόνομα αυτοκίνητα. (2020, May 20). Retrieved May 31, 2021, from Spotawheel Blog website: https://blog.spotawheel.gr/osa-prepei-na-kserete-gia-ta-autonoma-au/
40. Driving on the cutting edge of autonomous vehicle tech. (n.d.). Retrieved May 31, 2021, from MIT News | Massachusetts Institute of Technology website: https://news.mit.edu/2021/driving-cutting-edge-autonomous-vehicle-tech-mit-driverless-0225
41. Robust artificial intelligence tools to predict future cancer. (n.d.). Retrieved May 31, 2021, from MIT News | Massachusetts Institute of Technology website: https://news.mit.edu/2021/robust-artificial-intelligence-tools-predict-future-cancer-0128
42. Τι μπορεί να συμβεί όταν ένας αλγόριθμος κάνει λάθος; | LiFO. (2020, March 4). Retrieved May 31, 2021, from https://www.lifo.gr/now/tech-science/ti-mporei-na-symbei-otan-enas-algorithmos-kanei-lathos
43. *Face Detection and Tracking Using CAMShift - MATLAB & Simulink - MathWorks Switzerland*. (n.d.). MathWorks. Retrieved June 21, 2021, from https://ch.mathworks.com/help/vision/ug/face-detection-and-tracking-using-camshift.html
44. *Options for training deep learning neural network - MATLAB trainingOptions - MathWorks Switzerland*. (n.d.). MathWorks. Retrieved June 21, 2021, from https://ch.mathworks.com/help/deeplearning/ref/trainingoptions.html
45. MacCormick John. (2016). *Εννέα αλγόριθμοι που άλλαξαν το μέλλον*. Πανεπιστημιακές Εκδόσεις Κρήτης.

Παράρτημα Α

%κώδικας για την δημιουργία βάσης δεδομένων-λήψη εικόνων

```
clear all; close all; clc;
image=webcam;
faceDetector=vision.CascadeObjectDetector;
c=350; num_of_image=0;
for num_of_image=0:c
    i=image.snapshot;
    bboxes=step(faceDetector,i);
    if(sum(sum(bboxes))~=0)
    if(num_of_image>=c)
        break;
    else
    new_i=imcrop(i,bboxes(1,:));
    new_i=imresize(new_i,[227 227]);
    file=strcat(num2str(num_of_image),'.jpg');
    imwrite(new_i,file);
    imshow(new_i);
    drawnow;
    end
    else
        imshow(i);
        drawnow;
    end
end
```

%κώδικας για την εκπαίδευση του δικτύου & την αποθήκευση του

```
clc;close all;
cnn=alexnet;
layers=cnn.Layers;
layers(23)=fullyConnectedLayer(8);
layers(25)=classificationLayer
images=imageDatastore('collect', 'IncludeSubfolders', true,...
    'LabelSource', 'foldernames');
opts=trainingOptions('sgdm','MiniBatchSize',64,'MaxEpochs',20,...
    'InitialLearnRate',0.001);
Cnetwork2=trainNetwork(images,layers,opts);
save ('cnn.mat','Cnetwork2');
```

%εφαρμογή κώδικα

```
clc; close all; clear all;
c=webcam;
loaded_Network = load('cnn.mat');
net = loaded_Network.Cnetwork2;
faceDetector=vision.CascadeObjectDetector;
while true
    e=c.snapshot;
    bboxes =step(faceDetector,e);
    if(sum(sum(bboxes))~=0)
    es=imcrop(e,bboxes(1,:));
    es=imresize(es,[227 227]);
    [label, Probability] = classify(net, es);
    image(e);
    title({char(label), num2str(max(Probability)*100, 2)});
    drawnow;
    else
        image(e);
        title('Not a match');
```

```
    end
end
```