ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Ανίχνευση Πλαστογραφίας Υπογραφών μέσω Μηχανικής Μάθησης

Του φοιτητή

Στεργίου Κυριάκος

Αρ. Μητρώου: 164841

Επιβλέπων

Στέφανος Ουγιάρογλου

Επίκουρος Καθηγητής

10 Σεπτεμβρίου 2024

Τίτλος Δ.Ε.: Ανίχνευση Πλαστογραφίας Υπογραφών μέσω Μηχανικής Μάθησης
Κωδικός Δ.Ε.: 24177
Ονοματεπώνυμο φοιτητή: Στεργίου Κυριάκος
SOνοματεπώνυμο εισηγητή: Ουγιάρογλου Στέφανος
Ημερομηνία ανάληψης Δ.Ε.: 29-03-2024
Ημερομηνία περάτωσης Δ.Ε.: 10-09-2024

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Αφιέρωση

Αυτή η εργασία αφιερώνεται στον καθηγητή μου, Στέφανο Ουγιάρογλου , για την ανεκτίμητη καθοδήγησή τους και την ευκαιρία να συνεργαστώ μαζί του σε αυτήν την μελέτη.

Περίληψη

Η παρούσα πτυχιακή εργασία παρουσιάζει μια ολοκληρωμένη προσέγγιση για την ανίχνευση πλαστογραφίας υπογραφών με την ενσωμάτωση τόσο της βαθιάς μάθησης όσο και των παραδοσιακών τεχνικών μηχανικής μάθησης.

Η βασική συνεισφορά έγκειται στο συνδυασμό των δυνατοτήτων εξαγωγής χαρακτηριστικών των προ-εκπαιδευμένων μοντέλων βαθιάς μάθησης, όπως τα VGG16, DenseNet121, MobileNetV2 και EfficientNetV2S, με τη δύναμη ταξινόμησης παραδοσιακών αλγορίθμων όπως οι Μηχανές Διανυσμάτων Υποστήριξης (SVM), οι K-Nearest Neighbors (KNN), τα Δέντρα Αποφάσεων, τα Τυχαία Δάση και τα Naive Bayes. Αποδείξαμε με επιτυχία ότι αυτή η υβριδική προσέγγιση όχι μόνο βελτιώνει την ακρίβεια στον εντοπισμό πλαστών υπογραφών αλλά και την υπολογιστική αποδοτικότητα.

Η διαδικασία ξεκινά με την προεπεξεργασία της εικόνας με τη χρήση του OpenCV, ακολουθούμενη από την εξαγωγή χαρακτηριστικών με τη χρήση μοντέλων βαθιάς μάθησης που υλοποιούνται σε TensorFlow και Keras. Τα εξαγόμενα χαρακτηριστικά στη συνέχεια τροφοδοτούνται σε ταξινομητές μηχανικής μάθησης που αναπτύσσονται με τη χρήση του Scikit-learn. Πραγματοποιήθηκε αυστηρή αξιολόγηση σε σύνολα δεδομένων υπογραφής και τα πειραματικά αποτελέσματα υπογραμμίζουν την αποτελεσματικότητα αυτού του υβριδικού συστήματος.

Επιπλέον, η παρούσα πτυχιακή εργασία διερευνά τις προκλήσεις που αντιμετωπίστηκαν κατά την υλοποίηση, συμπεριλαμβανομένης της μεταβλητότητας των συνόλων δεδομένων και της διαχείρισης της μνήμης, και εξετάζει τον τρόπο με τον οποίο αντιμετωπίστηκαν. Τα ευρήματα αναδεικνύουν τις σημαντικές δυνατότητες του συνδυασμού της βαθιάς μάθησης και της παραδοσιακής μηχανικής μάθησης σε εφαρμογές βιομετρικής ασφάλειας, όπως η επαλήθευση υπογραφών.

Abstract

This thesis presents a comprehensive approach to signature forgery detection by integrating both deep learning and traditional machine learning techniques. The core contribution lies in combining the feature extraction capabilities of pre-trained deep learning models, such as VGG16, DenseNet121, MobileNetV2, and EfficientNetV2S, with the classification power of traditional algorithms like Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Decision Trees, Random Forests, and Naive Bayes. We have successfully demonstrated that this hybrid approach not only improves accuracy in detecting forged signatures but also enhances computational efficiency. The process begins with image preprocessing using OpenCV, followed by feature extraction using deep learning models implemented in TensorFlow and Keras. The extracted features are then fed into machine learning classifiers developed using Scikit-learn. Rigorous evaluation was conducted on signature datasets, and the experimental results underscore the effectiveness of this hybrid system. Furthermore, this thesis explores the challenges encountered during implementation, including dataset variability and memory management, and discusses how they were addressed. The findings highlight the significant potential advantages of combining deep learning and traditional machine learning in biometric security applications such as signature verification.

Keywords : Signature Forgery Detection, Forged Signatures, Deep Learning, Machine Learning, Feature Extraction, Convolutional Neural Networks, Signature Verification, Hybrid Models

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κεφάλαιο 1

Εισαγωγή

1.1 Το πρόβλημα της πλαστογράφησης υπογραφών

Η πλαστογραφία υπογραφών αντιπροσωπεύει ένα σημαντικό και διαδεδομένο ζήτημα που επηρεάζει διάφορους τομείς, συμπεριλαμβανομένων των χρηματοπιστωτικών υπηρεσιών, των νομικών ιδρυμάτων και των κρατικών λειτουργιών. Παραδοσιακά, οι υπογραφές χρησιμεύουν ως βασική μέθοδος για τον έλεγχο της ταυτότητας των ατόμων και την επαλήθευση της συγκατάθεσης ή της πρόθεσής τους σε επίσημα έγγραφα. Ωστόσο, καθώς οι τεχνικές παραποίησης υπογραφών γίνονται όλο και πιο περίπλοκες, η ανάγκη για αξιόπιστες και ισχυρές μεθόδους ανίχνευσης έχει γίνει πιο επείγουσα[16].

Οι πλαστογραφίες υπογραφών μπορούν να συμβούν τόσο σε φυσική όσο και σε ψηφιακή μορφή, γεγονός που περιπλέκει τον εντοπισμό τους. Ενώ η φυσική πλαστογραφία περιλαμβάνει τη μίμηση του στυλ και των χαρακτηριστικών της γραφής ενός ατόμου, η ψηφιακή πλαστογραφία μπορεί να περιλαμβάνει την τροποποίηση ηλεκτρονικών υπογραφών ή τη δημιουργία εξ ολοκλήρου κατασκευασμένων υπογραφών χρησιμοποιώντας εργαλεία λογισμικού[17]. Οι οικονομικές συνέπειες μιας τέτοιας απάτης είναι τεράστιες, ιδιαίτερα σε τομείς όπως ο τραπεζικός κλάδος, όπου οι πλαστογραφίες μπορούν να οδηγήσουν σε κλοπή ταυτότητας, χρηματική απώλεια και νομικές διαφορές[17].

Οι μη αυτόματες μέθοδοι ανίχνευσης πλαστών υπογραφών, αν και αποτελεσματικές σε ορισμένες περιπτώσεις, είναι επιρρεπείς σε σφάλματα λόγω της υποκειμενικής φύσης της ανθρώπινης κρίσης. Επιπλέον, η μη αυτόματη επαλήθευση είναι συχνά αργή, καθιστώντας την αδύνατη για μεγάλης κλίμακας επεξεργασία εγγράφων. Ως εκ τούτου, η ανάγκη για αυτοματοποιημένα και αποτελεσματικά συστήματα επαλήθευσης υπογραφών γίνεται όλο και πιο επιτακτική τόσο σε περιβάλλοντα εκτός σύνδεσης όσο και σε διαδικτυακά περιβάλλοντα[18].

1.2 Αυτόματη ανίχνευση πλαστογραφίας υπογραφής

Η ανάπτυξη συστημάτων αυτόματης ανίχνευσης πλαστογραφίας υπογραφών προέκυψε ως απάντηση στους περιορισμούς της χειροκίνητης επαλήθευσης. Αυτά τα συστήματα χρησιμοποιούν προηγμένες τεχνικές μηχανικής μάθησης και βαθιάς εκμάθησης για την ανάλυση υπογραφών και τον εντοπισμό πλαστών με βάση τα μοναδικά χαρακτηριστικά τους. Με την ανάλυση και την επεξεργασία ενός τεράστιου αριθμού δεδομένων υπογραφών σε ένα κλάσμα του χρόνου που απαιτείται από τις μη αυτόματες μεθόδους, αυτά τα συστήματα παρέχουν μια επεκτάσιμη και αξιόπιστη λύση για τον εντοπισμό πλαστών υπογραφών.
Οι μέθοδοι αυτόματης ανίχνευσης μπορούν γενικά να ταξινομηθούν σε δύο κατηγορίες: στατικές (εκτός σύνδεσης) και δυναμικές (online)[16]. Η στατική επαλήθευση περιλαμβάνει την ανάλυση μιας ψηφιοποιημένης εικόνας μιας υπογραφής, εστιάζοντας σε οπτικές πτυχές όπως το σχήμα, το πάχος της γραμμής και η σειρά διαδρομής. Αντίθετα, η δυναμική επαλήθευση χρησιμοποιεί βιομετρικά δεδομένα που συλλέγονται κατά τη διαδικασία υπογραφής, όπως η πίεση που ασκείται από το στυλό, η ταχύτητα γραφής και η γωνία της γραφίδας[17]. Η δυναμική επαλήθευση είναι ιδιαίτερα αποτελεσματική σε ψηφιακά περιβάλλοντα, όπου οι υπογραφές συλλέγονται μέσω συσκευών όπως ψηφιακά tablet και γραφίδες.
Οι πρόσφατες εξελίξεις στη βαθιά μάθηση έχουν βελτιώσει περαιτέρω την ακρίβεια των αυτόματων συστημάτων επαλήθευσης υπογραφών. Τα συνελικτικά νευρωνικά δίκτυα (CNN), ειδικότερα, έχουν δείξει μεγάλη υπόσχεση στην ανίχνευση πλαστών, εξάγοντας πολύπλοκα χαρακτηριστικά υψηλού επιπέδου από εικόνες υπογραφής[16][18]. Προεκπαιδευμένα μοντέλα όπως τα VGG, MobileNet, EfficientNet και DenseNet, βελτιωμένα για εργασίες επαλήθευσης υπογραφής, έχουν επιτύχει υψηλά επίπεδα ακρίβειας στη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών.

1.3 Κίνητρο

Το κίνητρο πίσω από αυτήν την έρευνα καθοδηγείται από την ανάγκη ενίσχυσης της ασφάλειας και της ακεραιότητας των διαδικασιών που βασίζονται στην επαλήθευση της υπογραφής. Σε μια εποχή όπου οι ψηφιακές συναλλαγές γίνονται κανόνας, η απειλή που ενέχει η πλαστογραφία υπογραφών έχει κλιμακωθεί. Οι τρέχουσες μέθοδοι για τον εντοπισμό πλαστών υπογραφών είναι ανεπαρκείς, ειδικά δεδομένης της ταχύτητας και της πολυπλοκότητας με την οποία μπορούν να πραγματοποιηθούν πλαστογραφίες χρησιμοποιώντας σύγχρονη τεχνολογία[18].
Η αυτόματη ανίχνευση πλαστογράφησης υπογραφής προσφέρει πολλά πλεονεκτήματα. Αρχικά, μειώνει την εξάρτηση από την ανθρώπινη τεχνογνωσία, η οποία είναι συχνά περιορισμένη σε διαθεσιμότητα και υπόκειται σε μεροληψία. Επιπλέον, παρέχει μια επεκτάσιμη λύση ικανή να χειριστεί μεγάλο όγκο υπογραφών σε πραγματικό χρόνο. Τέλος, αξιοποιώντας μο-

ντέλα μηχανικής μάθησης και βαθιάς μάθησης, αυτά τα συστήματα μπορούν να βελτιώνουν συνεχώς τις ικανότητές τους ανίχνευσης καθώς εκτίθενται σε περισσότερα δεδομένα, καθιστώντας τα προσαρμόσιμα σε εξελισσόμενες τεχνικές πλαστογραφίας[17].
Επιπλέον, τα αυτόματα συστήματα είναι απαραίτητα για τη διασφάλιση της συμμόρφωσης με τα νομικά και ρυθμιστικά πρότυπα, ιδιαίτερα σε βιομηχανίες όπου η γνησιότητα των υπογραφών είναι ζωτικής σημασίας. Για παράδειγμα, στους τομείς των τραπεζών, της υγειονομικής περίθαλψης και της κυβέρνησης, τα αυτόματα συστήματα μπορούν να βοηθήσουν στην πρόληψη της απάτης και να διασφαλίσουν ότι τα έγγραφα είναι νόμιμα[18].

1.4 Συνεισφορά

Αυτή η πτυχιακή εργασία συμβάλλει στον αυξανόμενο όγκο έρευνας στον τομέα της ανίχνευσης πλαστογραφίας υπογραφών διερευνώντας, συνδυάζοντας και συγκρίνοντας μια ποικιλία μοντέλων μηχανικής μάθησης και βαθιάς μάθησης. Οι κύριες συνεισφορές αυτής της εργασίας περιλαμβάνουν:

Υλοποίηση Μοντέλου
Η πτυχιακή εργασία εφαρμόζει μια σειρά μοντέλων μηχανικής μάθησης και βαθιάς μάθησης, συμπεριλαμβανομένων κλασσικών αλγορίθμων όπως Support Vector Machines (SVM), K-Nearest Neighbors (KNN), LogisticRegression (LR), DecisionTrees, Random Forests και NaiveBayes, καθώς και προηγμένα συνελικτικά νευρωνικά δίκτυα όπως το VGG19, DenseNet, MobileNet και EfficientNet[16][18].

Σύγκριση απόδοσης
Πραγματοποιείται λεπτομερής σύγκριση της απόδοσης αυτών των μοντέλων, εστιάζοντας σε βασικές μετρήσεις όπως η ακρίβεια (accuracy), η ευστοχία (presicion), η ανάκληση (recall), η βαθμολογία F1(F1-score) και η περιοχή κάτω από την καμπύλη (AUC). Αυτή η ανάλυση παρέχει πληροφορίες για τα πλεονεκτήματα και τις αδυναμίες κάθε προσέγγισης[18].

Προεκπαιδευμένη χρήση CNN
Η εργασία αξιοποιεί προεκπαιδευμένα CNN για μεταφορά μάθησης, αποδεικνύοντας την αποτελεσματικότητά τους στη βελτίωση της απόδοσης επαλήθευσης υπογραφής[16]. Ακόμη, δείχνει πώς η λεπτομερής ρύθμιση αυτών των μοντέλων σε σύνολα δεδομένων υπογραφών μπορεί να βελτιώσει σημαντικά την ακρίβεια ανίχνευσης.

Πειραματική αξιολόγηση
Εκτεταμένα πειράματα πραγματοποιούνται σε ευρέως αποδεκτά σύνολα δεδομένων υπογραφών για την αξιολόγηση της απόδοσης των μοντέλων. Οι πίνακες σύγχυσης(confusion matrix)

και άλλες απεικονίσεις χρησιμοποιούνται για να απεικονίσουν την ικανότητα των μοντέλων να διακρίνουν μεταξύ γνήσιων και πλαστών υπογραφών[17].

Πληροφορίες που βασίζονται σε δεδομένα
Η πτυχιακή εργασία παρέχει επίσης πληροφορίες για το πώς διαφορετικές τεχνικές προεπεξεργασίας δεδομένων και αρχιτεκτονικές μοντέλων επηρεάζουν τη συνολική απόδοση των συστημάτων ανίχνευσης πλαστογραφίας υπογραφών.

1.5 Οργάνωση της εργασίας

Η δομή της παρούσας πτυχιακής εργασίας έχει ως εξής:

Κεφάλαιο 2 - Μοντέλα βαθιάς μάθησης
Αυτό το κεφάλαιο συζητά διάφορα μοντέλα βαθιάς μάθησης που χρησιμοποιούνται στον εντοπισμό πλαστογραφίας υπογραφών, με έμφαση στις αρχιτεκτονικές του CNN και στο ρόλο της μάθησης μεταφοράς στη βελτίωση της απόδοσης.

Κεφάλαιο 3 - Αλγόριθμοι μηχανικής μάθησης
Αυτό το κεφάλαιο διερευνά τους παραδοσιακούς αλγόριθμους μηχανικής μάθησης και τις εφαρμογές τους στον εντοπισμό πλαστογραφίας υπογραφών. Η αποτελεσματικότητα αυτών των μοντέλων συγκρίνεται με εκείνη των προσεγγίσεων βαθιάς μάθησης.

Κεφάλαιο 4 - Τεχνολογίες
Το κεφάλαιο παρέχει μια επισκόπηση των εργαλείων και των βιβλιοθηκών που χρησιμοποιούνται για την υλοποίηση των μοντέλων, συμπεριλαμβανομένων των TensorFlow, Keras και Python.

Κεφάλαιο 5 - Εφαρμογή μοντέλων ανίχνευσης πλαστογράφησης υπογραφών
Αυτό το κεφάλαιο περιγράφει τις λεπτομέρειες υλοποίησης των διαφόρων μοντέλων, συμπεριλαμβανομένης της προεπεξεργασίας δεδομένων, των αρχιτεκτονικών μοντέλων και των διαδικασιών εκπαίδευσης.

Κεφάλαιο 6 - Πειραματική μελέτη
Αυτό το κεφάλαιο παρουσιάζει τα αποτελέσματα των πειραματικών αξιολογήσεων, συμπεριλαμβανομένων των μετρήσεων απόδοσης και των απεικονίσεων. Τα ευρήματα συζητούνται λεπτομερώς, επισημαίνοντας τις πιο αποτελεσματικές προσεγγίσεις.

Κεφάλαιο 7 - Συμπεράσματα και μελλοντική έρευνα
Η πτυχιακή εργασία ολοκληρώνεται με μια περίληψη των βασικών ευρημάτων και προτείνει

τομείς για μελλοντική έρευνα στον τομέα της ανίχνευσης πλαστογραφίας υπογραφών.

Κεφάλαιο 2

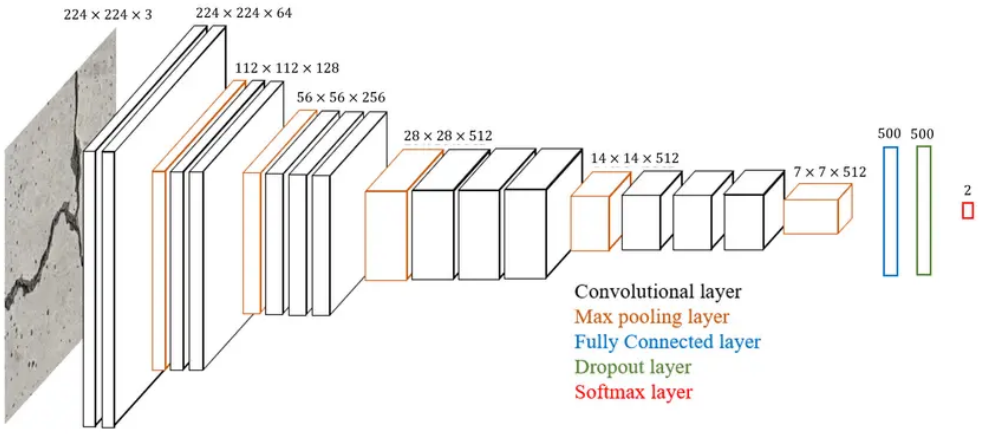
Μοντέλα Deep Learning

Η βαθιά μάθηση έχει φέρει επανάσταση στον τομέα της όρασης υπολογιστών και της αναγνώρισης εικόνων, προσφέροντας μοντέλα που μαθαίνουν αυτόματα σύνθετα χαρακτηριστικά από ακατέργαστα δεδομένα. Αυτές οι εξελίξεις ήταν καθοριστικής σημασίας για την αντιμετώπιση προκλήσεων όπως η ανίχνευση πλαστογράφησης υπογραφών, η οποία απαιτεί τη δυνατότητα διαφοροποίησης μεταξύ γνήσιων και παραποιημένων υπογραφών με βάση τις ανεπαίσθητες παραλλαγές στο σχήμα, την πίεση και τα μοτίβα της γραφίδας. Αυτό το κεφάλαιο διερευνά αρκετές αρχιτεκτονικές βαθιάς εκμάθησης που έχουν αποδειχθεί αποτελεσματικές στην επαλήθευση υπογραφών, εστιάζοντας συγκεκριμένα σε μοντέλα όπως τα VGG19, DenseNet, MobileNet, Xception και EfficientNet, μεταξύ άλλων. Επιπλέον, περιγράφει λεπτομερώς τις αρχιτεκτονικές βαθιάς μάθησης που χρησιμοποιούνται στο σύστημά μας, συζητώντας τη σημασία τους στο έργο της αναγνώρισης υπογραφών και εξηγώντας γιατί επιλέχθηκαν για τη συγκεκριμένη εφαρμογή. Εξηγούμε επίσης πώς αυτά τα μοντέλα υποστηρίζουν τη διαδικασία εξαγωγής χαρακτηριστικών, η οποία στη συνέχεια χρησιμοποιείται για τη βελτίωση της απόδοσης των παραδοσιακών ταξινομητών μηχανικής μάθησης.

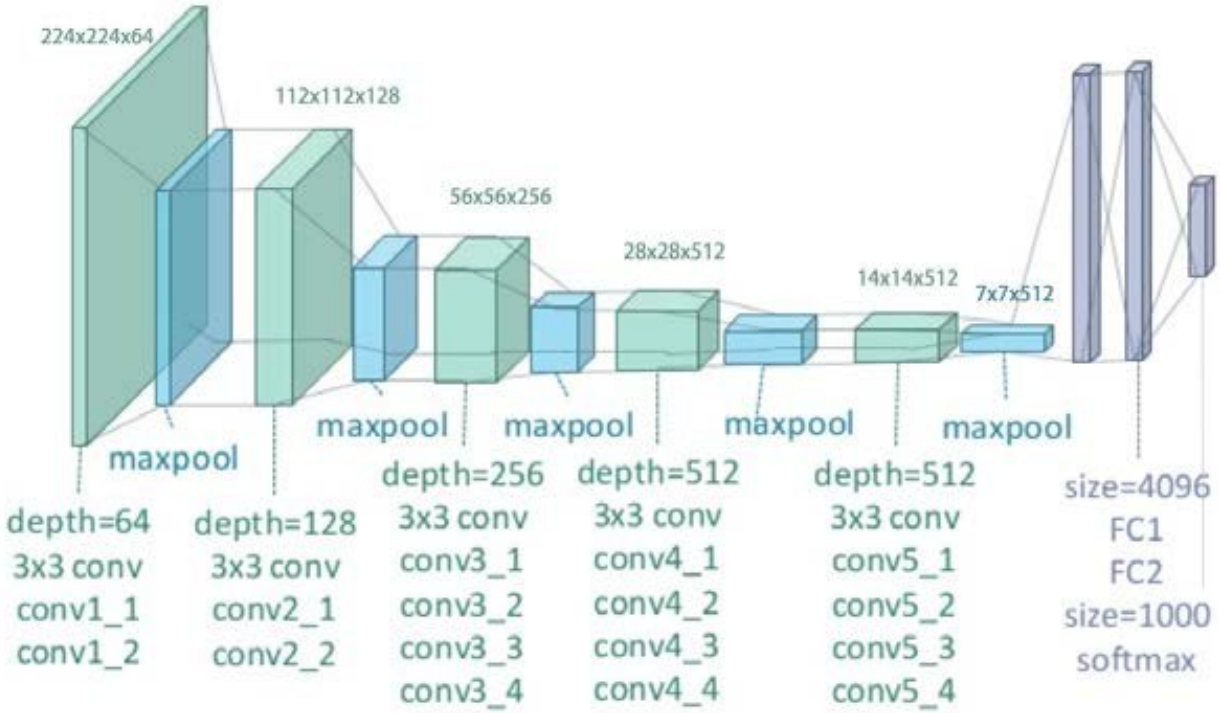
2.1 VGG19 και VGG16

Τα VGG19 και VGG16, που αναπτύχθηκαν από τους Simonyan και Zisserman (2014), είναι μερικά από τα πιο ευρέως χρησιμοποιούμενα συνελικτικά νευρωνικά δίκτυα (CNN) στην αναγνώριση εικόνων. Και οι δύο αρχιτεκτονικές αποτελούνται από μια σειρά συνελικτικών επιπέδων, με το VGG19 να περιλαμβάνει 19 επίπεδα και το VGG16 να περιλαμβάνει 16 επίπεδα. Αυτά τα μοντέλα χρησιμοποιούν μικρά φίλτρα 3x3 σε όλο το δίκτυο, τα οποία τους επιτρέπουν να καταγράφουν λεπτομέρειες στις εικόνες διατηρώντας τις χωρικές ιεραρχίες[19][20]. Η αρχιτεκτονική επιλέχθηκε για την απλότητα και την αποτελεσματικότητά τους στην εξαγωγή χαρακτηριστικών υψηλής ανάλυσης από εικόνες. Στην επαλήθευση υπογραφής, οι λεπτές διακυμάνσεις στη γραφή, την πίεση και τη γωνία είναι απαραίτητες για τη διάκριση με-

ταξύ γνήσιων και πλαστών υπογραφών. Ο σχεδιασμός του VGG, ο οποίος βασίζεται σε βαθιά στρώματα και ομοιόμορφα συνελικτικά φίλτρα, του επιτρέπει να μαθαίνει αποτελεσματικά αυτά τα περίπλοκα μοτίβα. Με τη στοίβαξη στρωμάτων συνέλιξης ακολουθούμενα από ομαδοποίηση στρωμάτων, το VGG δημιουργεί σταδιακά μια βαθύτερη κατανόηση της δομής της υπογραφής.



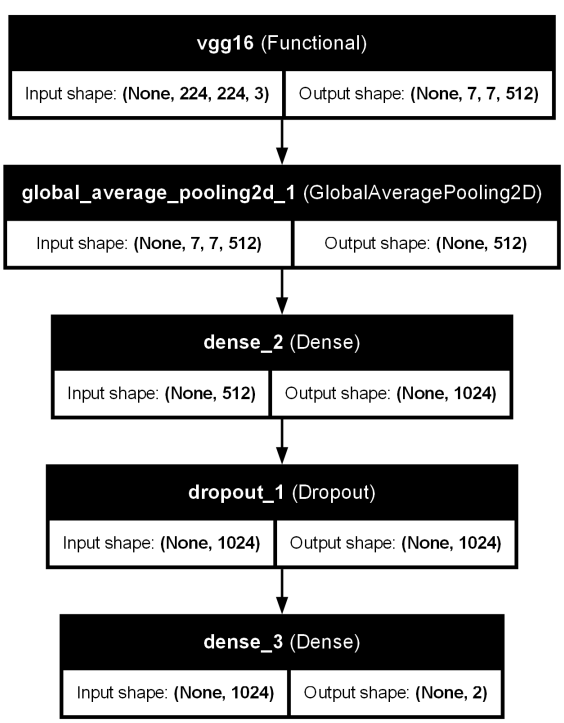
Σχήμα 2.1: Example : Architecture of the modified VGG16 model. Source: Choi et al. (2021)[1].



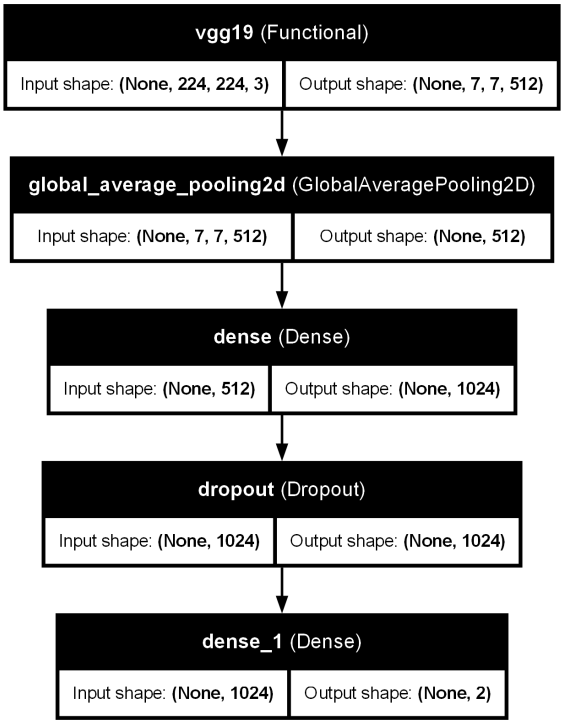
Σχήμα 2.2: Example : Illustration of the network architecture of VGG-19 model (conv means convolution, FC means fully connected). Source: Rasti et al. (2018)[2].

Τα μοντέλα VGG στην αναγνώριση εικόνας, και ιδιαίτερα στην επαλήθευση υπογραφών, έγκειται στην ικανότητά τους να μετατρέπουν πολύπλοκα οπτικά δεδομένα σε μια πιο αφηρημένη

και ενημερωτική αναπαράσταση χαρακτηριστικών. Για τον εντοπισμό πλαστογραφίας υπογραφών, αυτά τα αφηρημένα χαρακτηριστικά χρησιμοποιούνται στη συνέχεια για να διαφοροποιήσουν τις αυθεντικές υπογραφές από τις πλαστογραφίες, ακόμη και όταν οι διαφορές είναι λεπτές. Στην προσέγγισή μας, τα VGG19 και VGG16 χρησιμοποιούνται ως εξαγωγείς χαρακτηριστικών. Οι χάρτες χαρακτηριστικών που έχουν μάθει από αυτά τα μοντέλα μεταβιβάζονται σε παραδοσιακούς αλγόριθμους μηχανικής εκμάθησης για ταξινόμηση. Αυτός ο συνδυασμός αξιοποιεί τη δύναμη της βαθιάς μάθησης στην εξαγωγή χαρακτηριστικών με τις ισχυρές δυνατότητες ταξινόμησης των αλγορίθμων μηχανικής μάθησης όπως SVM και KNN.



(α′) Model visualization of VGG16.

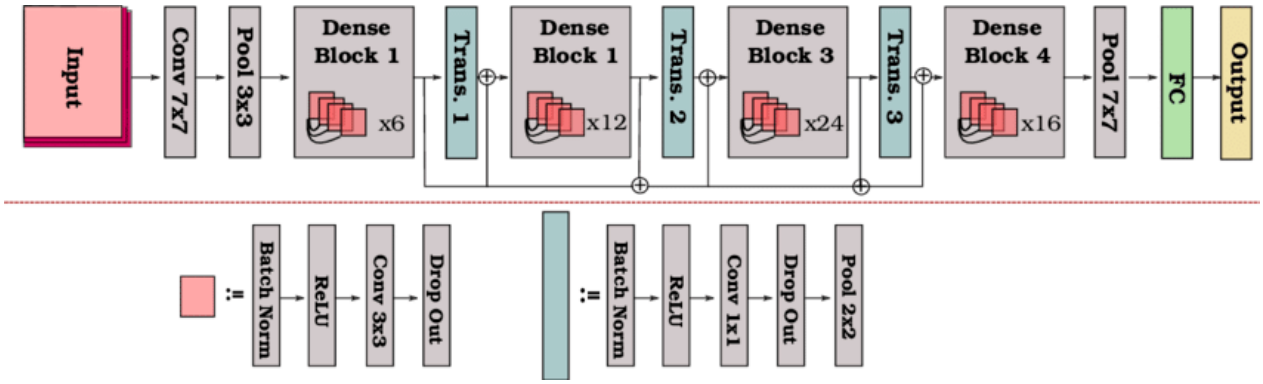


(β′) Model visualization of VGG19.

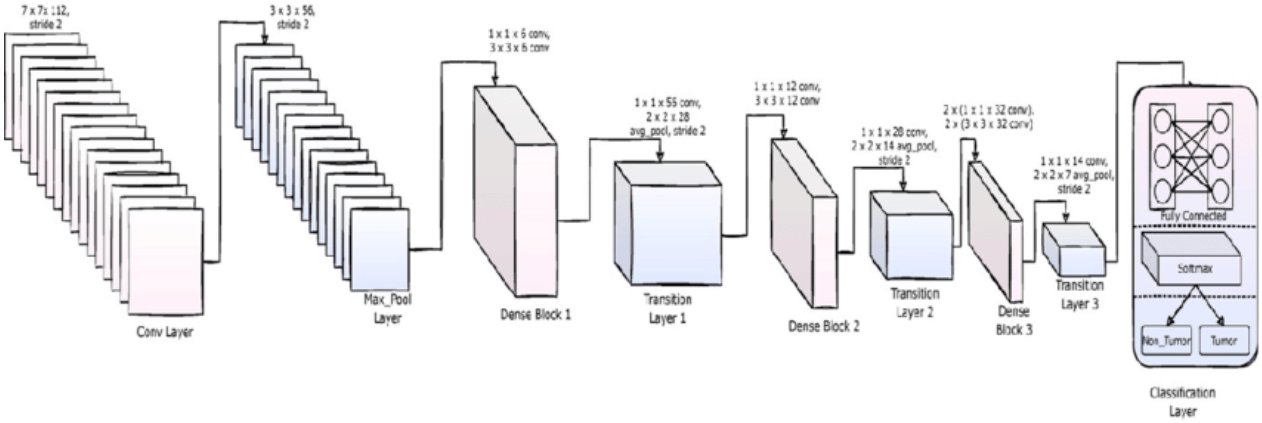
Σχήμα 2.3: Model Visualizations for VGG16 and VGG19.

2.2 DenseNet121, DenseNet169 και DenseNet201

Το Densely Connected Convolutional Networks (DenseNets), που εισήχθη από τους Huang et al. (2017), αντιπροσωπεύουν μια σημαντική πρόοδο στην αρχιτεκτονική του CNN. Το DenseNet χαρακτηρίζεται από το πυκνό μοτίβο συνδεσιμότητας του, όπου κάθε επίπεδο λαμβάνει είσοδο από όλα τα προηγούμενα επίπεδα. Αυτή η προσέγγιση διασφαλίζει τη μέγιστη ροή πληροφοριών μεταξύ των επιπέδων, ενθαρρύνει την επαναχρησιμοποίηση των χαρακτηριστικών και μετριάζει το πρόβλημα της εξαφάνισης της κλίσης που συναντάται συχνά στα βαθιά δίκτυα[20][19].

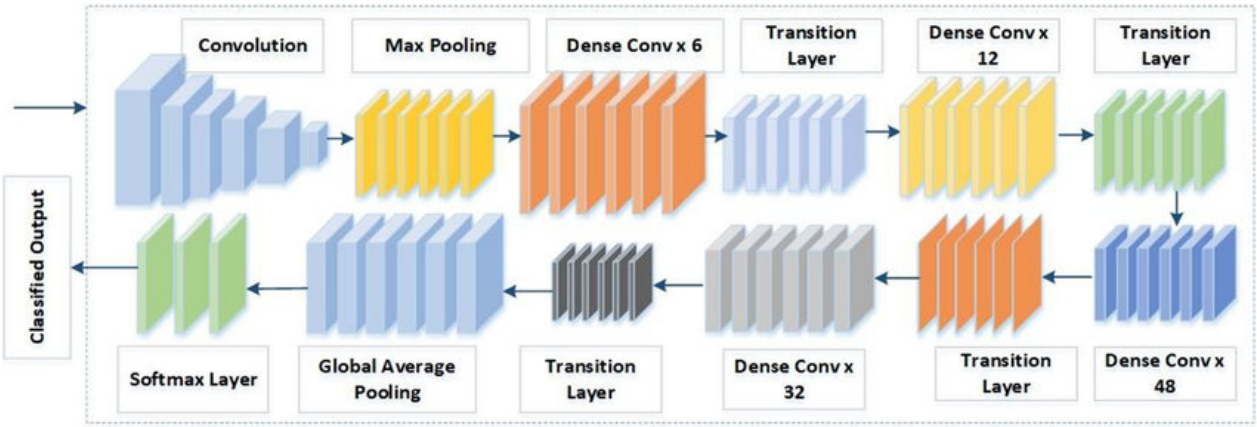


Σχήμα 2.4: Example : A schematic illustration of the DenseNet-121 architecture. Source: Radwan et al. (2019)[3].



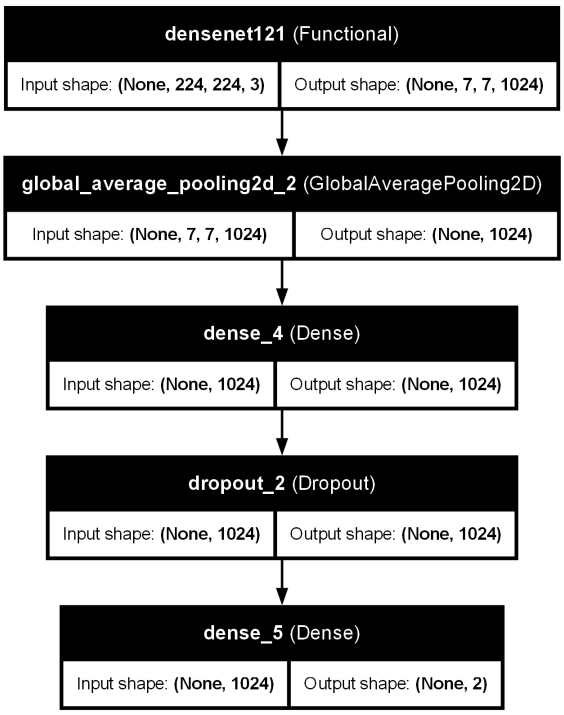
Σχήμα 2.5: Example : The architecture of DenseNet-169. Source: Madipally et al. (2022)[4].

Στο πλαίσιο της ανίχνευσης πλαστογραφίας υπογραφών, η πυκνή συνδεσιμότητα του DenseNet το καθιστά ιδανική επιλογή για την εκμάθηση των περίπλοκων παραλλαγών στις χειρόγραφες υπογραφές. Οι υπογραφές είναι εγγενώς μεταβλητές, ακόμη και όταν παράγονται από το ίδιο άτομο, και η ικανότητα του DenseNet να συγκεντρώνει χαρακτηριστικά από όλα τα προηγούμενα επίπεδα του επιτρέπει να καταγράφει τόσο τοπικά όσο και καθολικά μοτίβα εντός της εικόνας[19]. Αυτή η ικανότητα είναι ιδιαίτερα σημαντική για τη διαφοροποίηση μεταξύ γνήσιων και πλαστών υπογραφών, όπου μικρές αποκλίσεις στη σειρά διαδρομής ή στην πίεση της γραφής, μπορεί να σηματοδοτούν πλαστογραφία[20].

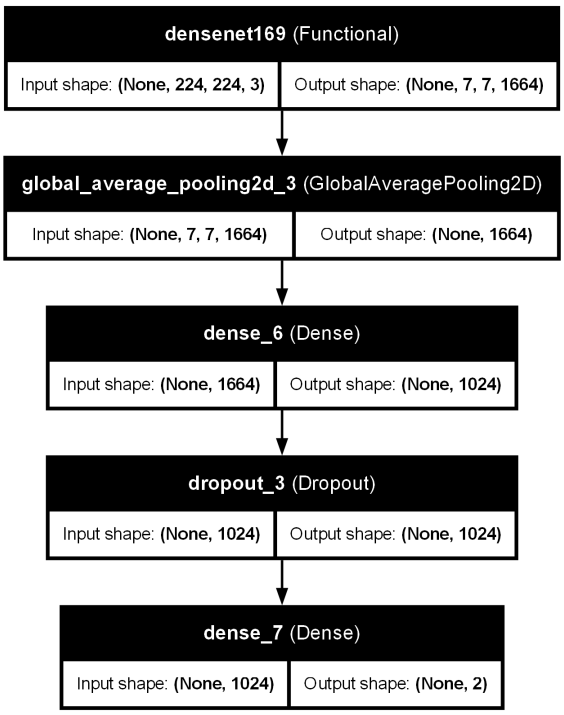


Σχήμα 2.6: Example : Detailed architecture of an Efficient DenseNet-201. Source: Mahum et al. (2022)[5].

Επιπλέον, η αποτελεσματικότητα του DenseNet στη χρήση παραμέτρων είναι πλεονεκτική όταν αντιμετωπίζουμε περιορισμένα δεδομένα, όπως συμβαίνει συχνά με τα σύνολα δεδομένων υπογραφών. Απαιτώντας λιγότερες παραμέτρους από τα παραδοσιακά CNN διατηρώντας παράλληλα υψηλή απόδοση, τα μοντέλα DenseNet είναι λιγότερο επιρρεπή σε υπερπροσαρμογή, καθιστώντας τα κατάλληλα για εργασίες όπως η επαλήθευση υπογραφής, όπου τα δεδομένα ενδέχεται να είναι περιορισμένα και οι διαφορές μεταξύ των κατηγοριών (γνήσια έναντι πλαστών) είναι διαφοροποιημένες[19][20]. Στο σύστημά μας, το DenseNet χρησιμεύει ως ισχυρός «εξορύκτης» χαρακτηριστικών, τα οποία στη συνέχεια χρησιμοποιούνται από μοντέλα μηχανικής μάθησης για την τελική ταξινόμηση[19].



(α′) Model visualization of DenseNet121.

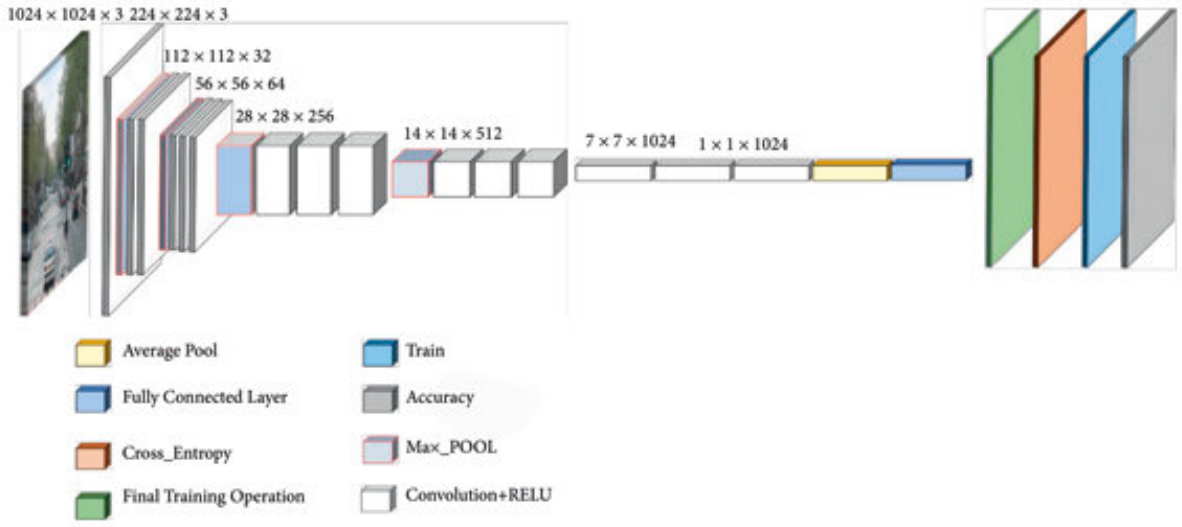


(β′) Model visualization of DenseNet169.

Σχήμα 2.7: Model Visualizations for DenseNet121 and DenseNet169.

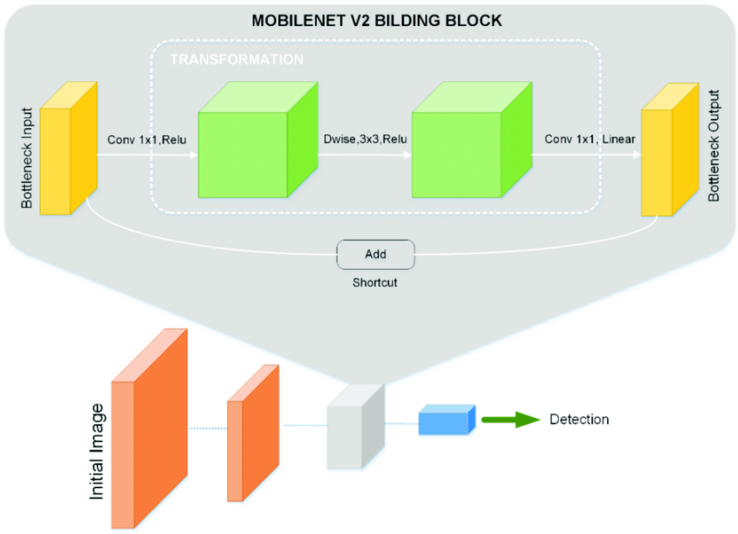
2.3 MobileNet και MobileNetV2

Τα MobileNet και MobileNetV2, που αναπτύχθηκαν από τους Howard et al. (2017), είναι νευρωνικά δίκτυα χαμηλής κατανάλωσης πόρων σχεδιασμένα για αποτελεσματικότητα, ιδιαίτερα σε περιβάλλοντα όπως κινητές συσκευές και ενσωματωμένα συστήματα. Το MobileNet επιτυγχάνει αυτήν την αποτελεσματικότητα χρησιμοποιώντας συνελίξεις που μπορούν να διαχωριστούν σε βάθος, οι οποίες μειώνουν σημαντικά τον αριθμό των παραμέτρων και το υπολογιστικό φορτίο, σε σύγκριση με τις τυπικές συνελίξεις[19][21]. Το MobileNetV2 βασίζεται σε αυτήν την αρχιτεκτονική εισάγοντας «ανεστραμμένα υπολειμματικά μπλοκ» (inverted residual blocks) και γραμμικά σημεία συμφόρησης, τα οποία βελτιώνουν περαιτέρω την απόδοση διατηρώντας παράλληλα την αποδοτικότητα[21].



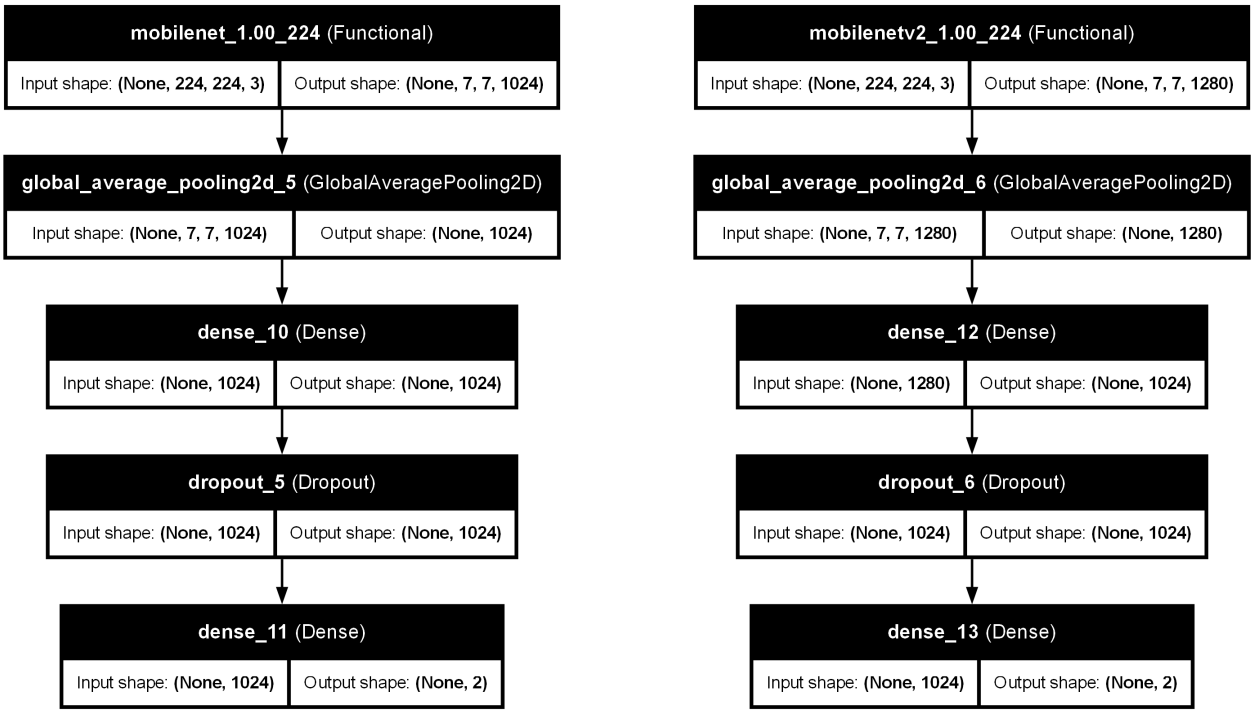
Σχήμα 2.8: Example : The architecture of MobileNet V1. Source: Asad et al. (2022)[6].

Για την εργασία επαλήθευσης υπογραφής, επιλέχθηκαν μοντέλα MobileNet λόγω της ισορροπίας μεταξύ ακρίβειας και υπολογιστικής αποτελεσματικότητας. Συστήματα επαλήθευσης υπογραφών αναπτύσσονται συχνά σε εφαρμογές σε πραγματικό χρόνο, όπως mobile banking ή υπογραφή ψηφιακών συμβολαίων, όπου απαιτείται γρήγορη και ακριβής επεξεργασία. Το MobileNet και το MobileNetV2 παρέχουν την απαραίτητη υπολογιστική απόδοση χωρίς να διακυβεύεται η ποιότητα των εξαγόμενων δυνατοτήτων. Παρά την ελαφριά φύση τους, τα μοντέλα MobileNet είναι σε θέση να καταγράφουν βασικές λεπτομέρειες σε εικόνες υπογραφής, όπως η κατεύθυνση και η πίεση, που είναι κρίσιμα για τη διάκριση των πλαστών από τις γνήσιες υπογραφές.



Σχήμα 2.9: Example : Architecture of MobileNetV2. Source: Martínez et al. (2021)[7].

Η εφαρμογή του MobileNet στο σύστημά μας διασφαλίζει ότι η διαδικασία εξαγωγής χαρακτηριστικών παραμένει γρήγορη και αποτελεσματική, καθιστώντας εφικτή την ανάπτυξη συστημάτων επαλήθευσης υπογραφής σε συσκευές με περιορισμένη επεξεργαστική ισχύ. Αυτές οι δυνατότητες μεταβιβάζονται στη συνέχεια σε ταξινομητές μηχανικής μάθησης, επιτρέποντας την ανίχνευση πλαστών υπογραφών σε πραγματικό χρόνο ακόμη και σε περιβάλλοντα με περιορισμούς πόρων.

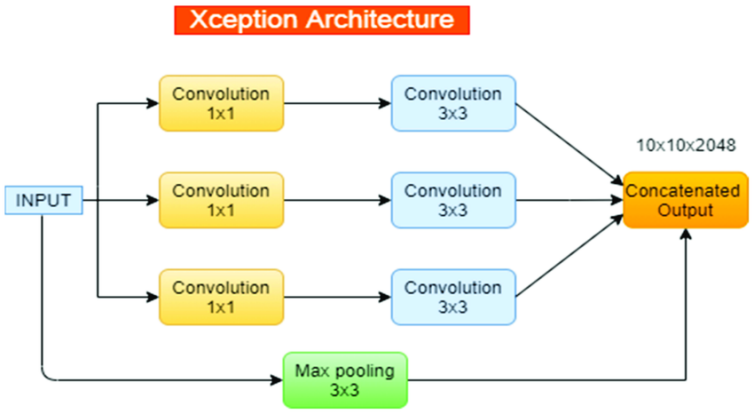


(α′) Model visualization of MobileNet(V1). (β′) Model visualization of MobileNetV2.

Σχήμα 2.10: Model Visualizations for MobileNet(V1) and MobileNetV2.

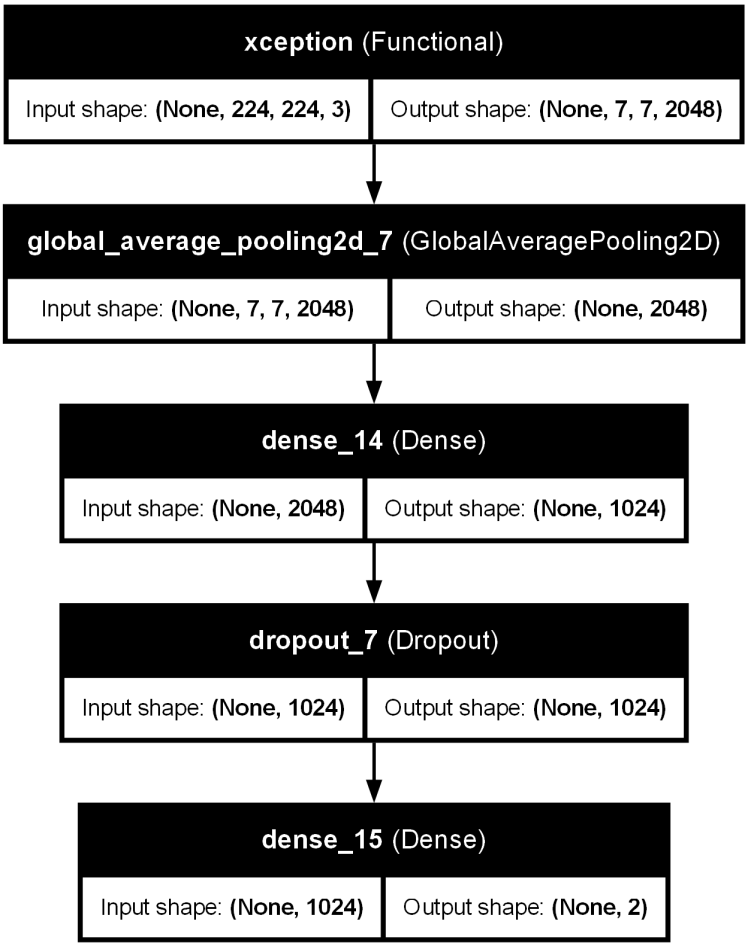
2.4 Xception

Το Xception, που εισήχθη από τον François Chollet το 2017, βασίζεται στην αρχιτεκτονική Inception αντικαθιστώντας τις μονάδες έναρξης με συνελεύσεις που μπορούν να διαχωριστούν σε βάθος. Η αρχιτεκτονική Xception βασίζεται στην υπόθεση ότι η αντιστοίχιση διακαναλικών και χωρικών συσχετισμών μπορεί να αποσυνδεθεί πλήρως, επιτρέποντας πιο αποτελεσματική χρήση παραμέτρων διατηρώντας παράλληλα υψηλή απόδοση. Αυτή η αρχιτεκτονική βελτίωση επιτρέπει στο Xception να επιτύχει ανώτερα αποτελέσματα σε εργασίες ταξινόμησης εικόνων μεγάλης κλίμακας χωρίς να αυξάνει τον αριθμό παραμέτρων του μοντέλου[19][20].



Σχήμα 2.11: Example : Xception CNN architecture. Source: Westphal et al. (2021)[8].

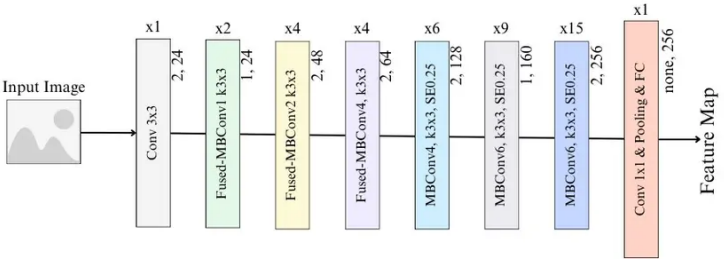
Στην ανίχνευση πλαστογραφίας υπογραφής, η αρχιτεκτονική του Xception είναι ιδιαίτερα ωφέλιμη επειδή επιτρέπει στο δίκτυο να εστιάσει τόσο στη χωρική διάταξη όσο και στα μεμονωμένα χαρακτηριστικά διαδρομής της υπογραφής. Οι πλαστές υπογραφές συχνά διαφέρουν από τις γνήσιες ως προς τις ανεπαίσθητες χωρικές παραμορφώσεις και τις ανωμαλίες στη συνοχή των κινήσεων γραφής. Η ικανότητα του Xception να μοντελοποιεί αυτά τα χαρακτηριστικά ξεχωριστά το καθιστά ένα ισχυρό εργαλείο για την επαλήθευση υπογραφής.
Οι σε βάθος διαχωριστικές περιελίξεις του Xception επιτρέπουν στο μοντέλο να αποτυπώνει λεπτομέρειες στην υπογραφή διατηρώντας παράλληλα την αποτελεσματικότητα. Στο σύστημά μας, το Xception χρησιμοποιείται ως εργαλείο εξαγωγής χαρακτηριστικών, δημιουργώντας αναπαραστάσεις χαρακτηριστικών υψηλής ποιότητας που στη συνέχεια τροφοδοτούνται σε ταξινομητές μηχανικής μάθησης για τη λήψη τελικών αποφάσεων. Αυτή η προσέγγιση διασφαλίζει ότι το σύστημα μπορεί να διαφοροποιήσει αποτελεσματικά τις γνήσιες και τις πλαστές υπογραφές, ακόμη και όταν οι διαφορές δεν είναι άμεσα εμφανείς στο ανθρώπινο μάτι.



Σχήμα 2.12: Model visualization of Xception.

2.5 EfficientNetV2S

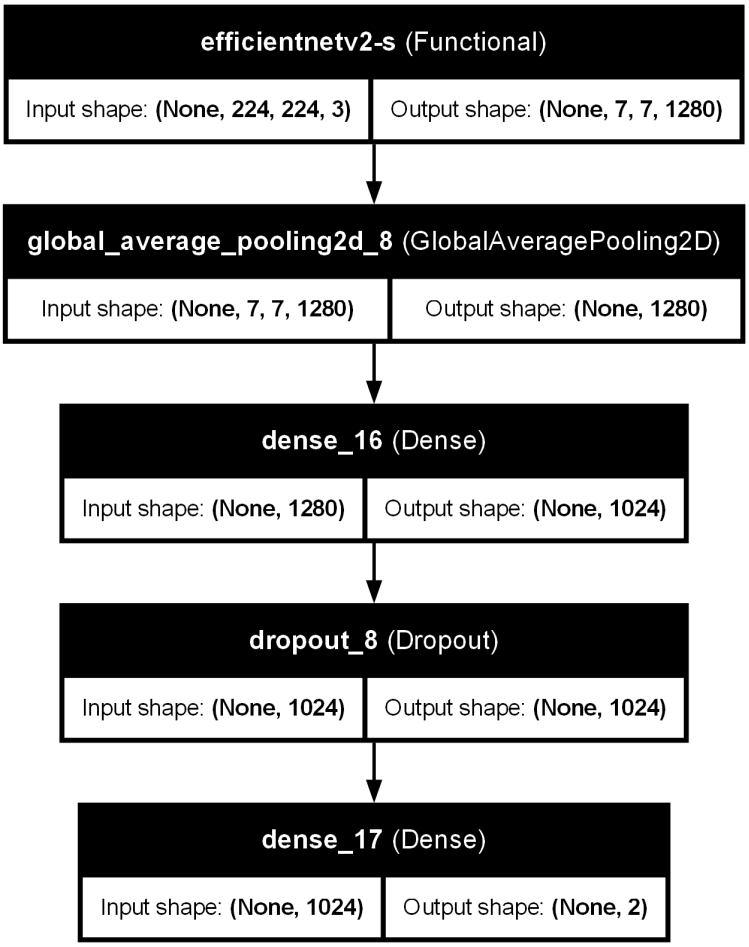
Το EfficientNet, που προτάθηκε από τους Tan και Le (2019), εισάγει μια νέα μέθοδο κλιμάκωσης των αρχιτεκτονικών του CNN εξισορροπώντας το βάθος, το πλάτος και την ανάλυση του δικτύου χρησιμοποιώντας μια μέθοδο σύνθετης κλίμακας[22]. Το EfficientNetV2S είναι μια μικρότερη, ταχύτερη έκδοση του EfficientNet, σχεδιασμένη να βελτιστοποιεί τόσο την ταχύτητα όσο και την ακρίβεια της εκπαίδευσης. Με τη συστηματική κλιμάκωση της αρχιτεκτονικής του δικτύου, το EfficientNetV2S επιτυγχάνει κορυφαίες επιδόσεις σε εργασίες ταξινόμησης εικόνων διατηρώντας παράλληλα την υπολογιστική απόδοση[20][22].



Σχήμα 2.13: Example : Architecture of EfficientNetV2. Source: Aldakhil et al. (2024)[9].

Επιλέχθηκε για το σύστημα επαλήθευσης υπογραφής λόγω της ικανότητάς του να παρέχει υψηλή ακρίβεια με λιγότερες παραμέτρους και μικρότερο υπολογιστικό κόστος. Η επαλήθευση υπογραφής συχνά περιλαμβάνει την επεξεργασία μεγάλων συνόλων δεδομένων σε πραγματικό χρόνο και η βελτιστοποιημένη αρχιτεκτονική του EfficientNetV2S διασφαλίζει ότι το σύστημα μπορεί να χειριστεί αυτό το φορτίο χωρίς να θυσιάζει την ακρίβεια. Η ικανότητα του μοντέλου να κλιμακώνεται αποτελεσματικά το καθιστά ιδιαίτερα κατάλληλο για περιβάλλοντα όπου τόσο η ταχύτητα όσο και η ακρίβεια είναι ζωτικής σημασίας, όπως οι οικονομικές συναλλαγές και η επαλήθευση νομικών εγγράφων

Στο σύστημά μας, το EfficientNetV2S χρησιμεύει ως εξαγωγέας χαρακτηριστικών, παρέχοντας λεπτομερή διανύσματα χαρακτηριστικών που καταγράφουν τα βασικά χαρακτηριστικά της υπογραφής. Αυτά τα χαρακτηριστικά μεταβιβάζονται στη συνέχεια σε ταξινομητές μηχανικής μάθησης, οι οποίοι τα χρησιμοποιούν για να προσδιορίσουν εάν η υπογραφή είναι γνήσια ή πλαστή. Χρησιμοποιώντας το EfficientNetV2S, διασφαλίζουμε ότι το σύστημά μας παραμένει ακριβές και αποτελεσματικό, ακόμη και όταν επεξεργάζεται μεγάλους όγκους δεδομένων υπογραφής.



Σχήμα 2.14: Model visualization of EfficientNetV2S.

2.6 Ενσωμάτωση Deep Learning και Machine Learning

Σε αυτή τη πτυχιακή εργασία, συνδυάζουμε τη δύναμη της εξαγωγής χαρακτηριστικών βαθιάς μάθησης με τις δυνατότητες ταξινόμησης των παραδοσιακών αλγορίθμων μηχανικής μάθησης. Καθένα από τα μοντέλα βαθιάς μάθησης που συζητούνται σε αυτό το κεφάλαιο χρησιμοποιούνται για την εξαγωγή αναπαραστάσεων χαρακτηριστικών από εικόνες υπογραφής. Αυτά τα διανύσματα χαρακτηριστικών καταγράφουν τις περίπλοκες λεπτομέρειες των υπογραφών, συμπεριλαμβανομένων των χωρικών σχέσεων, των μοτίβων διαδρομής και των διακυμάνσεων της πίεσης. Αφού εξαχθούν, αυτά τα χαρακτηριστικά τροφοδοτούνται σε ταξινομητές μηχανικής μάθησης όπως Υποστήριξη διανυσματικών μηχανών (SVM), K-Nearest Neighbors (KNN), Random Forests κ.α. [23].
Αυτή η υβριδική προσέγγιση αξιοποιεί τα δυνατά σημεία και των δύο παραδειγμάτων. Τα μοντέλα βαθιάς μάθησης διαπρέπουν στην αυτόματη εκμάθηση πολύπλοκων χαρακτηριστικών από ακατέργαστα δεδομένα, τα οποία θα ήταν δύσκολο να κατασκευαστούν με μη αυτόματο τρόπο. Εν τω μεταξύ, τα μοντέλα μηχανικής εκμάθησης είναι κατάλληλα για εργασίες ταξινόμησης, ιδιαίτερα όταν παρέχονται με διανύσματα χαρακτηριστικών υψηλής ποιότητας. Συνδυάζοντας την εξαγωγή χαρακτηριστικών βαθιάς εκμάθησης με την ταξινόμηση μηχανικής μάθησης, δημιουργούμε ένα ισχυρό σύστημα ικανό να ανιχνεύει με ακρίβεια πλαστές υπογραφές διατηρώντας παράλληλα την υπολογιστική απόδοση[23][24].

2.7 Συμπέρασμα

Αυτό το κεφάλαιο παρείχε μια εις βάθος εξερεύνηση των μοντέλων βαθιάς μάθησης που χρησιμοποιούνται στο σύστημα επαλήθευσης υπογραφών μας. Κάθε μοντέλο επιλέχθηκε για την ικανότητά του να εξάγει πλούσια, υψηλής ποιότητας χαρακτηριστικά από εικόνες υπογραφής, επιτρέποντας στο σύστημα να διαφοροποιεί τις γνήσιες και τις πλαστές υπογραφές με υψηλή ακρίβεια. Ο συνδυασμός βαθιάς μάθησης και μηχανικής μάθησης μας επιτρέπει να δημιουργήσουμε ένα σύστημα επαλήθευσης υπογραφής που είναι ταυτόχρονα ισχυρό και αποτελεσματικό, ικανό να λειτουργεί σε πραγματικό χρόνο διατηρώντας παράλληλα υψηλά επίπεδα ακρίβειας. Αυτά τα μοντέλα αποτελούν τη ραχοκοκαλιά του αγωγού εξαγωγής χαρακτηριστικών μας, παρέχοντας τα βασικά δεδομένα που καθοδηγούν τις τελικές αποφάσεις ταξινόμησης που λαμβάνονται από τους αλγόριθμους μηχανικής εκμάθησης.

Κεφάλαιο 3

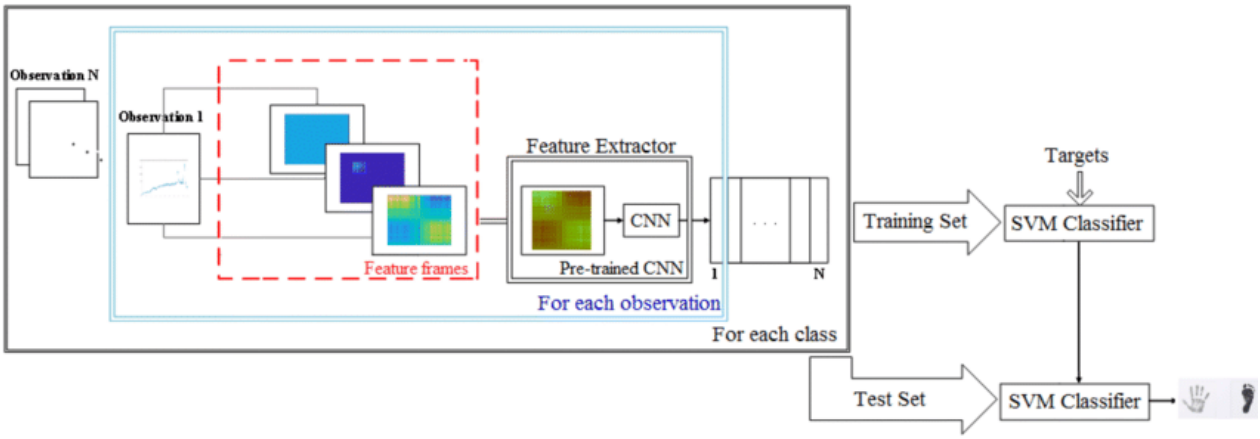
Αλγόριθμοι Μηχανικής Μάθησης

Σε αυτό το κεφάλαιο, εμβαθύνουμε στους αλγόριθμους μηχανικής μάθησης που χρησιμοποιούνται για την ταξινόμηση των χαρακτηριστικών που εξάγονται από μοντέλα βαθιάς μάθησης στο έργο της ανίχνευσης πλαστογραφίας υπογραφών. Αυτοί οι αλγόριθμοι —Support Vector Machines (SVM), K-Nearest Neighbors (KNN), Logistic Regression, Decision Trees, Random Forests και Naive Bayes— έχουν επιλεγεί προσεκτικά για την ευρωστία και την προσαρμοστικότητά τους σε πολύπλοκες εργασίες ταξινόμησης, ιδιαίτερα όταν αντιμετωπίζουμε υψηλών διαστάσεων χαρακτηριστικά που προέρχονται από αρχιτεκτονικές βαθιάς μάθησης. Κάθε αλγόριθμος συμβάλλει μοναδικά στη διαδικασία ταξινόμησης και διερευνούμε τους ρόλους, τα κριτήρια επιλογής και τον τρόπο ενσωμάτωσής τους με την εξαγωγή χαρακτηριστικών από εκπεδευμένα μοντέλα βαθιάς μάθησης.

3.1 Support Vector Machines (SVM)

Οι Μηχανές Διανυσμάτων Υποστήριξης (SVM) θεωρούνται ευρέως για την ικανότητά τους να εκτελούν δυαδική ταξινόμηση κατασκευάζοντας ένα βέλτιστο υπερεπίπεδο που μεγιστοποιεί το περιθώριο μεταξύ διαφορετικών κλάσεων. Τα SVM είναι ιδιαίτερα αποτελεσματικά σε χώρους υψηλών διαστάσεων και έχουν δείξει ισχυρή απόδοση σε εργασίες που περιλαμβάνουν βιομετρικά δεδομένα, όπως χειρόγραφες υπογραφές. Στο πλαίσιο της επαλήθευσης υπογραφής, τα SVM έχουν εφαρμοστεί σε συνδυασμό με μοντέλα βαθιάς μάθησης για την ακριβή ταξινόμηση των εξαγόμενων χαρακτηριστικών. Τα SVM χειρίζονται καλά την πολυπλοκότητα του χώρου χαρακτηριστικών(βλ. Σχήμα 3.1), καθιστώντας τα ιδανικά για τη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών[20][25].
Επιλέξαμε το SVM για την ικανότητά του να χειρίζεται πολύπλοκα δεδομένα υψηλών διαστάσεων διατηρώντας παράλληλα ένα υψηλό περιθώριο ταξινόμησης, το οποίο είναι ζωτικής σημασίας για τη διασφάλιση της ακριβούς διαφοροποίησης μεταξύ αυθεντικών και πλαστών υπογραφών. Όταν συνδυάζονται με μοντέλα βαθιάς μάθησης όπως το VGG19 ή το DenseNet,

τα εξαγόμενα χαρακτηριστικά χρησιμοποιούνται για τη δημιουργία ενός εξαιρετικά διακριτικού χώρου χαρακτηριστικών, επιτρέποντας στο SVM να δημιουργήσει σαφή όρια απόφασης μεταξύ των κλάσεων. Αυτός ο συνδυασμός αξιοποιεί την ικανότητα του SVM να γενικεύει καλά από την πλούσια σε χαρακτηριστικά αποτελέσματα των μοντέλων βαθιάς μάθησης

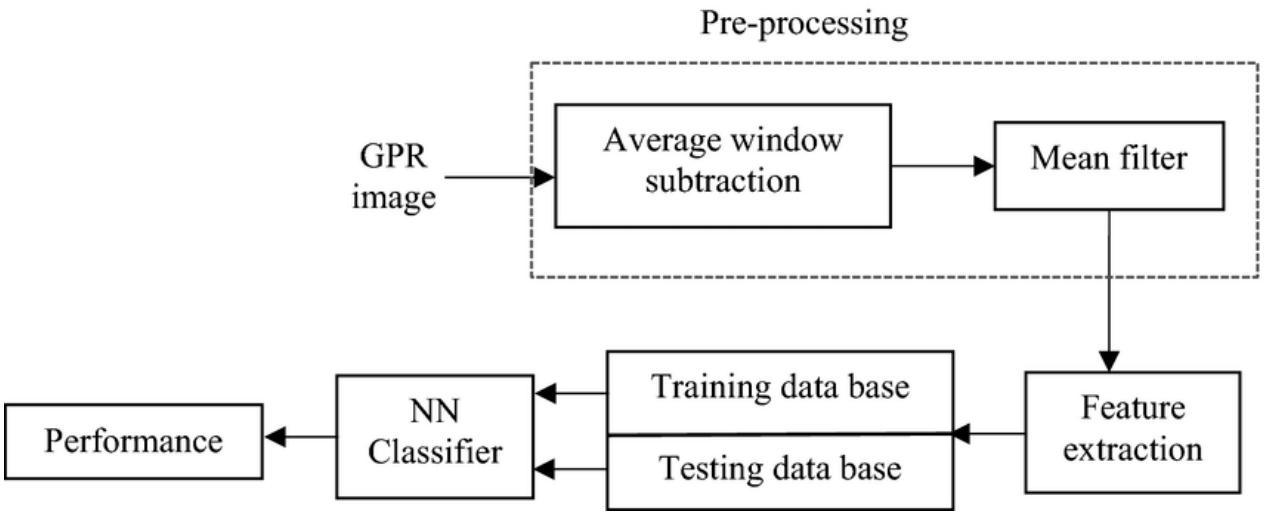


Σχήμα 3.1: An example of Support Vector Machine (SVM) classifier. Source: Journal of Neuroscience Methods. (2020)[10].

3.2 Κ-Κοντινότεροι γείτονες (KNN)

Το K-Nearest Neighbors (KNN) είναι ένας απλός αλγόριθμος μάθησης βασισμένος σε στιγμιότυπα που ταξινομεί δεδομένα με βάση την πλειοψηφία των Κ πλησιέστερων γειτόνων στον χώρο χαρακτηριστικών(βλ. Σχήμα 3.2). Το KNN είναι αποτελεσματικό σε εργασίες όπου το όριο απόφασης είναι πολύπλοκο και μη γραμμικό, καθιστώντας το μια κατάλληλη επιλογή για εργασίες βιομετρικής ταξινόμησης, όπως η επαλήθευση υπογραφής. Υπολογίζοντας την απόσταση μεταξύ των διανυσμάτων χαρακτηριστικών, το KNN προσδιορίζει τις πιο παρόμοιες υπογραφές, είτε είναι γνήσιες είτε πλαστές[25].

Το KNN επιλέχθηκε για την απλότητα και την αποτελεσματικότητά του στην αντιμετώπιση μη παραμετρικών δεδομένων, κάτι που συμβαίνει συχνά στην επαλήθευση υπογραφής. Όταν εφαρμόζεται στα χαρακτηριστικά που εξάγονται από μοντέλα βαθιάς μάθησης, το KNN αξιοποιεί την εγγύτητα παρόμοιων διανυσμάτων χαρακτηριστικών για την ακριβή ταξινόμηση των νέων υπογραφών. Η ικανότητά του να εργάζεται με δεδομένα υψηλών διαστάσεων, σε συνδυασμό με την εξαγωγή χαρακτηριστικών των μοντέλων βαθιάς μάθησης, παρέχει μια διαισθητική και ισχυρή μέθοδο ταξινόμησης για την επαλήθευση υπογραφής.

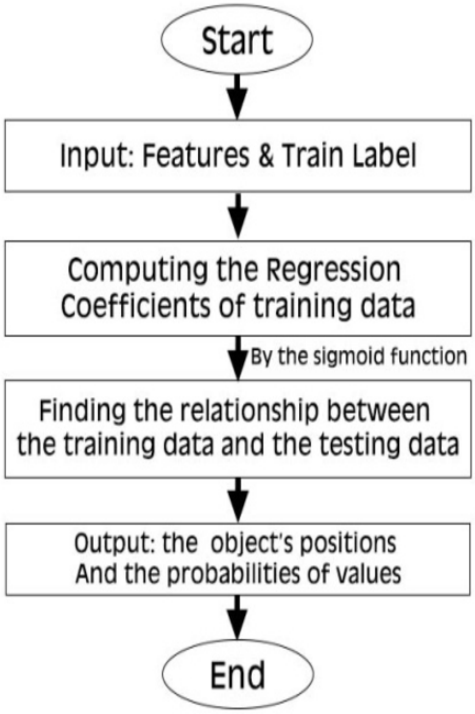


Σχήμα 3.2: An example of K-NN classifier.Source: International Journal of Remote Sensing. (2020)[11].

3.3 Logistic Regression (LR)

Η Λογιστική Παλινδρόμηση(LR) είναι ένα γραμμικό μοντέλο που χρησιμοποιείται για εργασίες δυαδικής ταξινόμησης, το οποίο μοντελοποιεί την πιθανότητα ότι μια δεδομένη είσοδος ανήκει σε μια συγκεκριμένη κλάση. Χρησιμοποιείται ευρέως λόγω της απλότητας, της ερμηνευσιμότητας και της αποτελεσματικότητάς του στη δυαδική ταξινόμηση(βλ. Σχήμα 3.3). Στην επαλήθευση υπογραφής, η λογιστική παλινδρόμηση βοηθά στον προσδιορισμό του αν μια υπογραφή είναι γνήσια ή πλαστή με βάση τα εξαγόμενα χαρακτηριστικά από μοντέλα βαθιάς μάθησης[20].

Επιλέξαμε την λογιστική παλινδρόμηση για την ικανότητά της να παρέχει ένα πιθανό πλαίσιο ταξινόμησης, επιτρέποντάς μας όχι μόνο να ταξινομήσουμε αλλά και να ερμηνεύσουμε την εμπιστοσύνη στα αποτελέσματα της ταξινόμησης. Όταν εφαρμόζεται στα χαρακτηριστικά που εξάγονται από μοντέλα βαθιάς μάθησης, η λογιστική παλινδρόμηση διαχωρίζει αποτελεσματικά τον χώρο χαρακτηριστικών σε δύο διακριτές κατηγορίες —γνήσιες και πλαστές υπογραφές— μοντελοποιώντας τη σχέση μεταξύ των διανυσμάτων χαρακτηριστικών και της πιθανότητας πλαστογραφίας.

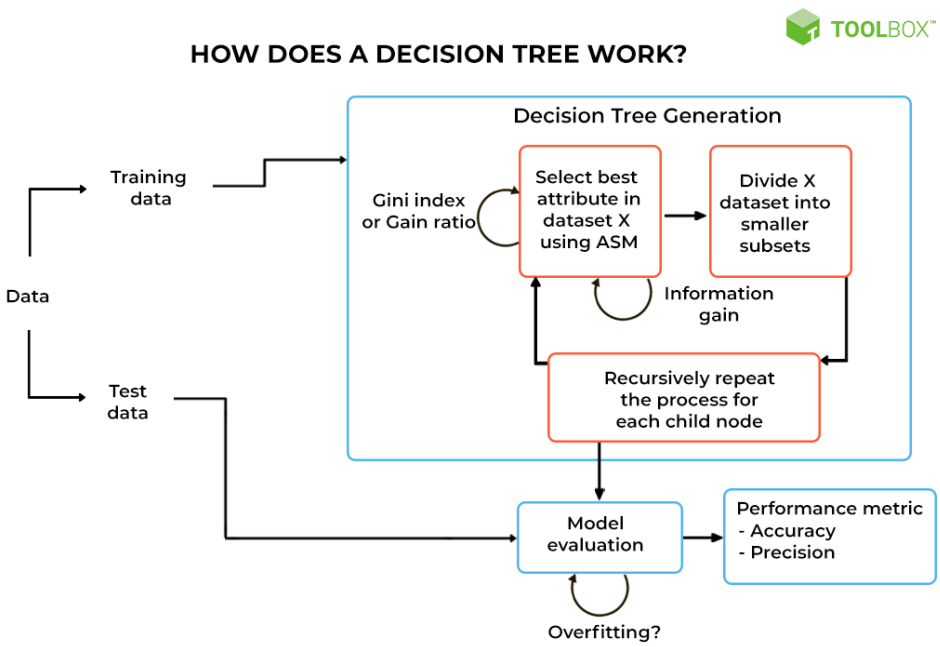


Σχήμα 3.3: Flowchart of the logistic regression algorithm. Source: Elnadree et al. (2021)[12].

3.4 Decision Tree

Τα δέντρα αποφάσεων είναι ιεραρχικά μοντέλα που διαχωρίζουν αναδρομικά τα δεδομένα με βάση τα πιο ενημερωτικά χαρακτηριστικά, δημιουργώντας μια δενδρική δομή που οδηγεί σε αποφάσεις ταξινόμησης. Τα δέντρα αποφάσεων εκτιμώνται για την ερμηνευτικότητά τους και την ικανότητά τους να μοντελοποιούν σύνθετα όρια αποφάσεων(βλ. Σχήμα 3.4). Στην επαλήθευση υπογραφών, τα Decision Trees μπορούν να ταξινομήσουν τις υπογραφές με βάση την ιεραρχική δομή των εξαγόμενων χαρακτηριστικών, καθιστώντας τα μια εξαιρετική επιλογή για την κατανόηση της υποκείμενης διαδικασίας λήψης αποφάσεων στον εντοπισμό πλαστογραφίας[20][25].

Επιλέξαμε Decision Trees λόγω της ερμηνευτικότητάς τους και της ικανότητάς τους να καταγράφουν περίπλοκα μοτίβα μέσα στα δεδομένα υπογραφής. Είναι ιδιαίτερα χρήσιμα στο πλαίσιο της εξαγωγής χαρακτηριστικών από μοντέλα βαθιάς μάθησης, καθώς τα εξαγόμενα χαρακτηριστικά μπορούν να οργανωθούν ιεραρχικά και να αξιολογηθούν για να δημιουργήσουν μια διαδικασία λήψης αποφάσεων που είναι ταυτόχρονα ερμηνεύσιμη και αποτελεσματική.



Σχήμα 3.4: An example of Decision Tree classifier.Source: Spiceworks. (2022)[13].

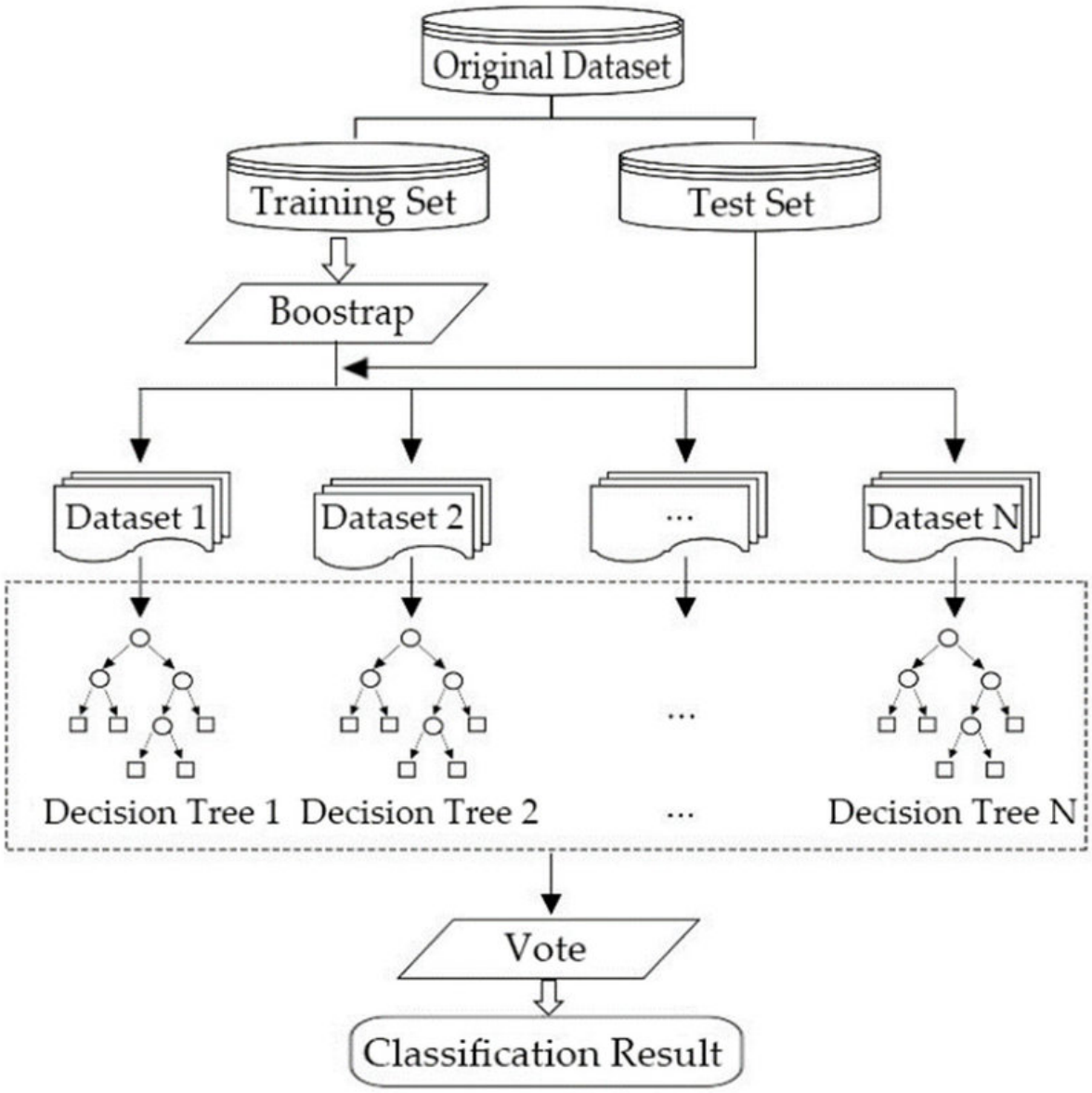
3.5 Random Forest

Το Random Forest είναι μια μέθοδος εκμάθησης συνόλου που λειτουργεί κατασκευάζοντας ένα πλήθος δέντρων αποφάσεων κατά τη διάρκεια της εκπαίδευσης και στη συνέχεια συγκεντρώνοντας τα αποτελέσματά τους για την παραγωγή της πιο δημοφιλής τάξης. Αυτή η μέθοδος αξιοποιεί την έννοια της «σοφίας του πλήθους», όπου κάθε δέντρο κάνει μια ανεξάρτητη ταξινόμηση και η τελική απόφαση βασίζεται στην πλειοψηφία των ψήφων σε όλα τα δέντρα. Το Random Forest υπερέχει στον χειρισμό θορυβωδών δεδομένων και χώρων χαρακτηριστικών υψηλών διαστάσεων, που είναι και τα δύο κοινά στις εργασίες επαλήθευσης υπογραφών(βλ. Σχήμα 3.5).

Σε αυτή τη πτυχιακή εργασία, το Random Forest χρησιμοποιείται για την ταξινόμηση των χαρακτηριστικών που εξάγονται από μοντέλα βαθιάς μάθησης όπως το VGG, το DenseNet και το EfficientNet. Δεδομένης της εγγενούς μεταβλητότητας στις χειρόγραφες υπογραφές, η ικανότητα του Random Forest να μειώνει την υπερπροσαρμογή με τον μέσο όρο των αποτελεσμάτων πολλών δέντρων είναι ιδιαίτερα πλεονεκτική. Αυτό οδηγεί σε ένα ισχυρό μοντέλο ταξινόμησης που μπορεί να γενικεύσει καλά σε μη ορατά δεδομένα, διαχωρίζοντας αποτελεσματικά μεταξύ γνήσιων και πλαστών υπογραφών.

Επιπλέον, ο αλγόριθμος Random Forest είναι ανθεκτικός στην υπερπροσαρμογή, ειδικά σε σενάρια με περιορισμένα δεδομένα εκπαίδευσης - ένα σύνηθες φαινόμενο στα σύνολα δεδομένων επαλήθευσης υπογραφών. Αξιοποιώντας την ισχύ πολλών δέντρων αποφάσεων, το Random Forest παρέχει μια ισχυρή ισορροπία μεταξύ της μεροληψίας και της διακύμανσης, καθιστώ-

ντας το μια κατάλληλη επιλογή για αυτήν την περίπλοκη εργασία[20].

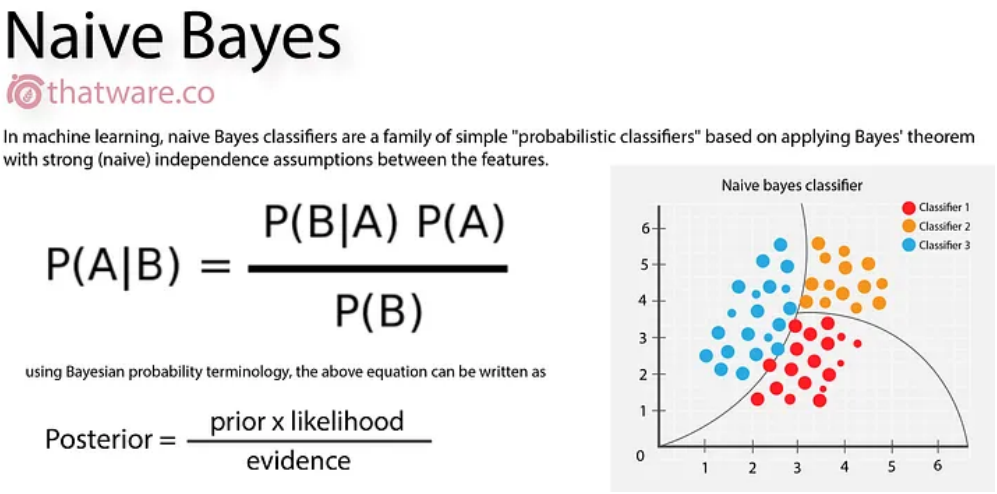


Σχήμα 3.5: An example of Random Forest classifier.Source: International Journal of Environmental Research and Public Health. (2019)[14].

3.6 Naive Bayes

Ο Naive Bayes είναι ένας πιθανολογικός ταξινομητής που βασίζεται στο θεώρημα του Bayes, υποθέτοντας ότι τα χαρακτηριστικά είναι υπό όρους ανεξάρτητα δεδομένης της ετικέτας/κλάσης. Παρά την "αφελή" παραδοχή της ανεξαρτησίας χαρακτηριστικών, ο αλγόριθμος αποδίδει

εξαιρετικά καλά σε διάφορες εργασίες ταξινόμησης, ιδιαίτερα όταν το σύνολο δεδομένων είναι μεγάλο και η διάσταση είναι υψηλή(βλ. Σχήμα 3.6).
Στο πλαίσιο της επαλήθευσης υπογραφής, το Naive Bayes χρησιμοποιείται για την ταξινόμηση των εξαγόμενων χαρακτηριστικών από μοντέλα βαθιάς μάθησης. Με τον υπολογισμό της μεταγενέστερης πιθανότητας για κάθε τάξη, ο αλγόριθμος εκχωρεί την υπογραφή στην κλάση με την υψηλότερη πιθανότητα. Ένα από τα βασικά πλεονεκτήματα του Naive Bayes είναι η ταχύτητα και η αποτελεσματικότητά του, γεγονός που το καθιστά κατάλληλο για συστήματα επαλήθευσης υπογραφών σε πραγματικό χρόνο. Ακόμη και με τα πολύπλοκα διανύσματα χαρακτηριστικών που προέρχονται από συνελικτικά επίπεδα, το Naive Bayes παρέχει ανταγωνιστική απόδοση λόγω της απλότητας και της επεκτασιμότητας[20][25].



Σχήμα 3.6: An example of Naive Bayes classifier.Source: Introduction to Naïve Bayes Classifier. (2019)[15].

3.7 Σύγκριση Αλγορίθμων

Καθένας από τους αλγόριθμους μηχανικής μάθησης που συζητούνται σε αυτό το κεφάλαιο έχει επιλεγεί προσεκτικά για τα μοναδικά πλεονεκτήματά του στον χειρισμό του πολύπλοκου έργου της ανίχνευσης πλαστογραφίας υπογραφών. Τα SVM και Random Forests υπερέχουν στον χειρισμό δεδομένων υψηλών διαστάσεων, καθιστώντας τα ιδιαίτερα αποτελεσματικά όταν συνδυάζονται με χαρακτηριστικά που προέρχονται από βαθιά μάθηση. Το K-Nearest Neighbors προσφέρει έναν απλό αλλά ισχυρό μηχανισμό ταξινόμησης που βασίζεται στην εγγύτητα χαρακτηριστικών, ενώ η Logistic Regression παρέχει ένα πιθανό και ερμηνεύσιμο μοντέλο για δυαδική ταξινόμηση.
Τα Decision Trees και τα Random Forests ξεχωρίζουν για την ικανότητά τους να χειρίζονται μη γραμμικές σχέσεις στα δεδομένα, παρέχοντας ερμηνευτικότητα παράλληλα με την ευρωστία στην υπερβολική προσαρμογή. Εν τω μεταξύ, το Naive Bayes προσφέρει μια αποτελεσμα-

τική και επεκτάσιμη προσέγγιση, ιδιαίτερα χρήσιμη σε σενάρια όπου απαιτείται ταξινόμηση σε πραγματικό χρόνο. Μαζί, αυτοί οι αλγόριθμοι καλύπτουν ένα ευρύ φάσμα μεθοδολογιών ταξινόμησης, διασφαλίζοντας ότι το σύστημα μπορεί να προσαρμοστεί στις περιπλοκές των δεδομένων υπογραφής διατηρώντας παράλληλα υψηλή ακρίβεια και αποτελεσματικότητα. Αξιοποιώντας τα δυνατά σημεία αυτών των μοντέλων μηχανικής μάθησης σε συνδυασμό με την εξαγωγή χαρακτηριστικών βαθιάς μάθησης, αυτή η πτυχιακή εργασία επιτυγχάνει μια ολοκληρωμένη και αποτελεσματική προσέγγιση για τον εντοπισμό πλαστογραφίας υπογραφών. Τα επόμενα κεφάλαια θα εξερευνήσουν τα πειραματικά αποτελέσματα και τις μετρήσεις απόδοσης αυτών των αλγορίθμων όταν εφαρμόζονται στην εργασία επαλήθευσης υπογραφής.

Algorithm	**Description**	**Advantages**	**Disadvantages**	**Use Case in Project**
Logistic Regression	A linear model used for binary classification problems.	Simple to implement, efficient for small datasets, interpretable.	Assumes linear relationship between features, less effective on complex data.	Used for initial binary classification of features extracted from deep learning models.
Support Vector Machine (SVM)	A supervised learning model that finds the optimal hyperplane for classifying data points.	Effective in high-dimensional spaces, works well for complex data.	Not suitable for large datasets, less interpretable.	Applied after feature extraction to classify signatures as genuine or forged.
K-Nearest Neighbors (KNN)	A non-parametric algorithm that classifies based on the closest training examples.	Simple, effective in small datasets, easy to understand.	Slow for large datasets, sensitive to noise and irrelevant features.	Used to classify extracted features when a simpler model was needed.
Decision Trees	A tree-like model that splits data into branches based on feature values.	Easy to interpret, handles both numerical and categorical data.	Prone to overfitting, can be unstable with small variations in data.	Used as a baseline classifier and to interpret feature importance.
Random Forest	An ensemble method that combines multiple decision trees for better accuracy.	Reduces overfitting, improves accuracy, handles large datasets well.	Less interpretable than single decision trees, requires more computation.	Applied to enhance classification accuracy and robustness against overfitting.
Naive Bayes	A probabilistic classifier based on Bayes' theorem with independence assumptions.	Fast, simple, effective for large datasets, performs well with high-dimensional data.	Assumes independence between features, which may not always hold.	Used to classify extracted features, particularly effective when feature independence was assumed.

Πίνακας 3.1: Comparison of Machine Learning Algorithms Used in the Project

Κεφάλαιο 4

Τεχνολογίες

Η ανάπτυξη του συστήματος ανίχνευσης πλαστογραφίας υπογραφών περιλάμβανε τη χρήση πολλών ισχυρών τεχνολογιών που επέτρεψαν την επεξεργασία, τη μοντελοποίηση και την αξιολόγηση πολύπλοκων συνόλων δεδομένων. Κάθε τεχνολογία επιλέχθηκε για τη συγκεκριμένη λειτουργικότητά της, τη συνάφεια με την αναγνώριση εικόνας και τη δυνατότητα εφαρμογής σε εργασίες επαλήθευσης υπογραφών. Αυτό το κεφάλαιο θα παρέχει μια λεπτομερή εξήγηση για κάθε τεχνολογία, γιατί επιλέχθηκε, πώς χρησιμοποιήθηκε στη πτυχιακή εργασία και την αποτελεσματικότητά της στον τομέα της αναγνώρισης εικόνων, ιδιαίτερα της ανίχνευσης πλαστογραφίας υπογραφών.

4.1 Python

Η Python είναι μια ευέλικτη, υψηλού επιπέδου γλώσσα προγραμματισμού που χρησιμοποιείται ευρέως στην επιστήμη των δεδομένων, τη μηχανική μάθηση και την επιστημονική πληροφορική. Προσφέρει ένα τεράστιο οικοσύστημα βιβλιοθηκών όπως οι TensorFlow, Keras, Scikit-learn, NumPy και Pandas αλλά και πλαισίων, καθιστώντας το ιδανική επιλογή για την εφαρμογή μοντέλων μηχανικής μάθησης και βαθιάς μάθησης. Η ενεργή κοινότητα και η ευκολία ενσωμάτωσής του με άλλα εργαλεία το κατέστησαν την καλύτερη επιλογή για την ανάπτυξη ενός ισχυρού και επεκτάσιμου συστήματος ανίχνευσης πλαστογραφίας υπογραφών[26][27].
Στη πτυχιακή εργασία, χρησιμοποίθηκε ως η βασική γλώσσα προγραμματισμού για ολόκληρο το σύστημα, από την προεπεξεργασία δεδομένων και την εκπαίδευση μοντέλων μέχρι την αξιολόγηση και την οπτικοποίηση. Η διαλειτουργικότητα της Python με πολλές βιβλιοθήκες μας επέτρεψε να εφαρμόσουμε και να δοκιμάσουμε γρήγορα μοντέλα βαθιάς μάθησης για εξαγωγή χαρακτηριστικών καθώς και παραδοσιακούς αλγόριθμους μηχανικής μάθησης για ταξινόμηση. Ο ρόλος της Python στον εντοπισμό πλαστογραφίας υπογραφών οφείλεται σε μεγάλο βαθμό στην ικανότητά της να ενσωματώνει απρόσκοπτα διάφορες βιβλιοθήκες που απαιτούνται για την επεξεργασία εικόνας και τη μηχανική εκμάθηση. Αυτή η ευελιξία επέτρεψε τον

αποτελεσματικό χειρισμό των δεδομένων εικόνας υπογραφής και την εκπαίδευση μοντέλων υψηλής απόδοσης για τον εντοπισμό πλαστών υπογραφών.

4.2 TensorFlow

Το TensorFlow είναι ένα πλαίσιο μηχανικής εκμάθησης ανοιχτού κώδικα που αναπτύχθηκε από την Google. Έχει σχεδιαστεί για να διευκολύνει την εκπαίδευση και την ανάπτυξη μοντέλων μηχανικής μάθησης και βαθιάς μάθησης, ιδιαίτερα εκείνων που απαιτούν υπολογισμούς μεγάλης κλίμακας σε διάφορα περιβάλλοντα υλικού, όπως CPU(επεξεργαστή) και GPU(κάρτα γραφικών).
Η συγκεκριμένη τεχνολογία επελέγη για τις ισχυρές δυνατότητες βαθιάς μάθησης και την υποστήριξη μηχανικής μάθησης μεγάλης κλίμακας. Η ευελιξία της και η ικανότητά της να χειρίζεται αποτελεσματικά δεδομένα εικόνας υψηλών διαστάσεων την καθιστούν ιδανική επιλογή για την εκπαίδευση μοντέλων βαθιάς μάθησης στα σύνολα δεδομένων υπογραφής μας.
Το TensorFlow χρησιμοποιήθηκε για την εφαρμογή προ-εκπαιδευμένων μοντέλων βαθιάς μάθησης (π.χ. VGG, DenseNet, EfficientNet) για την εξαγωγή χαρακτηριστικών από εικόνες υπογραφών. Τα μοντέλα βαθιάς μάθησης βελτιστοποιήθηκαν χρησιμοποιώντας τους αλγορίθμους βελτιστοποίησης του TensorFlow για την εξαγωγή σχετικών χαρακτηριστικών από τις υπογραφές, τα οποία στη συνέχεια διαβιβάστηκαν σε παραδοσιακούς ταξινομητές μηχανικής μάθησης για την ανίχνευση πλαστογραφίας.
Η ικανότητά του να χειρίζεται σύνθετα δεδομένα εικόνας και να εκπαιδεύει μοντέλα βαθιάς μάθησης το καθιστά ιδιαίτερα αποτελεσματικό στην αναγνώριση μοτίβων μέσα σε εικόνες υπογραφών. Η υποστήριξή του για μάθηση μεταφοράς μας επέτρεψε να αξιοποιήσουμε προεκπαιδευμένα μοντέλα, τα οποία βελτίωσαν την ακρίβεια της ανίχνευσης πλαστογραφίας, εξάγοντας χαρακτηριστικά που διακρίνουν μεταξύ γνήσιων και πλαστών υπογραφών[26][27].

4.3 Keras

Το Keras είναι ένα υψηλού επιπέδου API για την κατασκευή και την εκπαίδευση μοντέλων βαθιάς μάθησης.Έχει σχεδιαστεί για γρήγορο πειραματισμό, επιτρέποντας στους χρήστες να ορίζουν και να εκπαιδεύουν εύκολα νευρωνικά δίκτυα με ελάχιστο κώδικα. Το Keras εκτελείται πάνω από το TensorFlow, παρέχοντας μια φιλική προς το χρήστη διεπαφή για τις προηγμένες δυνατότητες του TensorFlow[28].
Επιλέχθηκε για την απλότητα και την ευελιξία του, επιτρέποντας τη γρήγορη πρωτοτυποποίηση μοντέλων βαθιάς μάθησης. Οι υψηλού επιπέδου αφαιρέσεις του διευκόλυναν την εστίαση στην αρχιτεκτονική του μοντέλου και την απόδοση αντί να ασχολούμαστε με κώδικα χαμηλού επιπέδου. Χρησιμοποιήθηκε για την κατασκευή και την εκπαίδευση μοντέλων βαθιάς μάθησης για την εξαγωγή χαρακτηριστικών από εικόνες υπογραφών. Χρησιμοποιώντας το

Keras, μπορέσαμε να υλοποιήσουμε και να τελειοποιήσουμε αρχιτεκτονικές όπως τα VGG16, DenseNet121 και MobileNet, τα οποία εξήγαγαν σημαντικά χαρακτηριστικά από εικόνες υπογραφών που ήταν κρίσιμα για την ανίχνευση πλαστογραφιών[26][28].
Το διαισθητικό API της Keras κατέστησε αποτελεσματικό τον πειραματισμό με διαφορετικά μοντέλα βαθιάς μάθησης και τη γρήγορη αξιολόγηση της απόδοσής τους σε δεδομένα υπογραφών. Η συμβατότητά του με το TensorFlow παρείχε την απαραίτητη υπολογιστική ισχύ για την αποτελεσματική εκπαίδευση των μοντέλων, με αποτέλεσμα την καλύτερη εξαγωγή χαρακτηριστικών και τη βελτιωμένη ανίχνευση πλαστών υπογραφών.

4.4 Scikit-learn

Το Scikit-learn είναι μια ευρέως χρησιμοποιούμενη βιβλιοθήκη Python για μηχανική μάθηση. Παρέχει απλά και αποτελεσματικά εργαλεία για την εξόρυξη και ανάλυση δεδομένων, συμπεριλαμβανομένου ενός ευρέος φάσματος αλγορίθμων μηχανικής μάθησης, όπως SVM, KNN, Random Forests, Logistic Regression και άλλα[26].
Επιλέχθηκε για την ολοκληρωμένη συλλογή αλγορίθμων μηχανικής μάθησης και την απρόσκοπτη ενσωμάτωσή του με άλλες βιβλιοθήκες Python, όπως η NumPy και η Pandas.Ο συνεπής σχεδιασμός του API του κατέστησε εύκολη την εκπαίδευση, την αξιολόγηση και τη σύγκριση διαφορετικών ταξινομητών μηχανικής μάθησης στα σύνολα χαρακτηριστικών που εξήχθησαν από εικόνες υπογραφών. Χρησιμοποιήθηκε για την υλοποίηση παραδοσιακών αλγορίθμων μηχανικής μάθησης (π.χ. SVM, KNN, Decision Trees, Random Forest, Naive Bayes) που ταξινόμησαν τα χαρακτηριστικά που εξήχθησαν από τα μοντέλα βαθιάς μάθησης.Αυτοί οι ταξινομητές εκπαιδεύτηκαν για να διακρίνουν μεταξύ γνήσιων και πλαστών υπογραφών με βάση τα εξαγόμενα διανύσματα χαρακτηριστικών[26][27][28].
Οι αλγόριθμοι του Scikit-learn είναι κατάλληλοι για την ταξινόμηση διανυσμάτων χαρακτηριστικών υψηλής διάστασης που προέρχονται από εικόνες.Χρησιμοποιώντας το Scikit-learn, μπορέσαμε να αξιολογήσουμε αποτελεσματικά την απόδοση διαφόρων ταξινομητών και να τους βελτιστοποιήσουμε για εργασίες ανίχνευσης πλαστογραφίας υπογραφών, με αποτέλεσμα υψηλή ακρίβεια και ισχυρή ταξινόμηση[27].

4.5 NumPy

Το NumPy παρέχει υποστήριξη για πολυδιάστατους πίνακες και πίνακες, καθώς και μια μεγάλη συλλογή μαθηματικών συναρτήσεων που λειτουργούν σε αυτές τις δομές δεδομένων[29].
Επιλέχθηκε για την αποτελεσματικότητά του στο χειρισμό μεγάλων συνόλων δεδομένων και την εκτεταμένη λειτουργικότητά του για αριθμητικές πράξεις. Δεδομένου ότι οι εικόνες υπογραφών αναπαρίστανται ως πίνακες τιμών εικονοστοιχείων, το NumPy ήταν απαραίτητο για τον χειρισμό και την προεπεξεργασία αυτών των πινάκων πριν από την τροφοδότησή τους

σε μοντέλα μηχανικής μάθησης και βαθιάς μάθησης. Στην παρούσα πτυχιακή εργασία, το NumPy χρησιμοποιήθηκε για την εκτέλεση ενός ευρέος φάσματος λειτουργιών στα δεδομένα εικόνων, συμπεριλαμβανομένης της αλλαγής μεγέθους, της κανονικοποίησης και του μετασχηματισμού των εικόνων υπογραφής σε μορφές συμβατές με τα μοντέλα βαθιάς μάθησης.Οι πίνακες NumPy χρησιμοποιήθηκαν επίσης για την αποθήκευση και τη διαχείριση διανυσμάτων χαρακτηριστικών που εξήχθησαν από τις εικόνες[28][29].
Η ικανότητα της NumPy να χειρίζεται αποτελεσματικά μεγάλους πίνακες την κατέστησε ζωτικής σημασίας για την επεξεργασία εικόνων υπογραφών.Οι λειτουργίες του σε πίνακες μας επέτρεψαν να χειριστούμε τα δεδομένα γρήγορα, διασφαλίζοντας ότι τα μοντέλα βαθιάς μάθησης λάμβαναν υψηλής ποιότητας, τυποποιημένες εισροές για καλύτερη αναγνώριση εικόνων και ανίχνευση πλαστογραφίας.

4.6 Pandas

Η Pandas είναι μια ισχυρή βιβλιοθήκη ανάλυσης και χειρισμού δεδομένων που βασίζεται στη NumPy. Παρέχει δομές δεδομένων, όπως τα DataFrames, που επιτρέπουν την εύκολη επεξεργασία δεδομένων σε μορφή πίνακα, συμπεριλαμβανομένης της δυνατότητας χειρισμού ελλιπών δεδομένων, φιλτραρίσματος και αναδιαμόρφωσης[27].
Επιλέχθηκε για την ικανότητά του να διαχειρίζεται και να προεπεξεργάζεται αποτελεσματικά μεγάλα σύνολα δεδομένων, διευκολύνοντας τον καθαρισμό και την προετοιμασία των δεδομένων υπογραφής για την εκπαίδευση μοντέλων. Υπερέχει στο χειρισμό δομημένων δεδομένων, κάτι που ήταν απαραίτητο για την οργάνωση των συνόλων δεδομένων υπογραφών και την ενσωμάτωσή τους σε μοντέλα μηχανικής μάθησης.Χρησιμοποιήθηκε για την προεπεξεργασία των συνόλων δεδομένων υπογραφών, τη φόρτωση των δεδομένων, το φιλτράρισμα των μη έγκυρων καταχωρίσεων και ο μετασχηματισμός των συνόλων δεδομένων σε μορφές που θα μπορούσαν να χρησιμοποιηθούν άμεσα από τα μοντέλα μηχανικής μάθησης. Το Pandas βοήθησε επίσης στην επιλογή χαρακτηριστικών και στην οργάνωση των δεδομένων για σκοπούς εκπαίδευσης και αξιολόγησης[27].
Η ικανότητα του Pandas να χειρίζεται και να μετασχηματίζει μεγάλα σύνολα δεδομένων ήταν ζωτικής σημασίας για την προετοιμασία των δεδομένων υπογραφών για ανάλυση. Εξασφαλίζοντας ότι τα δεδομένα ήταν καθαρά και καλά δομημένα, το Pandas έπαιξε βασικό ρόλο στη βελτιστοποίηση της απόδοσης των μοντέλων μηχανικής μάθησης και βαθιάς μάθησης που χρησιμοποιήθηκαν για την ανίχνευση πλαστογραφίας.

4.7 Matplotlib και Seaborn

Το Matplotlib είναι μια βιβλιοθήκη γραφικών παραστάσεων 2D στην Python που χρησιμοποιείται για τη δημιουργία στατικών, κινούμενων και διαδραστικών απεικονίσεων. Το Seaborn είναι

μια βιβλιοθήκη ανώτερου επιπέδου που βασίζεται στην Matplotlib και έχει σχεδιαστεί για τη δημιουργία πιο εξελιγμένων και στατιστικά τεκμηριωμένων οπτικοποιήσεων[30].
Η Matplotlib και η Seaborn επιλέχθηκαν για τις δυνατότητές τους στη δημιουργία σαφών και κατατοπιστικών οπτικοποιήσεων. Αυτές οι βιβλιοθήκες μας επέτρεψαν να οπτικοποιήσουμε την απόδοση των μοντέλων, συμπεριλαμβανομένων των διαγραμμάτων απωλειών και των πινάκων σύγχυσης, τα οποία ήταν κρίσιμα για την κατανόηση και την επικοινωνία της αποτελεσματικότητας των μοντέλων. Και οι δύο βιβλιοθήκες χρησιμοποιήθηκαν για τη δημιουργία γραφημάτων που οπτικοποιούσαν την απόδοση των μοντέλων μηχανικής μάθησης και βαθιάς μάθησης. Αυτά περιλάμβαναν γραφήματα που έδειχναν την ακρίβεια και την απώλεια των μοντέλων με την πάροδο του χρόνου, καθώς και πίνακες σύγχυσης που απεικόνιζαν πόσο καλά τα μοντέλα ήταν σε θέση να ταξινομήσουν τις γνήσιες έναντι των πλαστών υπογραφών[30].
Η οπτικοποίηση διαδραματίζει κρίσιμο ρόλο στην αξιολόγηση της απόδοσης των μοντέλων. Η δυνατότητα δημιουργίας γραφικών παραστάσεων διαγραμμάτων απώλειας μας επέτρεψε να εντοπίσουμε πιθανά προβλήματα με την εκπαίδευση των μοντέλων, ενώ οι πίνακες σύγχυσης παρείχαν εικόνα της ακρίβειας ταξινόμησης των μοντέλων στη διάκριση πλαστών υπογραφών από γνήσιες.

4.8 OpenCV

Το OpenCV (Open Source Computer Vision Library) είναι μια βιβλιοθήκη ανοικτού κώδικα που έχει σχεδιαστεί για εργασίες υπολογιστικής όρασης και επεξεργασίας εικόνας σε πραγματικό χρόνο. Παρέχει ένα ευρύ φάσμα λειτουργιών για τον χειρισμό εικόνων, όπως φιλτράρισμα, ανίχνευση ακμών και γεωμετρικούς μετασχηματισμούς.Το OpenCV χρησιμοποιείται ευρέως σε εφαρμογές μηχανικής μάθησης όπου η ποιότητα της εισόδου εικόνας είναι κρίσιμη για την ακρίβεια των μοντέλων.
Το OpenCV επιλέχθηκε για το εκτεταμένο σύνολο εργαλείων που επιτρέπει την αποτελεσματική προεπεξεργασία εικόνων, η οποία είναι ζωτικής σημασίας για τη διασφάλιση της τυποποίησης των εικόνων υπογραφής πριν από την εισαγωγή τους σε μοντέλα μηχανικής μάθησης και βαθιάς μάθησης. Η δυνατότητα αυτοματοποίησης των λειτουργιών βελτίωσης και προεπεξεργασίας εικόνων, όπως η αφαίρεση θορύβου, η αλλαγή μεγέθους και η ανίχνευση ακμών, κατέστησε το OpenCV βασικό συστατικό του συστήματός μας[31].
Στην παρούσα πτυχιακή εργασία, το OpenCV χρησιμοποιήθηκε για την προεπεξεργασία των εικόνων υπογραφής πριν αυτές περάσουν σε μοντέλα βαθιάς μάθησης για την εξαγωγή χαρακτηριστικών. Αυτά τα βήματα προεπεξεργασίας περιλάμβαναν τη μετατροπή των εικόνων σε κλίμακα του γκρι, την εφαρμογή της θολούρας Gauss για τη μείωση του θορύβου, την αλλαγή μεγέθους των εικόνων ώστε να ανταποκρίνονται στις απαιτήσεις διαστάσεων των μοντέλων CNN και τη χρήση τεχνικών ανίχνευσης ακμών για την ανάδειξη των σημαντικών χαρακτηριστικών των υπογραφών, όπως τα μοτίβα των κινήσεων γραφής.Αυτές οι τεχνικές προεπεξερ-

γασίας βοήθησαν να διασφαλιστεί ότι τα δεδομένα που εισήχθησαν στα μοντέλα ήταν καθαρά, συνεπή και τόνιζαν τα βασικά στοιχεία της υπογραφής.
Η αποτελεσματικότητα του OpenCV στην αναγνώριση εικόνων και συγκεκριμένα στην ανίχνευση πλαστογραφίας υπογραφών έχει τις ρίζες της στην ικανότητά του να βελτιώνει την ποιότητα των δεδομένων εισόδου. Βελτιώνοντας τα κρίσιμα χαρακτηριστικά των εικόνων υπογραφών και αφαιρώντας τον άσχετο θόρυβο, το OpenCV διευκόλυνε την ικανότητα των μοντέλων να εστιάζουν στα ουσιώδη στοιχεία που διακρίνουν τις γνήσιες υπογραφές από τις πλαστές.Αυτή η προεπεξεργασία βελτίωσε την ακρίβεια των αλγορίθμων ταξινόμησης και βοήθησε στην επίτευξη πιο αξιόπιστων αποτελεσμάτων ανίχνευσης, καθιστώντας το OpenCV ένα ζωτικής σημασίας εργαλείο στο συνολικό σύστημα [31].

4.9 Pickle

Το Pickle είναι μια βιβλιοθήκη Python που χρησιμοποιείται για τη σειριοποίηση και την αποσειριοποίηση αντικειμένων Python, η οποία περιλαμβάνει την αποθήκευση και τη φόρτωση μοντέλων μηχανικής μάθησης, πινάκων και άλλων δομών δεδομένων.Παρέχει μια απλή και αποτελεσματική μέθοδο για την αποθήκευση σύνθετων μοντέλων με τις παραμέτρους τους, εξασφαλίζοντας ότι μπορούν να επαναχρησιμοποιηθούν ή να διαμοιραστούν χωρίς να χρειάζεται να τα επανεκπαιδεύσουμε[32].
Επιλέχθηκε για την ικανότητά του να διατηρεί τα εκπαιδευμένα μοντέλα μηχανικής μάθησης σε μορφή που μπορεί εύκολα να αποθηκευτεί και να επαναφορτωθεί για μελλοντική χρήση. Αυτό ήταν ζωτικής σημασίας στη πτυχιακή εργασία μας, καθώς μας επέτρεψε να αποθηκεύσουμε βελτιστοποιημένα μοντέλα μετά την εκπαίδευση και τη δοκιμή, αποτρέποντας έτσι την ανάγκη επανεκπαίδευσης κατά τη διάρκεια μεταγενέστερων αξιολογήσεων ή αναπτύξεων. Χρησιμοποιήθηκε για την αποθήκευση των εκπαιδευμένων ταξινομητών και των μοντέλων βαθιάς μάθησης αφού είχαν βελτιστοποιηθεί και επικυρωθεί. Αυτό μας επέτρεψε να επαναφορτώσουμε τα μοντέλα ανά πάσα στιγμή, επιτρέποντας την περαιτέρω ανάλυση, δοκιμή ή ανάπτυξη χωρίς επανεκπαίδευση. Με την αποθήκευση των μοντέλων, εξασφαλίσαμε ότι οι ακριβείς διαμορφώσεις και η εκμάθηση που προϋπήρξε θα μπορούσαν να επαναχρησιμοποιηθούν, διατηρώντας την απόδοση του συστήματος και διευκολύνοντας την αναπαραγωγιμότητα στα πειράματα, μειώνοντας τον χρόνο εκμάθησης και τους υπολογιστικούς πόρους.
Ο ρόλος του Pickle στην αναγνώριση εικόνων και στην ανίχνευση πλαστογραφίας υπογραφών ήταν ζωτικής σημασίας για τον εξορθολογισμό της ροής εργασίας. Η ικανότητά του να σειριοποιεί γρήγορα τα μοντέλα επέτρεψε στο σύστημα να διατηρεί σταθερή απόδοση.Με την αποτελεσματική διαχείριση της αποθήκευσης των εκπαιδευμένων μοντέλων, το Pickle βοήθησε να διασφαλιστεί ότι το σύστημα παρέμεινε επεκτάσιμο και προσαρμόσιμο, ικανό να διαχειρίζεται πρόσθετα δεδομένα και εξελισσόμενες ανάγκες[32].

Κεφάλαιο 5

Εφαρμογή μοντέλων ανίχνευσης πλαστογραφίας υπογραφών

Η υλοποίηση του συστήματος ανίχνευσης πλαστότητας υπογραφών περιλάμβανε μια δομημένη προσέγγιση που συνδύαζε τόσο τη βαθιά μάθηση όσο και τις παραδοσιακές τεχνικές μηχανικής μάθησης. Ο στόχος ήταν να δημιουργηθεί ένα σύστημα ικανό να διακρίνει με ακρίβεια μεταξύ γνήσιων και πλαστών υπογραφών αξιοποιώντας προηγμένες μεθόδους εξαγωγής χαρακτηριστικών και ισχυρούς αλγορίθμους ταξινόμησης. Στο παρόν κεφάλαιο περιγράφεται η βήμα προς βήμα διαδικασία που χρησιμοποιήθηκε για την ανάπτυξη, την εκπαίδευση και την αξιολόγηση των μοντέλων στο πλαίσιο του συστήματός μας.

5.1 Προεπεξεργασία δεδομένων

Το πρώτο και αναμφισβήτητα ένα από τα πιο σημαντικά βήματα στην υλοποίηση του συστήματος ανίχνευσης πλαστογραφίας υπογραφών ήταν η προεπεξεργασία των δεδομένων. Η κατάλληλη προετοιμασία των δεδομένων πριν από την εισαγωγή τους στα μοντέλα είναι ζωτικής σημασίας για τη διασφάλιση της βέλτιστης απόδοσης του συστήματος, ιδίως όταν πρόκειται για δεδομένα εικόνας. Στην παρούσα πτυχιακή εργασία, το στάδιο της προεπεξεργασίας επικεντρώθηκε στη μετατροπή των ακατέργαστων εικόνων υπογραφών σε μορφή κατάλληλη για εξαγωγή χαρακτηριστικών και ταξινόμηση, ενώ παράλληλα βελτιώθηκε η ποιότητα της εικόνας για τη βελτίωση της ακρίβειας του μοντέλου.
Η βιβλιοθήκη OpenCV χρησιμοποιήθηκε για τη διεκπεραίωση των εργασιών προεπεξεργασίας. Οι εικόνες υπογραφών μετατράπηκαν πρώτα σε κλίμακα του γκρι, μειώνοντας τη διαστατικότητα των δεδομένων και εξαλείφοντας τις περιττές έγχρωμες πληροφορίες, οι οποίες δεν είναι συνήθως σχετικές για την επαλήθευση υπογραφών. Η μετατροπή σε κλίμακα του γκρι βοηθά επίσης τα μοντέλα να εστιάζουν στα βασικά χαρακτηριστικά των υπογραφών, όπως τα μοτίβα και τα σχήματα των γραφογραμμών, χωρίς να αποσπούν την προσοχή τους οι

διακυμάνσεις του χρώματος.
Αφού οι εικόνες μετατράπηκαν σε κλίμακα του γκρι, εφαρμόσαμε θόλωση Gauss για να μειώσουμε το θόρυβο. Ο θόρυβος στις εικόνες μπορεί να προκύψει από διάφορους παράγοντες, όπως η διαδικασία σάρωσης, οι κηλίδες μελανιού ή η υφή του χαρτιού, και μπορεί να επηρεάσει αρνητικά την απόδοση των μοντέλων βαθιάς μάθησης. Με την εφαρμογή της Gaussian blur, καταφέραμε να εξομαλύνουμε τις εικόνες και να μειώσουμε τον ανεπιθύμητο θόρυβο, κάνοντας τα βασικά χαρακτηριστικά των υπογραφών να ξεχωρίζουν πιο καθαρά.
Μετά τη μείωση του θορύβου, οι εικόνες άλλαξαν μέγεθος σε τυποποιημένο μέγεθος 224x224 εικονοστοιχείων. Αυτό το βήμα ήταν απαραίτητο για να διασφαλιστεί ότι οι εικόνες υπογραφών θα μπορούσαν να τροφοδοτηθούν στα προ-εκπαιδευμένα μοντέλα βαθιάς μάθησης, τα οποία απαιτούν ένα σταθερό μέγεθος εισόδου. Η αλλαγή μεγέθους των εικόνων εξασφάλισε επίσης ότι όλες οι υπογραφές αναπαρίσταντο σε ίση βάση, αποτρέποντας τις διακυμάνσεις στο μέγεθος της εικόνας από το να επηρεάσουν την ικανότητα του μοντέλου να μαθαίνει σχετικά μοτίβα.
Για την περαιτέρω ενίσχυση των βασικών χαρακτηριστικών των υπογραφών, εφαρμόσαμε ανίχνευση ακμών χρησιμοποιώντας τον αλγόριθμο ανίχνευσης ακμών Canny. Η ανίχνευση αυτή των ακμών αναδεικνύει τα περιγράμματα και τα όρια των πινελιών της υπογραφής, τα οποία αποτελούν κρίσιμα χαρακτηριστικά για τη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών. Δίνοντας έμφαση στη δομή των υπογραφών, η ανίχνευση ακμών βοηθά τα μοντέλα να επικεντρωθούν στις πιο σημαντικές πτυχές των εικόνων.

```python
import cv2
import numpy as np

# Function to load and preprocess images
def preprocess_image(filepath):
    image = cv2.imread(filepath, cv2.IMREAD_GRAYSCALE)
    image = cv2.GaussianBlur(image, (5, 5), 0)  # Noise removal
    image = cv2.resize(image, (224, 224))  # Resize to fit model input
    edges = cv2.Canny(image, 100, 200)  # Edge detection
    return edges / 255.0  # Normalize pixel values

# Example usage
preprocessed_image = preprocess_image('signature.jpg')
```

Listing 5.1: Preprocessing Python Code

Αφού οι εικόνες προεπεξεργάστηκαν, κανονικοποιήθηκαν με κλιμάκωση των τιμών των εικονοστοιχείων σε ένα εύρος μεταξύ 0 και 1. Αυτό το βήμα κανονικοποίησης είναι κρίσιμο για να διασφαλιστεί ότι τα μοντέλα δεν επηρεάζονται από τις απόλυτες τιμές έντασης των εικονοστοιχείων, επιτρέποντάς τους να εστιάσουν στις σχετικές διαφορές στις τιμές των εικονοστοιχείων, οι οποίες είναι περισσότερο ενδεικτικές των μοναδικών μοτίβων στην υπογραφή.
Στη συνέχεια, οι προεπεξεργασμένες εικόνες χωρίστηκαν σε σύνολα εκπαίδευσης, επικύρω-

σης και δοκιμής με διαχωρισμό 80/20. Το σύνολο εκπαίδευσης χρησιμοποιήθηκε για την εκπαίδευση των μοντέλων βαθιάς μάθησης, ενώ το σύνολο επικύρωσης χρησιμοποιήθηκε για την παρακολούθηση της απόδοσης και την προσαρμογή των υπερπαραμέτρων κατά τη διάρκεια της εκπαίδευσης. Το σύνολο δοκιμής προοριζόταν για την τελική αξιολόγηση της ικανότητας των μοντέλων να γενικεύουν σε αόρατα δεδομένα. Αυτός ο διαχωρισμός εξασφάλισε ότι τα μοντέλα εκπαιδεύτηκαν σε ένα ποικίλο σύνολο δεδομένων, επιτρέποντάς τους να μάθουν ισχυρά πρότυπα και να γενικεύσουν αποτελεσματικά σε νέες, προηγουμένως αθέατες υπογραφές.
Η προεπεξεργασία των δεδομένων έπαιξε καθοριστικό ρόλο στη διασφάλιση ότι το σύστημα ανίχνευσης πλαστογραφίας υπογραφών θα μπορούσε να μάθει αποτελεσματικά από τα δεδομένα. Βελτιώνοντας την ποιότητα των εικόνων και τυποποιώντας την είσοδο, δώσαμε στα μοντέλα βαθιάς μάθησης τα καλύτερα δυνατά δεδομένα, επιτρέποντάς τους να επικεντρωθούν στην εκμάθηση των βασικών χαρακτηριστικών που είναι απαραίτητα για την ακριβή ταξινόμηση υπογραφών.

5.2 Εξαγωγή χαρακτηριστικών με χρήση μοντέλων βαθιάς μάθησης

Ένα κρίσιμο βήμα στην υλοποίηση του συστήματος ανίχνευσης πλαστογραφίας υπογραφών ήταν η εξαγωγή χαρακτηριστικών από τις εικόνες υπογραφών με τη χρήση προεκπαιδευμένων μοντέλων βαθιάς μάθησης. Η εξαγωγή χαρακτηριστικών επιτρέπει στο σύστημα να συλλαμβάνει σύνθετα μοτίβα και χαρακτηριστικά από τις εικόνες που είναι απαραίτητα για τη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών. Στην παρούσα πτυχιακή εργασία, χρησιμοποιήθηκαν για τον σκοπό αυτό διάφορες αρχιτεκτονικές νευρωνικών δικτύων συνελικτικού τύπου (CNN), συμπεριλαμβανομένων των VGG16, DenseNet121, MobileNetV2 και EfficientNetV2S.
Τα μοντέλα βαθιάς μάθησης που επιλέχθηκαν είχαν προ-εκπαιδευτεί στο μεγάλης κλίμακας σύνολο δεδομένων ImageNet, το οποίο τους παρείχε μια ευρεία γνώση των οπτικών χαρακτηριστικών που μπορούσαν να μεταφερθούν στο έργο της επαλήθευσης υπογραφών. Χρησιμοποιώντας τη μάθηση μεταφοράς, προσαρμόσαμε αυτά τα προ-εκπαιδευμένα μοντέλα στο συγκεκριμένο πρόβλημα της ανίχνευσης πλαστογραφίας υπογραφών με τη λεπτομερή ρύθμιση των τελικών επιπέδων τους. Η εκμάθηση μεταφοράς πλεονεκτεί σε περιπτώσεις όπου το σύνολο δεδομένων είναι σχετικά μικρό, καθώς επιτρέπει στο μοντέλο να αξιοποιήσει την εκτεταμένη γνώση που αποκτήθηκε από μεγάλα σύνολα δεδομένων και να την εφαρμόσει στο πιο εξειδικευμένο έργο.
Τα προ-εκπαιδευμένα μοντέλα υλοποιήθηκαν με τη χρήση των TensorFlow και Keras. Η συνελικτική βάση κάθε μοντέλου ήταν παγωμένη, πράγμα που σημαίνει ότι τα βάρη στα προηγούμενα στρώματα (τα οποία καταγράφουν γενικά χαρακτηριστικά της εικόνας, όπως ακμές, σχήματα και υφές) διατηρήθηκαν από την εκπαίδευση στο ImageNet. Μόνο τα ανώτερα στρώ-

ματα των μοντέλων επανεκπαιδεύτηκαν στο σύνολο δεδομένων υπογραφών, διασφαλίζοντας ότι τα μοντέλα θα μπορούσαν να προσαρμοστούν στα ειδικά χαρακτηριστικά των εικόνων χωρίς να χάσουν τα γενικά οπτικά χαρακτηριστικά που είχαν μάθει από το ευρύτερο σύνολο δεδομένων.

Για να μειώσουμε τη διαστατικότητα των χαρτών χαρακτηριστικών που παράγονται από τα CNN, εφαρμόσαμε ένα στρώμα Global Average Pooling μετά το τελευταίο επίπεδο συνελίξεων κάθε μοντέλου. Αυτό το βήμα μετέτρεψε την υψηλής διάστασης έξοδο του CNN σε ένα συμπαγές διάνυσμα χαρακτηριστικών, το οποίο διατήρησε τις πιο σχετικές πληροφορίες, ενώ μείωσε σημαντικά το μέγεθος των δεδομένων. Αυτά τα διανύσματα χαρακτηριστικών χρησιμοποιήθηκαν στη συνέχεια ως είσοδος για τους επόμενους ταξινομητές μηχανικής μάθησης.

Μόλις εξήχθησαν τα διανύσματα χαρακτηριστικών, χρησιμοποιήθηκαν ως είσοδοι για τους παραδοσιακούς ταξινομητές μηχανικής μάθησης. Κάθε προ-εκπαιδευμένο μοντέλο παρήγαγε ένα διαφορετικό σύνολο διανυσμάτων χαρακτηριστικών, αποτυπώνοντας διαφορετικά επίπεδα λεπτομέρειας και μοτίβων στις εικόνες υπογραφών. Για παράδειγμα, το VGG16 εστιάζει σε βαθύτερα επίπεδα αφαίρεσης, ενώ το EfficientNetV2S υπερέχει στην εξισορρόπηση ακρίβειας και υπολογιστικής απόδοσης.

Χρησιμοποιώντας πολλαπλά προ-εκπαιδευμένα μοντέλα για την εξαγωγή χαρακτηριστικών, εξασφαλίσαμε ότι το σύστημα κατέγραφε μια μεγάλη ποικιλία χαρακτηριστικών της εικόνας, βελτιώνοντας την ικανότητά του να διακρίνει μεταξύ γνήσιων και πλαστών υπογραφών. Αυτό το ποικιλόμορφο σύνολο χαρακτηριστικών παρείχε μια ισχυρή βάση για τους ταξινομητές μηχανικής μάθησης για τον ακριβή εντοπισμό πλαστών υπογραφών με βάση τις λεπτές διαφορές στα εξαγόμενα χαρακτηριστικά.

Η χρήση μοντέλων βαθιάς μάθησης για την εξαγωγή χαρακτηριστικών ήταν ζωτικής σημασίας στην παρούσα πτυχιακή εργασία, καθώς επέτρεψε στο σύστημα να μάθει αυτόματα τα σχετικά πρότυπα από τις εικόνες υπογραφών, αντί να βασίζεται σε χειροκίνητα κατασκευασμένα χαρακτηριστικά. Αυτή η προσέγγιση βελτίωσε σημαντικά την ικανότητα του συστήματος να ανιχνεύει πλαστογραφίες, αξιοποιώντας τη δύναμη των CNN για την επεξεργασία πολύπλοκων οπτικών δεδομένων με ιδιαίτερα αποτελεσματικό τρόπο.

```
from tensorflow.keras.applications import VGG16, DenseNet121, MobileNetV2,
    EfficientNetV2S
from tensorflow.keras.models import Sequential
from tensorflow.keras.layers import GlobalAveragePooling2D

# Load pre-trained models for feature extraction
base_model = VGG16(weights='imagenet', include_top=False, input_shape=(224,
    224, 3))

# Add global average pooling layer to reduce dimensionality of features
model = Sequential([
    base_model,
```

```
    GlobalAveragePooling2D()
])

# Extract features from the signature images
features = model.predict(np.array([preprocessed_image]))  # Example with a
    single preprocessed image

print("Extracted Features Shape:", features.shape)
```

Listing 5.2: Preprocessing Python Code

5.3 Ταξινόμηση με μηχανική μάθηση

Αφού εξήχθησαν τα χαρακτηριστικά από τα μοντέλα βαθιάς μάθησης, χρησιμοποιήθηκαν παραδοσιακοί αλγόριθμοι μηχανικής μάθησης για την ταξινόμηση των υπογραφών ως γνήσιες ή πλαστές. Αυτοί οι ταξινομητές υλοποιήθηκαν χρησιμοποιώντας τη βιβλιοθήκη Scikit-learn, η οποία προσφέρει ένα ευρύ φάσμα αλγορίθμων που είναι κατάλληλοι για εργασίες επιβλεπόμενης μάθησης. Οι ταξινομητές που χρησιμοποιήθηκαν στην παρούσα πτυχιακή εργασία περιλαμβάνουν τις μηχανές διανυσμάτων υποστήριξης (SVM), τους K-Nearest Neighbors (KNN), τα δέντρα αποφάσεων, τα τυχαία δάση, τη λογιστική παλινδρόμηση και τον Naive Bayes.
Κάθε ταξινομητής εκπαιδεύτηκε στα διανύσματα χαρακτηριστικών που εξήχθησαν από τα μοντέλα βαθιάς μάθησης. Η διαδικασία εκπαίδευσης ξεκίνησε με τον διαχωρισμό των εξαχθέντων χαρακτηριστικών σε σύνολα δεδομένων εκπαίδευσης και δοκιμών χρησιμοποιώντας έναν διαχωρισμό 80/20, ώστε να διασφαλιστεί ότι τα μοντέλα θα μπορούσαν να γενικεύσουν καλά σε αόρατα δεδομένα. Αφού προετοιμάστηκαν τα δεδομένα, κάθε ταξινομητής εκπαιδεύτηκε χρησιμοποιώντας τα εξαγόμενα διανύσματα χαρακτηριστικών ως εισόδους και τις αντίστοιχες ετικέτες (γνήσια ή πλαστά) ως στόχο εξόδου.
Για παράδειγμα, ο ταξινομητής SVM εκπαιδεύτηκε χρησιμοποιώντας έναν γραμμικό πυρήνα, ο οποίος επιλέχθηκε με βάση τη βελτιστοποίηση της αναζήτησης πλέγματος. Αυτή η διαδικασία βελτιστοποίησης περιελάμβανε τη δοκιμή διαφορετικών συνδυασμών υπερπαραμέτρων, όπως ο τύπος του πυρήνα και οι παράμετροι κανονικοποίησης, για τον εντοπισμό της καλύτερης διαμόρφωσης για τον ταξινομητή. Ομοίως, ο ταξινομητής Random Forest βελτιστοποιήθηκε με τη ρύθμιση του αριθμού των δέντρων και του μέγιστου βάθους των δέντρων. Ο ταξινομητής K-Nearest Neighbors βελτιστοποιήθηκε μεταβάλλοντας τον αριθμό των γειτόνων που λαμβάνονται υπόψη κατά την ταξινόμηση, διασφαλίζοντας ότι επιλέγεται η καταλληλότερη διαμόρφωση για κάθε αλγόριθμο.

```
from sklearn.svm import SVC
from sklearn.ensemble import RandomForestClassifier
from sklearn.neighbors import KNeighborsClassifier
from sklearn.model_selection import train_test_split
```

```
5
6  # Split data into training and testing sets
7  X_train, X_test, y_train, y_test = train_test_split(features, labels,
       test_size=0.2, random_state=42)
8
9  # Train a Support Vector Machine (SVM) classifier
10 svm_classifier = SVC(kernel='linear')
11 svm_classifier.fit(X_train, y_train)
12
13 # Train a Random Forest classifier
14 rf_classifier = RandomForestClassifier(n_estimators=100)
15 rf_classifier.fit(X_train, y_train)
16
17 # Train a K-Nearest Neighbors (KNN) classifier
18 knn_classifier = KNeighborsClassifier(n_neighbors=5)
19 knn_classifier.fit(X_train, y_train)
```

Listing 5.3: Preprocessing Python Code

Μετά την εκπαίδευση, κάθε ταξινομητής αξιολογήθηκε στο σύνολο δεδομένων δοκιμής για να προσδιοριστεί η απόδοσή του. Οι ταξινομητές αξιολογήθηκαν με τη χρήση διαφόρων μετρικών, όπως η ακρίβεια, η ευστοχία, η ανάκληση και το F1-score, οι οποίες παρείχαν μια ολοκληρωμένη κατανόηση του πόσο καλά κάθε αλγόριθμος ήταν σε θέση να ταξινομήσει τις υπογραφές. Αυτές οι μετρικές υπολογίστηκαν συγκρίνοντας τις προβλεπόμενες ετικέτες που παρήγαγαν οι ταξινομητές με τις πραγματικές ετικέτες στο σύνολο δοκιμών.
Επιπλέον, δημιουργήθηκαν πίνακες σύγχυσης για κάθε ταξινομητή για την οπτική αναπαράσταση της απόδοσής τους. Αυτοί οι πίνακες παρείχαν πληροφορίες για τον αριθμό των αληθώς θετικών (γνήσιες υπογραφές που ταξινομήθηκαν σωστά), των αληθώς αρνητικών (πλαστές υπογραφές που ταξινομήθηκαν σωστά), των ψευδώς θετικών (γνήσιες υπογραφές που ταξινομήθηκαν εσφαλμένα ως πλαστές) και των ψευδώς αρνητικών (πλαστές υπογραφές που ταξινομήθηκαν εσφαλμένα ως γνήσιες).

```
1  from sklearn.metrics import accuracy_score, precision_score, recall_score,
       f1_score, confusion_matrix
2
3  # Predict using the trained SVM classifier
4  y_pred = svm_classifier.predict(X_test)
5
6  # Calculate evaluation metrics for SVM classifier
7  accuracy = accuracy_score(y_test, y_pred)
8  precision = precision_score(y_test, y_pred, average='weighted')
9  recall = recall_score(y_test, y_pred, average='weighted')
10 f1 = f1_score(y_test, y_pred, average='weighted')
11
12 # Display confusion matrix
```

```
conf_matrix = confusion_matrix(y_test, y_pred)
print("Confusion Matrix:\n", conf_matrix)

# Display evaluation metrics
print(f"Accuracy: {accuracy}, Precision: {precision}, Recall: {recall}, F1-
    Score: {f1}")
```

Listing 5.4: Preprocessing Python Code

Αξιοποιώντας αυτούς τους παραδοσιακούς ταξινομητές μηχανικής μάθησης στα εξαγόμενα διανύσματα χαρακτηριστικών, μπορέσαμε να αξιολογήσουμε την αποτελεσματικότητα διαφορετικών αλγορίθμων στη διάκριση γνήσιων υπογραφών από πλαστές. Οι βελτιστοποιημένοι ταξινομητές πέτυχαν υψηλή ακρίβεια και μπόρεσαν να γενικεύσουν καλά σε αόρατα δεδομένα, καθιστώντας τους κατάλληλους για το έργο της ανίχνευσης πλαστογραφίας υπογραφών. Ο συνδυασμός της βαθιάς μάθησης για την εξαγωγή χαρακτηριστικών και της μηχανικής μάθησης για την ταξινόμηση οδήγησε σε ένα ισχυρό και αποδοτικό σύστημα ικανό να χειριστεί τις πολυπλοκότητες της επαλήθευσης υπογραφών.

5.4 Εκπαίδευση και αξιολόγηση του μοντέλου

Η εκπαίδευση και η αξιολόγηση των μοντέλων ανίχνευσης πλαστογραφίας υπογραφών ήταν κρίσιμα βήματα στη διαδικασία ανάπτυξης. Μετά την προεπεξεργασία των δεδομένων και την εξαγωγή χαρακτηριστικών με τη χρήση των μοντέλων βαθιάς μάθησης, το επόμενο βήμα ήταν η εκπαίδευση των ταξινομητών μηχανικής μάθησης και η αξιολόγηση των επιδόσεών τους στη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών.
Η διαδικασία εκπαίδευσης ξεκίνησε με την τροφοδοσία των προεπεξεργασμένων εικόνων στα μοντέλα εξαγωγής χαρακτηριστικών. Αυτά τα μοντέλα, όπως τα VGG16, DenseNet121, MobileNetV2 και EfficientNetV2S, παρήγαγαν διανύσματα χαρακτηριστικών υψηλού επιπέδου για κάθε εικόνα υπογραφής. Αυτά τα διανύσματα χαρακτηριστικών μεταφέρθηκαν στη συνέχεια στους παραδοσιακούς ταξινομητές μηχανικής μάθησης, όπως οι μηχανές διανυσμάτων υποστήριξης (SVM), οι K-κοντινότεροι γείτονες (KNN), τα δέντρα αποφάσεων, τα τυχαία δάση, η λογιστική παλινδρόμηση και ο Naive Bayes, οι οποίοι ήταν υπεύθυνοι για την ταξινόμηση των υπογραφών ως γνήσιες ή πλαστές.
Για να διασφαλίσουμε ότι τα μοντέλα εκπαιδεύτηκαν αποτελεσματικά, χρησιμοποιήσαμε έναν διαχωρισμό 80/20 για το σύνολο δεδομένων, με το 80/100 των δεδομένων να χρησιμοποιείται για εκπαίδευση και το 20/100 για δοκιμή. Κατά τη διάρκεια της φάσης εκπαίδευσης, κάθε ταξινομητής μηχανικής μάθησης έμαθε να συσχετίζει τα εξαγόμενα χαρακτηριστικά με τις αντίστοιχες ετικέτες (γνήσια ή πλαστά). Η διαδικασία εκπαίδευσης περιελάμβανε πολλαπλές επαναλήψεις, όπου τα μοντέλα προσάρμοζαν τις εσωτερικές τους παραμέτρους για την ελαχιστοποίηση του σφάλματος ταξινόμησης.

Μετά από κάθε εποχή, τα μοντέλα επικυρώνονταν σε ένα ξεχωριστό σύνολο επικύρωσης. Αυτό μας επέτρεψε να παρακολουθούμε την απόδοσή τους και να προσαρμόζουμε τις υπερπαραμέτρους, εάν ήταν απαραίτητο. Για παράδειγμα, ο ρυθμός μάθησης των μοντέλων βαθιάς μάθησης ρυθμίστηκε λεπτομερώς κατά τη διάρκεια της εκπαίδευσης, ενώ παράμετροι όπως ο αριθμός των γειτόνων για το KNN και το μέγιστο βάθος των δέντρων για το Random Forest βελτιστοποιήθηκαν μέσω αναζήτησης πλέγματος και διασταυρούμενης επικύρωσης. Αυτές οι τεχνικές βοήθησαν στη βελτίωση της ακρίβειας των μοντέλων, μειώνοντας παράλληλα τον κίνδυνο υπερπροσαρμογής.

```
from sklearn.model_selection import train_test_split
from sklearn.svm import SVC
from sklearn.ensemble import RandomForestClassifier
from sklearn.neighbors import KNeighborsClassifier

# Split the data into training and testing sets
X_train, X_test, y_train, y_test = train_test_split(features, labels,
    test_size=0.2, random_state=42)

# Train SVM classifier
svm_classifier = SVC(kernel='linear', probability=True)
svm_classifier.fit(X_train, y_train)

# Train Random Forest classifier
rf_classifier = RandomForestClassifier(n_estimators=100)
rf_classifier.fit(X_train, y_train)

# Train K-Nearest Neighbors classifier
knn_classifier = KNeighborsClassifier(n_neighbors=5)
knn_classifier.fit(X_train, y_train)
```

Listing 5.5: Preprocessing Python Code

Η διαδικασία αξιολόγησης επικεντρώθηκε στη μέτρηση των επιδόσεων των ταξινομητών στο σύνολο δοκιμών, το οποίο δεν χρησιμοποιήθηκε κατά την εκπαίδευση. Για την αξιολόγηση των επιδόσεων των μοντέλων χρησιμοποιήθηκαν διάφορες βασικές μετρικές, όπως η ακρίβεια, η ευστοχία, η ανάκληση, το F1-score και η περιοχή κάτω από την καμπύλη ROC (AUC). Αυτές οι μετρικές παρείχαν μια ολοκληρωμένη κατανόηση του πόσο καλά τα μοντέλα μπορούσαν να ταξινομήσουν υπογραφές και να ανιχνεύσουν πλαστογραφίες.
Η ακρίβεια μέτρησε τη συνολική ορθότητα των ταξινομητών, ενώ η ευστοχία επικεντρώθηκε στην αναλογία των σωστά αναγνωρισμένων πλαστογραφιών σε σχέση με το σύνολο των υπογραφών που ταξινομήθηκαν ως πλαστογραφίες. Η ανάκληση μετρούσε το ποσοστό των πραγματικών πλαστογραφιών που αναγνωρίστηκαν σωστά και το F1-score παρείχε ένα ισορροπημένο μέτρο που συνδύαζε τόσο την ακρίβεια όσο και την ανάκληση. Επιπλέον, η AUC χρησιμοποιήθηκε για να αξιολογηθεί η ικανότητα των μοντέλων να διακρίνουν μεταξύ των δύο

κατηγοριών σε όλα τα πιθανά όρια ταξινόμησης.

```
from sklearn.metrics import accuracy_score, precision_score, recall_score,
    f1_score, roc_auc_score, confusion_matrix

# Predict on test data using SVM
y_pred_svm = svm_classifier.predict(X_test)

# Calculate evaluation metrics for SVM
accuracy_svm = accuracy_score(y_test, y_pred_svm)
precision_svm = precision_score(y_test, y_pred_svm, average='weighted')
recall_svm = recall_score(y_test, y_pred_svm, average='weighted')
f1_svm = f1_score(y_test, y_pred_svm, average='weighted')
auc_svm = roc_auc_score(y_test, svm_classifier.predict_proba(X_test),
    multi_class='ovo')

# Display confusion matrix
conf_matrix_svm = confusion_matrix(y_test, y_pred_svm)
print("Confusion Matrix SVM:\n", conf_matrix_svm)

# Print evaluation metrics
print(f"SVM Accuracy: {accuracy_svm}, Precision: {precision_svm}, Recall: {
    recall_svm}, F1-Score: {f1_svm}, AUC: {auc_svm}")
```

Listing 5.6: Preprocessing Python Code

Δημιουργήθηκαν πίνακες σύγχυσης για να απεικονιστεί η απόδοση κάθε ταξινομητή, εμφανίζοντας τον αριθμό των σωστά και λανθασμένα ταξινομημένων υπογραφών. Ο πίνακας παρείχε λεπτομερή ανάλυση των αληθώς θετικών, των αληθώς αρνητικών, των ψευδώς θετικών και των ψευδώς αρνητικών, προσφέροντας βαθύτερη εικόνα των δυνατών και αδύνατων σημείων κάθε μοντέλου.

Για να αποφευχθεί η υπερπροσαρμογή κατά την εκπαίδευση, εφαρμόστηκε πρώιμη διακοπή. Η πρόωρη διακοπή είναι μια τεχνική κανονικοποίησης που σταματά τη διαδικασία εκπαίδευσης όταν η απόδοση του μοντέλου στο σύνολο επικύρωσης παύει να βελτιώνεται μετά από έναν προκαθορισμένο αριθμό εποχών. Αυτό διασφαλίζει ότι το μοντέλο δεν προσαρμόζεται υπερβολικά στα δεδομένα εκπαίδευσης, βελτιώνοντας έτσι τη δυνατότητα γενίκευσής του σε νέα, αόρατα δεδομένα. Επιπλέον, χρησιμοποιήθηκαν σημεία ελέγχου των μοντέλων για την αποθήκευση των μοντέλων με τις καλύτερες επιδόσεις κατά τη διάρκεια της εκπαίδευσης. Αυτό εξασφάλιζε ότι τα τελικά μοντέλα που χρησιμοποιήθηκαν στην αξιολόγηση ήταν οι πιο ακριβείς εκδόσεις που προέκυψαν κατά τη διαδικασία εκπαίδευσης.

```
from tensorflow.keras.callbacks import EarlyStopping, ModelCheckpoint

# Early stopping to prevent overfitting
early_stopping = EarlyStopping(monitor='val_loss', patience=5,
    restore_best_weights=True)
```

```
5
6  # Model checkpoint to save the best model
7  model_checkpoint = ModelCheckpoint('best_model.h5', save_best_only=True,
       monitor='val_accuracy', mode='max')
8
9  # Training the model with early stopping and checkpointing
10 history = model.fit(X_train, y_train, validation_data=(X_val, y_val), epochs
       =50, callbacks=[early_stopping, model_checkpoint])
```

Listing 5.7: Preprocessing Python Code

Συνολικά, ο συνδυασμός ισχυρών στρατηγικών εκπαίδευσης, ολοκληρωμένων μετρικών αξιολόγησης και μηχανισμών έγκαιρης διακοπής επέτρεψε στο σύστημα να παράγει εξαιρετικά ακριβή και αξιόπιστα αποτελέσματα. Αυτή η μεθοδολογία εξασφάλισε ότι τα τελικά μοντέλα ανίχνευσης πλαστογραφίας υπογραφών δεν ήταν μόνο αποτελεσματικά στον εντοπισμό πλαστογραφημένων υπογραφών, αλλά και ικανά να γενικεύουν καλά σε σενάρια του πραγματικού κόσμου.

5.5 Ενσωμάτωση της βαθιάς μάθησης και της μηχανικής μάθησης

Η ενσωμάτωση της εξαγωγής χαρακτηριστικών βαθιάς μάθησης με την παραδοσιακή ταξινόμηση με μηχανική μάθηση είναι μια από τις βασικές καινοτομίες στο σύστημα ανίχνευσης πλαστογραφίας υπογραφών που διαθέτουμε. Αυτή η υβριδική προσέγγιση αξιοποιεί τα πλεονεκτήματα και των δύο παραδειγμάτων, συνδυάζοντας την ικανότητα των μοντέλων βαθιάς μάθησης να μαθαίνουν αυτόματα πολύπλοκα και ταυτόχρονα υψηλής διάστασης χαρακτηριστικά από ακατέργαστα δεδομένα εικόνας με την αποτελεσματικότητα και την ερμηνευσιμότητα των παραδοσιακών αλγορίθμων μηχανικής μάθησης για ταξινόμηση.
Στο πρώτο στάδιο, μοντέλα βαθιάς μάθησης, όπως τα VGG16, DenseNet121, MobileNetV2 και EfficientNetV2S, χρησιμοποιήθηκαν για την εξαγωγή αναπαραστάσεων χαρακτηριστικών από τις εικόνες υπογραφής. Αυτά τα προ-εκπαιδευμένα νευρωνικά δίκτυα συνελικτικού τύπου (CNN), που έχουν εκπαιδευτεί σε σύνολα δεδομένων εικόνων μεγάλης κλίμακας, όπως το ImageNet, είναι ιδιαίτερα αποτελεσματικά στην καταγραφή περίπλοκων μοτίβων και οπτικών ενδείξεων στις εικόνες. Τα μοντέλα βαθιάς μάθησης προσαρμόστηκαν στο συγκεκριμένο έργο της ανίχνευσης πλαστογραφίας υπογραφών με τη χρήση της μάθησης μεταφοράς. Σε αυτή τη ρύθμιση, διατηρήθηκε η συνελικτική βάση κάθε μοντέλου, η οποία καταγράφει γενικά οπτικά χαρακτηριστικά, όπως ακμές και υφές, ενώ τα ανώτερα στρώματα προσαρμόστηκαν ώστε να προσαρμοστούν στα μοναδικά χαρακτηριστικά των εικόνων υπογραφών.
Μετά την εξαγωγή χαρακτηριστικών, η έξοδος των μοντέλων βαθιάς μάθησης - διανύσματα χαρακτηριστικών υψηλού επιπέδου που αντιπροσωπεύουν τις υπογραφές - διαβιβάστηκε σε

παραδοσιακούς ταξινομητές μηχανικής μάθησης για το τελικό βήμα ταξινόμησης. Αυτό το βήμα περιελάμβανε τη λήψη των εξαχθέντων χαρακτηριστικών και τη χρήση τους για να προβλεφθεί εάν μια υπογραφή ήταν γνήσια ή πλαστή.

```
# Extract features from signature images using deep learning models
features_train = model.predict(X_train)  # Extract features from training data
features_test = model.predict(X_test)    # Extract features from test data

# Train a machine learning classifier on the extracted features
svm_classifier.fit(features_train, y_train)

# Use the trained classifier to make predictions on the test set
y_pred = svm_classifier.predict(features_test)
```

Listing 5.8: Preprocessing Python Code

Οι ταξινομητές μηχανικής μάθησης, όπως οι Μηχανές Διανυσμάτων Υποστήριξης (SVM), τα Τυχαία Δάση (Random Forests), οι K-Κοντινότεροι Γείτονες (KNN), η Λογιστική Παλινδρόμηση και τα Δέντρα Αποφάσεων, επιλέχθηκαν για την αποτελεσματικότητά τους στην ταξινόμηση δεδομένων υψηλής διάστασης, όπως τα διανύσματα χαρακτηριστικών που παράγονται από τα CNN. Με την εφαρμογή αυτών των αλγορίθμων στα χαρακτηριστικά που εξάγονται από τα μοντέλα βαθιάς μάθησης, μπορούσαμε να εκτελέσουμε αποτελεσματικά την εργασία ταξινόμησης χωρίς το υπολογιστικό κόστος της εκπαίδευσης ενός μοντέλου βαθιάς μάθησης για ολόκληρη την εργασία.

Οι ταξινομητές βελτιστοποιήθηκαν μέσω τεχνικών όπως η αναζήτηση πλέγματος και η διασταυρούμενη επικύρωση για τον εντοπισμό των καλύτερων υπερπαραμέτρων για κάθε αλγόριθμο. Αυτό εξασφάλισε ότι τα μοντέλα ήταν λεπτομερώς προσαρμοσμένα στα συγκεκριμένα χαρακτηριστικά των διανυσμάτων χαρακτηριστικών που παράγονται από τα μοντέλα βαθιάς μάθησης.

```
# Example: Use GridSearchCV to optimize SVM classifier
from sklearn.model_selection import GridSearchCV

param_grid = {'C': [0.1, 1, 10], 'kernel': ['linear', 'rbf']}
grid = GridSearchCV(SVC(), param_grid, refit=True)
grid.fit(features_train, y_train)

# Predict using the best model found by GridSearchCV
best_model = grid.best_estimator_
y_pred_best = best_model.predict(features_test)
```

Listing 5.9: Preprocessing Python Code

Αυτή η υβριδική προσέγγιση συνδυάζει τη δύναμη της βαθιάς μάθησης για την εξαγωγή σύνθετων χαρακτηριστικών εικόνας με την απλότητα και την ερμηνευσιμότητα των παραδοσιακών ταξινομητών μηχανικής μάθησης. Τα μοντέλα βαθιάς μάθησης μάθαιναν αυτόματα τα

σχετικά μοτίβα στις εικόνες υπογραφών, καταγράφοντας αποχρώσεις όπως οι λεπτές παραλλαγές στο πλάτος της πινελιάς, οι καμπύλες και η υφή που είναι συχνά ενδεικτικές του στυλ γραφής ενός ατόμου. Αυτά τα διαφοροποιημένα χαρακτηριστικά, τα οποία είναι δύσκολο να κατασκευαστούν χειροκίνητα, παρέχουν κρίσιμες πληροφορίες για τη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών.
Αξιοποιώντας αυτά τα αυτόματα εξαγόμενα χαρακτηριστικά, οι παραδοσιακοί ταξινομητές μηχανικής μάθησης ήταν σε θέση να κάνουν ακριβείς προβλέψεις σχετικά με τη γνησιότητα των υπογραφών. Τα μοντέλα βαθιάς μάθησης συμπύκνωσαν αποτελεσματικά τα ακατέργαστα δεδομένα εικόνας σε διανύσματα χαρακτηριστικών υψηλής διάστασης, τα οποία στη συνέχεια χρησίμευσαν ως είσοδος για τους ταξινομητές. Αυτός ο καταμερισμός εργασίας μεταξύ των δύο προτύπων επέτρεψε ένα πιο αποτελεσματικό και ακριβές σύστημα από ό,τι αν χρησιμοποιούσαμε μόνο τη βαθιά μάθηση ή την παραδοσιακή μηχανική μάθηση.
Ένα από τα κύρια πλεονεκτήματα αυτής της ενοποίησης είναι ότι η βαθιά μάθηση υπερέχει στην εξαγωγή χαρακτηριστικών, αλλά μπορεί να είναι υπολογιστικά εντατική όταν χρησιμοποιείται από άκρη σε άκρη, ειδικά με μικρότερα σύνολα δεδομένων όπως το δικό μας. Απομονώνοντας τα μοντέλα βαθιάς μάθησης μόνο στο στάδιο της εξαγωγής χαρακτηριστικών, μετριάσαμε το υπολογιστικό κόστος που συνήθως συνδέεται με την εκπαίδευση μοντέλων βαθιάς μάθησης από το μηδέν, ιδίως σε περιορισμένα δεδομένα. Οι παραδοσιακοί ταξινομητές μηχανικής μάθησης, οι οποίοι είναι λιγότερο απαιτητικοί σε πόρους, χειρίστηκαν την πραγματική εργασία ταξινόμησης, καθιστώντας το σύστημα ταχύτερο και πιο επεκτάσιμο.

5.6 Τελικό σύστημα και ανάπτυξη

Το τελικό σύστημα ανίχνευσης πλαστογραφίας υπογραφών σχεδιάστηκε ως αρθρωτός και επεκτάσιμος αγωγός, συνδυάζοντας προεπεξεργασία εικόνας, εξαγωγή χαρακτηριστικών με χρήση μοντέλων βαθιάς μάθησης και ταξινόμηση με χρήση παραδοσιακών αλγορίθμων μηχανικής μάθησης. Αυτή η σπονδυλωτή αρχιτεκτονική επέτρεψε την ευελιξία προσαρμογής σε διαφορετικά σύνολα δεδομένων και την προσαρμογή σε πρόσθετες κατηγορίες υπογραφών, καθιστώντας το σύστημα εφαρμόσιμο σε διάφορα σενάρια του πραγματικού κόσμου, όπως οι τραπεζικές συναλλαγές, η επαλήθευση νομικών εγγράφων και ο έλεγχος πρόσβασης.
Το σύστημα ξεκινά με την προεπεξεργασία της εικόνας, όπου οι ακατέργαστες εικόνες υπογραφών καθαρίζονται, τυποποιούνται και βελτιώνονται. Τα βήματα προεπεξεργασίας, όπως η μετατροπή των εικόνων σε κλίμακα του γκρι, η εφαρμογή της θολούρας Gauss για την απομάκρυνση του θορύβου, η αλλαγή μεγέθους σε τυποποιημένη μορφή 224x224 pixel και η χρήση ανίχνευσης ακμών για την ανάδειξη των κινήσεων γραφής υτων υπογραφών, διασφάλισαν ότι τα μοντέλα βαθιάς μάθησης έλαβαν υψηλής ποιότητας, ομοιόμορφη είσοδο. Αυτό το στάδιο προεπεξεργασίας, το οποίο χρησιμοποιεί το OpenCV, είναι κρίσιμο για να διασφαλιστεί ότι οι εικόνες υπογραφών βρίσκονται σε μορφή που μπορεί να υποστεί αποτελεσματική επεξερ-

γασία από τα επόμενα μοντέλα βαθιάς μάθησης.
Μόλις οι εικόνες υπογραφών υποβληθούν σε προεπεξεργασία, το σύστημα χρησιμοποιεί προεκπαιδευμένα μοντέλα βαθιάς μάθησης για την εξαγωγή χαρακτηριστικών. Αυτά τα μοντέλα, συμπεριλαμβανομένων των VGG16, DenseNet121, MobileNetV2 και EfficientNetV2S, εξάγουν αναπαραστάσεις χαρακτηριστικών υψηλού επιπέδου από τις εικόνες υπογραφής. Αυτά τα χαρακτηριστικά αποτυπώνουν τα μοναδικά μοτίβα κάθε υπογραφής, όπως οι παραλλαγές των γραμμών, οι υφές και η συνολική δομή, τα οποία είναι ζωτικής σημασίας για τη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών. Τα μοντέλα βαθιάς μάθησης λειτουργούν ως εκχυλιστές χαρακτηριστικών, μειώνοντας τη διαστατικότητα των δεδομένων και συμπυκνώνοντας τις πολύπλοκες πληροφορίες από τις εικόνες σε διανύσματα χαρακτηριστικών με νόημα.
Αυτά τα διανύσματα χαρακτηριστικών περνούν στη συνέχεια σε παραδοσιακούς ταξινομητές μηχανικής μάθησης, οι οποίοι εκτελούν την τελική εργασία ταξινόμησης. Οι ταξινομητές - όπως οι μηχανές διανυσμάτων υποστήριξης (SVM), τα τυχαία δάση, οι K-κοντινότεροι γείτονες (KNN) και η λογιστική παλινδρόμηση- έχουν εκπαιδευτεί στα εξαγόμενα χαρακτηριστικά για να διακρίνουν μεταξύ γνήσιων και πλαστών υπογραφών με βάση τα πρότυπα που μαθαίνονται κατά την εκπαίδευση. Αυτή η υβριδική προσέγγιση διασφαλίζει ότι το σύστημα επωφελείται από την ισχύ της βαθιάς μάθησης στην εξαγωγή χαρακτηριστικών, διατηρώντας παράλληλα την αποτελεσματικότητα και την ερμηνευσιμότητα των παραδοσιακών αλγορίθμων μηχανικής μάθησης για ταξινόμηση.
Για να διευκολυνθεί η ανάπτυξη, τα εκπαιδευμένα μοντέλα σειριοποιήθηκαν χρησιμοποιώντας τη βιβλιοθήκη Pickle της Python. Αυτό επιτρέπει την αποθήκευση των μοντέλων μετά την εκπαίδευση, διασφαλίζοντας ότι μπορούν εύκολα να επαναφορτωθούν και να χρησιμοποιηθούν για εργασίες επαλήθευσης υπογραφών σε πραγματικό χρόνο χωρίς να απαιτείται επανεκπαίδευση. Η σειριοποίηση διατηρεί την κατάσταση των εκπαιδευμένων μοντέλων, συμπεριλαμβανομένων των μαθημένων βαρών και παραμέτρων τους, επιτρέποντας στο σύστημα να αναπτυχθεί σε διάφορα περιβάλλοντα χωρίς απώλεια ακρίβειας ή επιδόσεων.

```python
import pickle
# Save the trained SVM classifier
with open('svm_classifier.pkl', 'wb') as model_file:
    pickle.dump(svm_classifier, model_file)

# Load the trained SVM classifier for future use
with open('svm_classifier.pkl', 'rb') as model_file:
    loaded_model = pickle.load(model_file)

# Use the loaded model to make predictions on new data
loaded_model.predict(new_signature_features)
```

Listing 5.10: Preprocessing Python Code

Το τελικό σύστημα ενσωματώθηκε σε μια εφαρμογή Python, η οποία σχεδιάστηκε για να εν-

σωματωθεί σε μεγαλύτερα συστήματα ασφαλείας ή βιομετρικής επαλήθευσης. Η εφαρμογή αυτή αυτοματοποιεί ολόκληρο το σύστημα, από τη φόρτωση της εικόνας της υπογραφής έως την απόφαση ταξινόμησης (γνήσια ή πλαστή). Παρέχει επίσης ανατροφοδότηση σε πραγματικό χρόνο, καθιστώντας την κατάλληλη για περιβάλλοντα με υψηλά διακυβεύματα, όπως οι τράπεζες, όπου οι γρήγορες και ακριβείς αποφάσεις είναι κρίσιμες.
Ο αρθρωτός σχεδιασμός του συστήματος καθιστά εύκολη την ενημέρωση ή την επέκτασή του. Για παράδειγμα, νέα μοντέλα βαθιάς μάθησης μπορούν να προστεθούν στο στάδιο εξαγωγής χαρακτηριστικών χωρίς να τροποποιηθεί η υπόλοιπη αγωγός. Ομοίως, εάν ένας νέος ταξινομητής μηχανικής μάθησης αποδειχθεί πιο αποτελεσματικός στο χειρισμό των εξαχθέντων χαρακτηριστικών, μπορεί να ενσωματωθεί στο στάδιο της ταξινόμησης με ελάχιστες αλλαγές στη συνολική αρχιτεκτονική. Αυτή η ευελιξία διασφαλίζει ότι το σύστημα παραμένει προσαρμόσιμο στις εξελίξεις των τεχνολογιών μηχανικής μάθησης και βαθιάς μάθησης.
Εκτός από προσαρμοστικό, το σύστημα είναι επεκτάσιμο. Μπορεί να διαχειριστεί μεγαλύτερα σύνολα δεδομένων ή πρόσθετες κατηγορίες υπογραφών με ελάχιστες τροποποιήσεις. Αυτή η επεκτασιμότητα είναι απαραίτητη για εφαρμογές στον πραγματικό κόσμο, όπου το σύστημα μπορεί να χρειαστεί να επεξεργαστεί μεγάλο όγκο υπογραφών ή να προσαρμοστεί σε νέες απαιτήσεις καθώς εξελίσσεται το τοπίο των απειλών (π.χ. εμφάνιση πιο εξελιγμένων τεχνικών παραποίησης).
Συμπερασματικά, το τελικό σύστημα ανίχνευσης πλαστογραφίας υπογραφών είναι μια ισχυρή, προσαρμόσιμη και κλιμακούμενη λύση που αξιοποιεί τα πλεονεκτήματα τόσο της βαθιάς μάθησης όσο και της παραδοσιακής μηχανικής μάθησης. Η σπονδυλωτή αρχιτεκτονική του διευκολύνει την εύκολη ανάπτυξη και ενσωμάτωση σε υπάρχουσες υποδομές, ενώ ο σχεδιασμός του εξασφαλίζει ότι μπορεί να εξελίσσεται με την πρόοδο της τεχνολογίας. Συνδυάζοντας την εξελιγμένη εξαγωγή χαρακτηριστικών με την αποτελεσματική ταξινόμηση, το σύστημα παρέχει ένα ισχυρό εργαλείο για την ανίχνευση πλαστών υπογραφών σε ένα ευρύ φάσμα εφαρμογών, εξασφαλίζοντας ακρίβεια, αξιοπιστία και ασφάλεια στις διαδικασίες επαλήθευσης υπογραφών.

5.7 Προκλήσεις και λύσεις

Κατά τη διάρκεια της υλοποίησης του συστήματος ανίχνευσης πλαστογραφίας υπογραφών προέκυψαν διάφορες προκλήσεις, οι οποίες απαιτούν στοχευμένες λύσεις για να διασφαλιστεί η αποτελεσματική απόδοση και η επεκτασιμότητα.

5.7.1 Ποιότητα και μεταβλητότητα δεδομένων

Το σύνολο δεδομένων περιείχε υπογραφές διαφορετικής ποιότητας, που επηρεάζονταν από διαφορές στη σάρωση, το μελάνι και την υφή του χαρτιού. Αυτή η μεταβλητότητα εισήγαγε

θόρυβο, ο οποίος δυνητικά εμπόδιζε την ακρίβεια του μοντέλου. Για να το αντιμετωπίσουμε αυτό, εφαρμόσαμε τεχνικές προεπεξεργασίας χρησιμοποιώντας το OpenCV, όπως μετατροπή σε κλίμακα του γκρι, Gaussian blur για μείωση του θορύβου και ανίχνευση ακμών, διασφαλίζοντας ότι τα μοντέλα βαθιάς μάθησης έλαβαν καθαρή και συνεπή είσοδο.

5.7.2 Περιορισμένο μέγεθος συνόλου δεδομένων

Το σχετικά μικρό σύνολο δεδομένων εγκυμονούσε τον κίνδυνο υπερπροσαρμογής στα μοντέλα βαθιάς μάθησης. Για να το μετριάσουμε αυτό, αξιοποιήσαμε τη μάθηση μεταφοράς, χρησιμοποιώντας προ-εκπαιδευμένα μοντέλα όπως το VGG16 και το DenseNet121. Αυτά τα μοντέλα προσαρμόστηκαν στο σύνολο δεδομένων υπογραφών, επιτρέποντάς τους να προσαρμόσουν τις προ-εκπαιδευμένες γνώσεις τους στην εργασία ανίχνευσης πλαστογραφίας υπογραφών με ελάχιστα δεδομένα εκπαίδευσης.

5.7.3 Διαχείριση μνήμης

Η εκπαίδευση μοντέλων βαθιάς μάθησης σε μεγάλα σύνολα δεδομένων εισήγαγε ζητήματα διαχείρισης μνήμης. Για να αντιμετωπιστεί αυτό, χρησιμοποιήθηκε η μονάδα συλλογής σκουπιδιών της Python (gc) για την απελευθέρωση μνήμης κατά τη διάρκεια της εκπαίδευσης και της αξιολόγησης, διασφαλίζοντας ότι το σύστημα μπορούσε να χειριστεί το σύνολο δεδομένων χωρίς να υπερβεί τα όρια μνήμης.

```
import gc
gc.collect()
```

Listing 5.11: Preprocessing Python Code

5.7.4 Ρύθμιση υπερπαραμέτρων

Η βελτιστοποίηση των ταξινομητών μηχανικής μάθησης, όπως οι SVM και τα τυχαία δάση, απαιτούσε συντονισμό υπερπαραμέτρων. Χρησιμοποιήσαμε αναζήτηση πλέγματος και διασταυρούμενη επικύρωση για να προσδιορίσουμε τις βέλτιστες διαμορφώσεις για κάθε ταξινομητή, βελτιώνοντας την απόδοση του μοντέλου και ελαχιστοποιώντας παράλληλα την υπερπροσαρμογή.

Με την αντιμετώπιση αυτών των προκλήσεων μέσω στοχευμένης προεπεξεργασίας, μάθησης μεταφοράς, αποδοτικής διαχείρισης μνήμης και βελτιστοποίησης υπερπαραμέτρων, το σύστημα ανίχνευσης πλαστών υπογραφών κατάφερε να επιτύχει υψηλή ακρίβεια και επεκτασιμότητα, εξασφαλίζοντας την καταλληλότητά του για πραγματικές εφαρμογές.

Κεφάλαιο 6

Πειραματική μελέτη

Η πειραματική μελέτη του συστήματος ανίχνευσης πλαστογραφίας υπογραφών διεξήχθη για την αξιολόγηση της αποτελεσματικότητας, της ακρίβειας και της ευρωστίας του στη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών. Στο παρόν κεφάλαιο περιγράφεται το σύνολο δεδομένων που χρησιμοποιήθηκε για την εκπαίδευση και τη δοκιμή των μοντέλων, παρουσιάζονται οι πειραματικές μετρήσεις και συζητούνται τα αποτελέσματα των πειραμάτων.

6.1 Σύνολο δεδομένων

Το σύνολο δεδομένων που χρησιμοποιήθηκε για το σύστημα ανίχνευσης πλαστογραφίας υπογραφών ήταν ζωτικής σημασίας για την εκπαίδευση και τη δοκιμή των μοντέλων. Αποτελούνταν από γνήσιες και πλαστές υπογραφές που προέρχονταν από καθιερωμένα, δημόσια διαθέσιμα σύνολα δεδομένων υπογραφών που χρησιμοποιούνται συνήθως στην έρευνα για την επαλήθευση υπογραφών. Αυτά τα σύνολα δεδομένων παρείχαν μια ισορροπημένη αναπαράσταση και των δύο κατηγοριών - γνήσιες υπογραφές και τις αντίστοιχες πλαστές - επιτρέποντας την αποτελεσματική μάθηση με επίβλεψη.
Οι εικόνες υπογραφών διέφεραν ως προς το στυλ, τη γραφή, το πλάτος και τη συνολική εμφάνιση, αντιπροσωπεύοντας τα χαρακτηριστικά γραφής διαφορετικών ατόμων. Αυτή η ποικιλομορφία ήταν απαραίτητη για την εκπαίδευση των μοντέλων ώστε να μπορούν να γενικεύονται καλά σε διάφορα στυλ γραφής και να ανιχνεύουν πλαστογραφίες σε ένα ευρύ φάσμα πλαισίων. Το σύνολο δεδομένων σχεδιάστηκε για να προκαλέσει το σύστημα, περιλαμβάνοντας πλαστογραφίες που μιμούνταν στενά τις γνήσιες υπογραφές, καθιστώντας το έργο ανίχνευσης πιο ρεαλιστικό και περίπλοκο.
Κάθε υπογραφή χαρακτηριζόταν χειροκίνητα ως γνήσια ή πλαστή, επιτρέποντας τη χρήση τεχνικών μάθησης με επίβλεψη. Το σύνολο δεδομένων περιλάμβανε σκαναρισμένες εικόνες υψηλής ανάλυσης, διασφαλίζοντας ότι τα μοντέλα βαθιάς μάθησης μπορούσαν να συλλάβουν τις λεπτές λεπτομέρειες κάθε υπογραφής. Ωστόσο, οι ακατέργαστες εικόνες συχνά διέφεραν

ως προς την ποιότητα, την ανάλυση και τη συνοχή λόγω των διαφορών στις τεχνικές σάρωσης και το χειρισμό των εγγράφων, γεγονός που παρουσίασε προκλήσεις κατά την εκπαίδευση των μοντέλων.

Για την αντιμετώπιση αυτών των προκλήσεων και την τυποποίηση του συνόλου δεδομένων, εφαρμόστηκε εκτεταμένη προεπεξεργασία με τη χρήση του OpenCV. Ο αγωγός προεπεξεργασίας περιελάμβανε τη μετατροπή των εικόνων σε κλίμακα του γκρι για την αφαίρεση των άσχετων χρωματικών πληροφοριών, την εφαρμογή Gaussian blur για τη μείωση του θορύβου, την αλλαγή μεγέθους των εικόνων σε ομοιόμορφο μέγεθος 224x224 pixels για να ταιριάξουν στις απαιτήσεις εισόδου των μοντέλων βαθιάς μάθησης και τη χρήση ανίχνευσης ακμών για την ανάδειξη των δομικών χαρακτηριστικών των υπογραφών, όπως τα μοτίβα των γραφών και οι καμπύλες. Αυτά τα βήματα διασφάλισαν ότι τα δεδομένα που τροφοδοτήθηκαν στα μοντέλα ήταν καθαρά, συνεπή και υψηλής ποιότητας.

Μετά την προεπεξεργασία, το σύνολο δεδομένων χωρίστηκε σε σύνολα εκπαίδευσης, επικύρωσης και δοκιμής, ώστε να διασφαλιστεί ότι τα μοντέλα εκπαιδεύτηκαν σε ένα τμήμα των δεδομένων και δοκιμάστηκαν σε εντελώς ξεχωριστά δεδομένα. Χρησιμοποιήσαμε έναν διαχωρισμό 80/20, όπου το 80/100 των δεδομένων διατέθηκε για εκπαίδευση και επικύρωση και το υπόλοιπο 20/100 προοριζόταν για δοκιμή. Αυτός ο διαχωρισμός εξασφάλισε ότι τα μοντέλα μπορούσαν να μάθουν από ένα ποικίλο σύνολο υπογραφών, διατηρώντας παράλληλα την ικανότητα να γενικεύουν καλά σε νέα, αθέατα παραδείγματα.

Για να βελτιστοποιηθεί η διαδικασία εκπαίδευσης, το σύνολο εκπαίδευσης χωρίστηκε περαιτέρω σε υποσύνολα εκπαίδευσης και επικύρωσης, συνήθως με κατανομή 75/25. Το υποσύνολο εκπαίδευσης χρησιμοποιήθηκε για την εκπαίδευση των μοντέλων, ενώ το υποσύνολο επικύρωσης επέτρεπε τη ρύθμιση των υπερπαραμέτρων και την παρακολούθηση της απόδοσης των μοντέλων κατά τη διάρκεια της εκπαίδευσης, αποτρέποντας την υπερπροσαρμογή.

Το προσεκτικά επιμελημένο σύνολο δεδομένων, σε συνδυασμό με τις ισχυρές τεχνικές προεπεξεργασίας, παρείχε μια σταθερή βάση για την εκπαίδευση των μοντέλων βαθιάς μάθησης και μηχανικής μάθησης. Αυτό εξασφάλισε ότι το σύστημα ανίχνευσης πλαστογραφίας υπογραφών μπορούσε να διακρίνει αποτελεσματικά μεταξύ γνήσιων και πλαστών υπογραφών σε ένα ευρύ φάσμα στυλ και συνθηκών, καθιστώντας το κατάλληλο για εφαρμογές στον πραγματικό κόσμο όπου η ακριβής επαλήθευση είναι απαραίτητη[31].

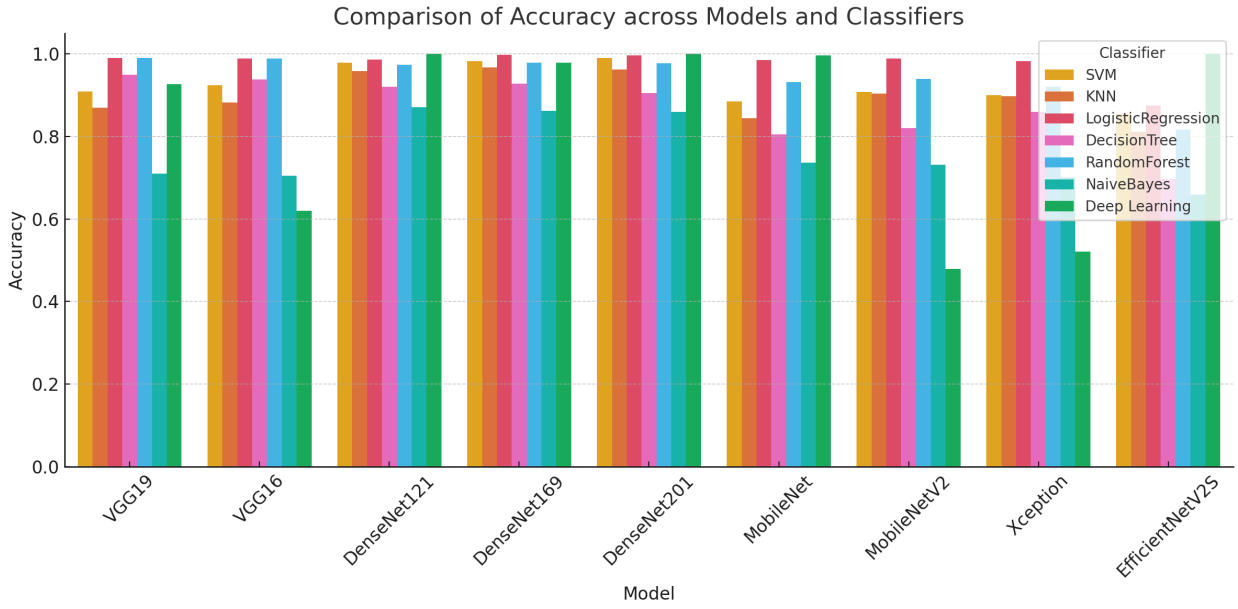
6.2 Πειραματικές μετρήσεις

Η απόδοση του συστήματος ανίχνευσης πλαστογραφίας υπογραφών αξιολογήθηκε με τη χρήση μιας σειράς βασικών πειραματικών μετρήσεων που παρείχαν πληροφορίες σχετικά με την αποτελεσματικότητα του συστήματος στη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών. Αυτές οι μετρήσεις, οι οποίες περιλάμβαναν την ακρίβεια, την ευστοχία, την ανάκληση, το F1-score και την περιοχή κάτω από την καμπύλη ROC (AUC), επιλέχθηκαν για την ολοκληρωμένη

αξιολόγηση των δυνατοτήτων ταξινόμησης του συστήματος.

6.2.1 Ακρίβεια

Η ακρίβεια χρησιμεύει ως θεμελιώδης μετρική για την αξιολόγηση της συνολικής απόδοσης του συστήματος στην ταξινόμηση υπογραφών ως γνήσιες ή πλαστές. Υπολογίζεται ως ο λόγος των σωστά ταξινομημένων υπογραφών (γνήσιων και πλαστών) προς το συνολικό αριθμό υπογραφών στο σύνολο δοκιμών. Ουσιαστικά, η ακρίβεια παρέχει μια επισκόπηση του πόσο καλά απέδωσε το μοντέλο στη διάκριση μεταξύ των δύο κατηγοριών, προσφέροντας έναν απλό αλλά αποτελεσματικό τρόπο μέτρησης της συνολικής αποτελεσματικότητας του συστήματος.



Σχήμα 6.1: Accuracy based comparison plot.

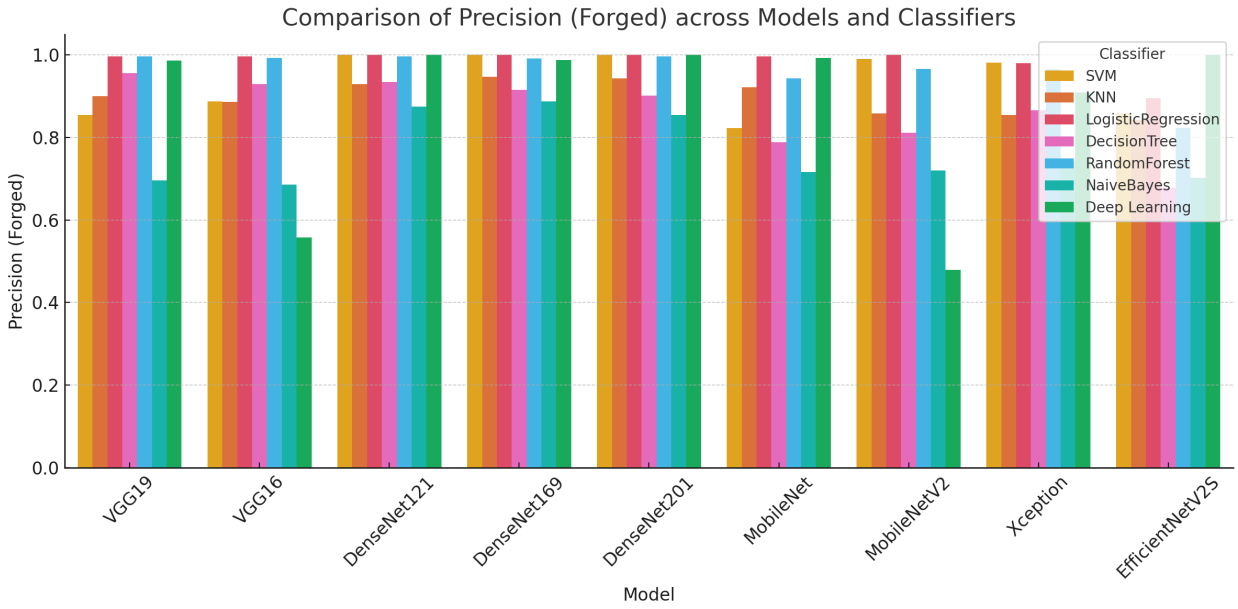
Ωστόσο, ενώ η ακρίβεια είναι μια χρήσιμη μετρική, θα πρέπει να ερμηνεύεται με προσοχή σε μη ισορροπημένα σύνολα δεδομένων. Εάν το σύνολο δεδομένων περιέχει σημαντικά μεγαλύτερο αριθμό γνήσιων υπογραφών από ό,τι πλαστών, το μοντέλο μπορεί να επιτύχει υψηλή ακρίβεια προβλέποντας κατά κύριο λόγο την πλειοψηφούσα κλάση. Παρόλα αυτά, στο πλαίσιο της παρούσας πτυχιακής εργασίας, το σύνολο δεδομένων εξισορροπήθηκε ώστε να διασφαλιστεί ότι η ακρίβεια παραμένει ένας ουσιαστικός δείκτης απόδοσης[33][34].

```
accuracy = accuracy_score(y_test, y_pred)
print(f"Accuracy: {accuracy}
```

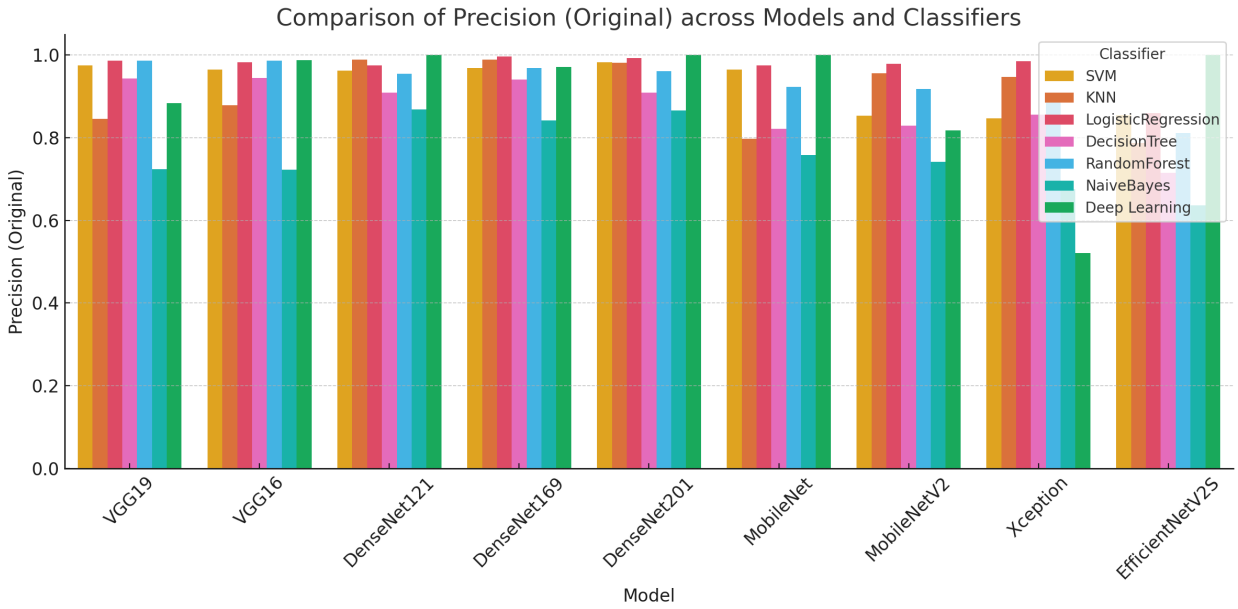
Listing 6.1: Accuracy pyhton code

6.2.2 Ευστοχία

Η ευστοχία είναι μια κρίσιμη μετρική στο πλαίσιο της ανίχνευσης πλαστογραφίας υπογραφών, ιδίως όταν ο στόχος είναι να ελαχιστοποιηθούν τα ψευδώς θετικά αποτελέσματα - περιπτώσεις όπου μια γνήσια υπογραφή ταξινομείται λανθασμένα ως πλαστή. Η ευστοχία ορίζεται ως το ποσοστό των αληθώς θετικών προβλέψεων (σωστά αναγνωρισμένες πλαστές υπογραφές) σε σχέση με όλες τις θετικές προβλέψεις που έκανε το μοντέλο (τόσο τις σωστά όσο και τις λανθασμένα αναγνωρισμένες πλαστές υπογραφές). Μια υψηλή βαθμολογία ευστοχίας υποδηλώνει ότι το μοντέλο είναι αποτελεσματικό στον περιορισμό του αριθμού των ψευδώς θετικών προβλέψεων, διασφαλίζοντας ότι οι γνήσιες υπογραφές είναι λιγότερο πιθανό να ταξινομηθούν εσφαλμένα ως πλαστές.



Σχήμα 6.2: Precision based comparison plot (Forged).



Σχήμα 6.3: Precision based comparison plot (Original).

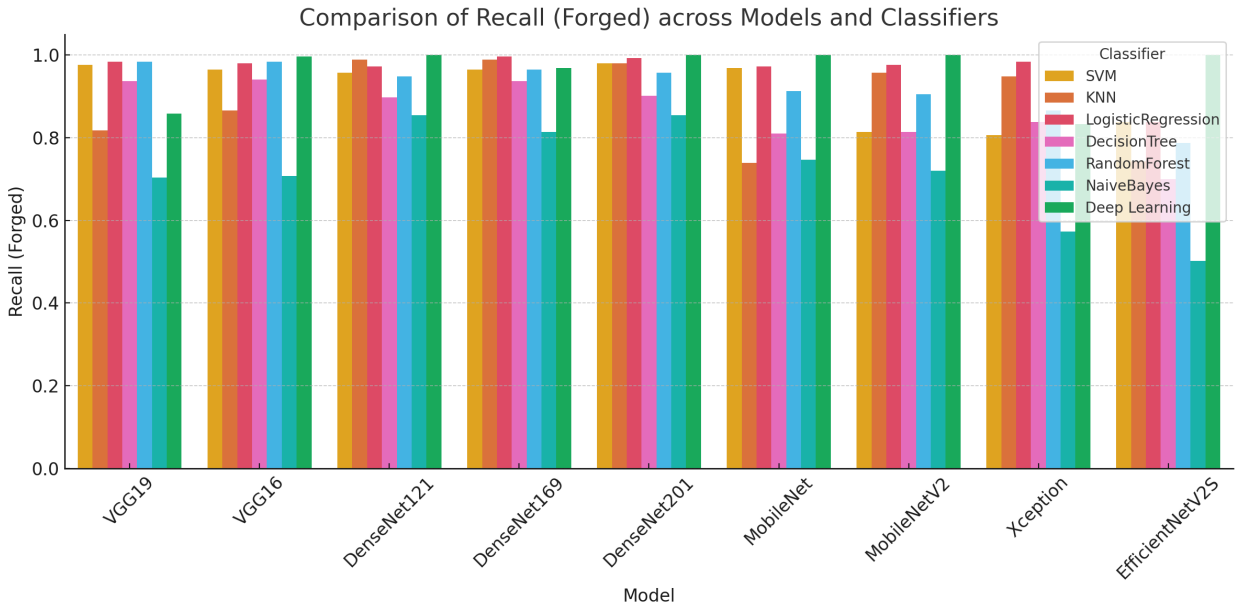
Στην ανίχνευση πλαστογραφίας υπογραφών, η ευστοχία είναι ιδιαίτερα σημαντική όταν το κόστος του λανθασμένου χαρακτηρισμού μιας γνήσιας υπογραφής ως πλαστογραφημένης είναι υψηλό, όπως σε οικονομικές ή νομικές εφαρμογές. Οι λανθασμένοι χαρακτηρισμοί σε αυτούς τους τομείς θα μπορούσαν να οδηγήσουν σε σημαντικές αρνητικές συνέπειες για άτομα ή ιδρύματα, καθιστώντας την ευστοχία βασικό δείκτη απόδοσης[33][34].

```
precision = precision_score(y_test, y_pred, average='weighted')
print(f"Precision: {precision}")
```

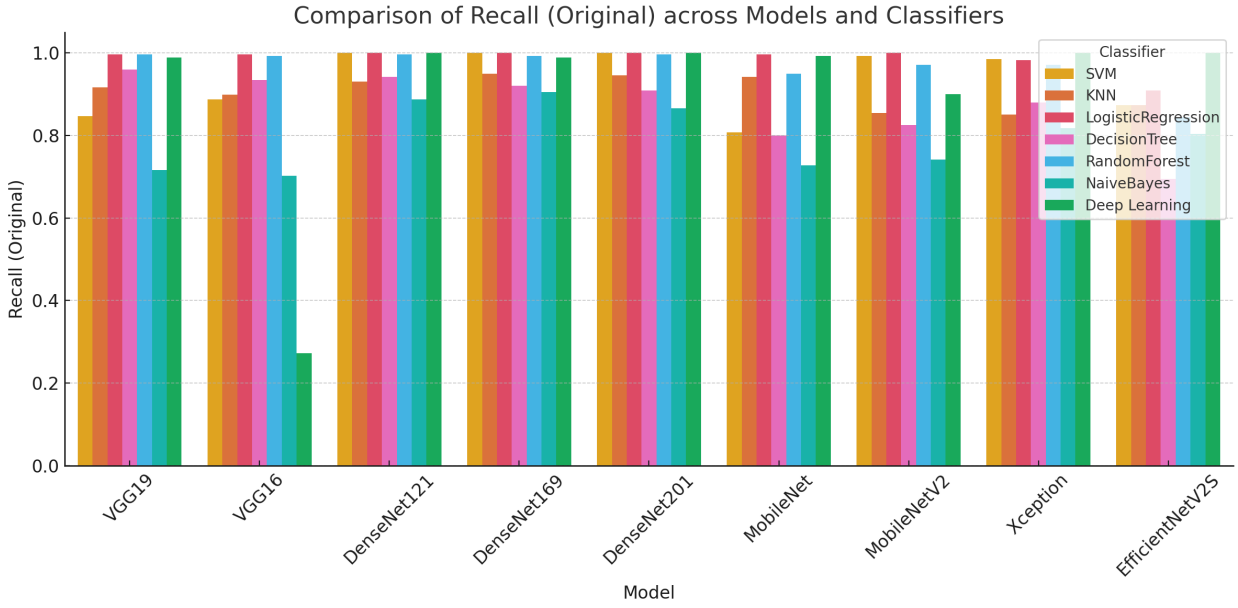
Listing 6.2: Precision python code

6.2.3 Ανάκληση

Η ανάκληση, επίσης γνωστή ως ευαισθησία ή ποσοστό αληθώς θετικών υπογραφών, είναι μια κρίσιμη μετρική για την αξιολόγηση του συστήματος ανίχνευσης πλαστογράφησης υπογραφών, ιδίως σε σενάρια όπου η ανίχνευση πλαστογραφημένων υπογραφών είναι υψίστης σημασίας. Η ανάκληση ορίζεται ως το ποσοστό των πραγματικών πλαστών υπογραφών (αληθώς θετικών) που αναγνωρίστηκαν σωστά από το μοντέλο, σε σχέση με τον συνολικό αριθμό των πλαστών υπογραφών που υπάρχουν στο σύνολο δοκιμών. Μια υψηλή βαθμολογία ανάκλησης υποδηλώνει ότι το μοντέλο είναι αποτελεσματικό στον εντοπισμό της πλειονότητας των πλαστών υπογραφών, διασφαλίζοντας ότι πολύ λίγες πλαστές υπογραφές θα ταξινομηθούν εσφαλμένα ως γνήσιες.



Σχήμα 6.4: Recall based comparison plot (Forged).



Σχήμα 6.5: Recall based comparison plot (Original).

Στο πλαίσιο της ανίχνευσης πλαστογραφίας υπογραφών, η ανάκληση είναι ιδιαίτερα σημαντική όταν το κόστος της εξαφάνισης μιας πλαστογραφίας είναι υψηλό. Για παράδειγμα, στα νομικά και χρηματοπιστωτικά συστήματα, η μη ανίχνευση μιας πλαστής υπογραφής μπορεί να οδηγήσει σε σημαντικές παραβιάσεις της ασφάλειας ή σε απάτη. Ως εκ τούτου, η ανάκληση παρέχει πληροφορίες σχετικά με την ικανότητα του μοντέλου να εντοπίζει πλαστογραφίες χωρίς να παραβλέπει καμία, καθιστώντας το ζωτικής σημασίας μέτρο για την αξιολόγηση της

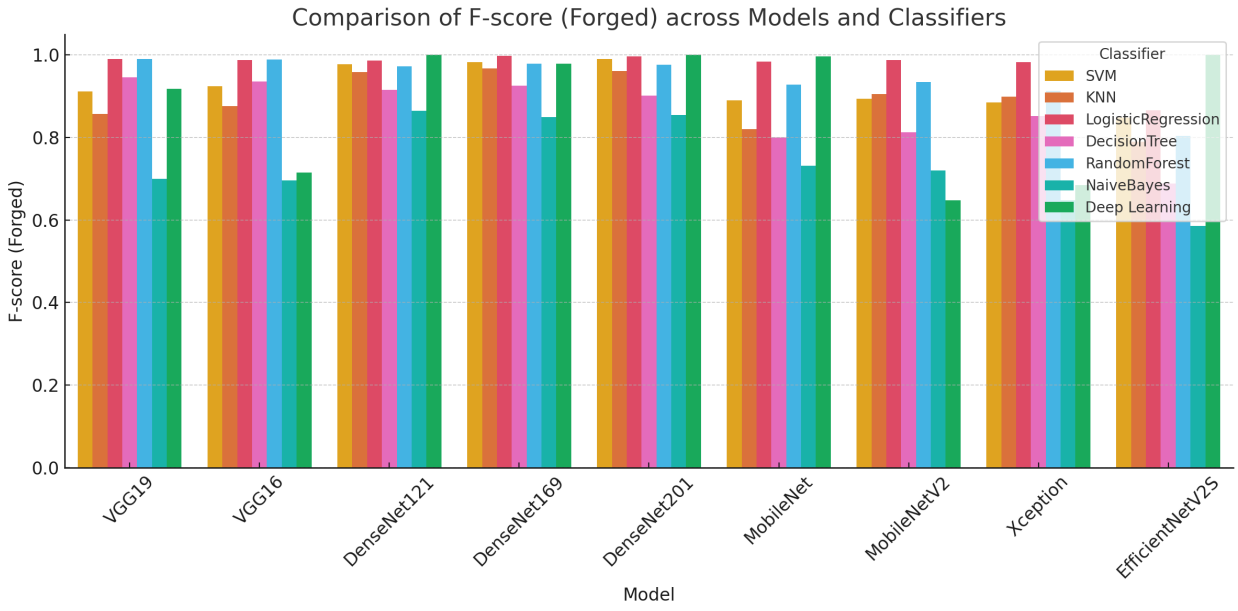
ευρωστίας του συστήματος στον εντοπισμό δόλιων δραστηριοτήτων[33][34].

```
recall = recall_score(y_test, y_pred, average='weighted')
print(f"Recall: {recall}")
```

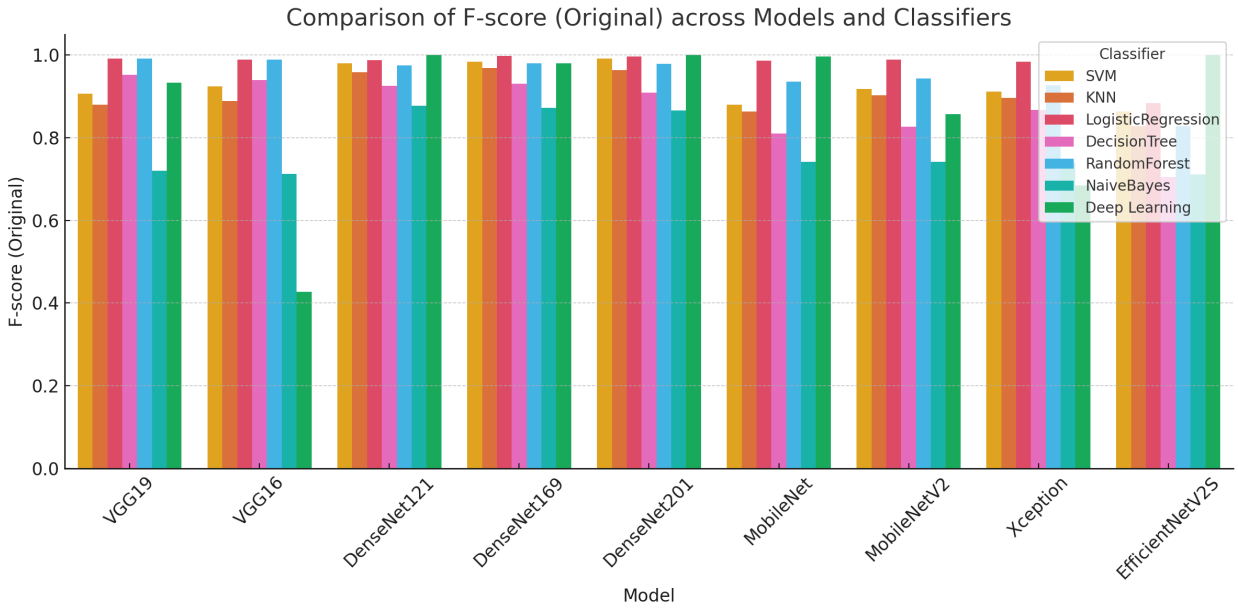
Listing 6.3: Recall python code

6.2.4 F1-Score

Το F1-Score είναι μια ισορροπημένη μετρική που συνδυάζει την ακρίβεια και την ανάκληση, παρέχοντας ένα ενιαίο μέτρο που λαμβάνει υπόψη τόσο τα ψευδώς θετικά όσο και τα ψευδώς αρνητικά αποτελέσματα. Είναι ιδιαίτερα χρήσιμο όταν υπάρχει άνιση κατανομή μεταξύ των κλάσεων, καθώς λαμβάνει υπόψη τόσο την ακρίβεια (πόσες από τις ανιχνευθείσες πλαστογραφίες ήταν πράγματι πλαστογραφίες) όσο και την ανάκληση (πόσες από τις πραγματικές πλαστογραφίες ανιχνεύθηκαν). Το F1-Score υπολογίζεται ως ο αρμονικός μέσος όρος της ακρίβειας και της ανάκλησης, προσφέροντας μια πιο ολοκληρωμένη εικόνα της απόδοσης του μοντέλου από ό,τι οποιαδήποτε από τις δύο μετρικές από μόνη της.



Σχήμα 6.6: F-Score based comparison plot (Forged).



Σχήμα 6.7: F-Score based comparison plot (Original).

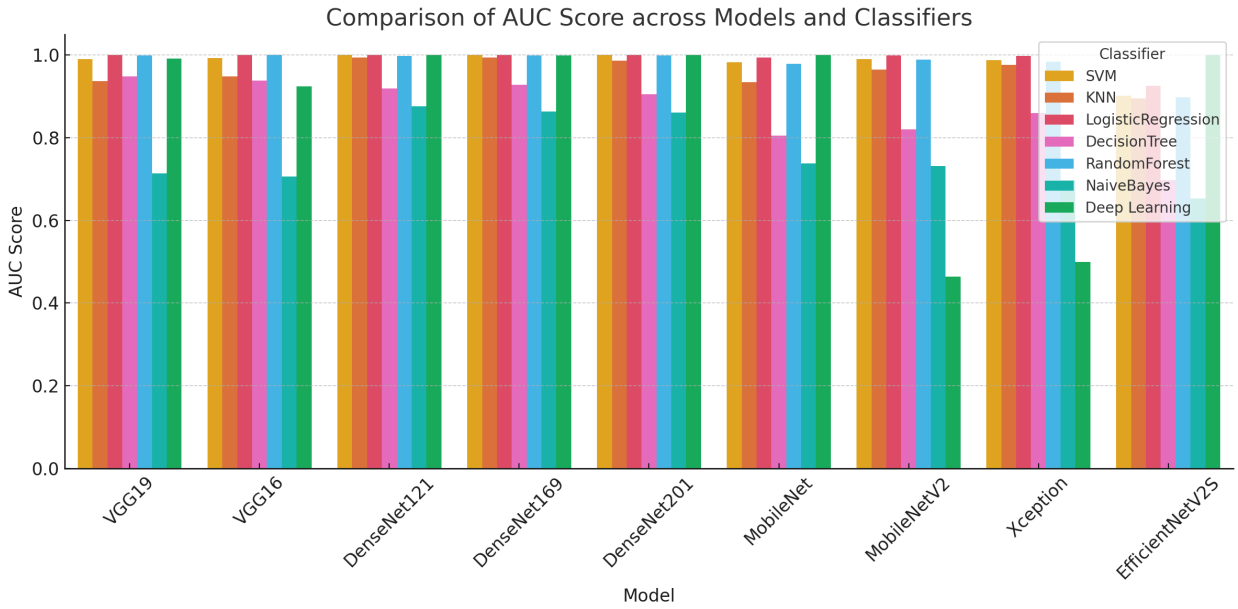
Στο πλαίσιο της ανίχνευσης πλαστογραφίας υπογραφών, το F1-Score είναι ζωτικής σημασίας, διότι διασφαλίζει ότι το μοντέλο όχι μόνο αναγνωρίζει σωστά τις πλαστογραφίες αλλά και αποφεύγει να χαρακτηρίζει λανθασμένα τις γνήσιες υπογραφές ως πλαστές. Αυτή η ισορροπία είναι ζωτικής σημασίας σε περιβάλλοντα υψηλού κινδύνου, όπως ο τραπεζικός ή ο νομικός έλεγχος, όπου και οι δύο τύποι λανθασμένης ταξινόμησης (ψευδώς θετικά και ψευδώς αρνητικά) μπορεί να έχουν σημαντικές συνέπειες[33][34].

```
f1 = f1_score(y_test, y_pred, average='weighted')
print(f"F1-Score: {f1}")
```

Listing 6.4: F-Score python code

6.2.5 Περιοχή κάτω από την καμπύλη ROC (AUC)

Η περιοχή κάτω από τη χαρακτηριστική καμπύλη λειτουργίας δέκτη (AUC) είναι μια ισχυρή μετρική για την αξιολόγηση της συνολικής απόδοσης του συστήματος ανίχνευσης πλαστογραφίας υπογραφών, ιδίως όσον αφορά την ικανότητά του να διακρίνει μεταξύ γνήσιων και πλαστών υπογραφών σε διαφορετικά κατώφλια ταξινόμησης. Η καμπύλη ROC απεικονίζει το αληθώς θετικό ποσοστό (ανάκληση) έναντι του ψευδώς θετικού ποσοστού, παρέχοντας μια ολοκληρωμένη εικόνα των συμβιβασμών μεταξύ ευαισθησίας και ειδικότητας καθώς μεταβάλλεται το κατώφλι απόφασης.



Σχήμα 6.8: AUC based comparison plot.

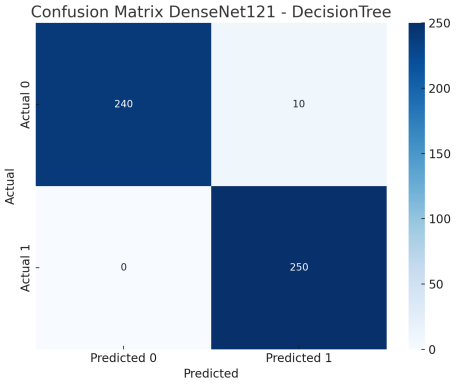
Μια υψηλότερη τιμή AUC υποδεικνύει ότι το μοντέλο έχει ισχυρή ικανότητα διάκρισης μεταξύ των δύο κατηγοριών - γνήσιες και πλαστές υπογραφές - ανεξάρτητα από το επιλεγμένο κατώφλι. Μια τιμή AUC 1,0 αντιπροσωπεύει τέλεια ταξινόμηση, ενώ μια τιμή AUC 0,5 υποδηλώνει μηδενική ικανότητα διάκρισης, που μοιάζει με τυχαία εικασία. Στο πλαίσιο της ανίχνευσης πλαστογραφημένων υπογραφών, η AUC είναι ιδιαίτερα χρήσιμη για την κατανόηση του πόσο καλά αποδίδει το μοντέλο σε διαφορετικές συνθήκες και πόσο αποτελεσματικά μπορεί να διακρίνει τις πλαστογραφημένες από τις γνήσιες υπογραφές[33][34].

```
auc = roc_auc_score(y_test, svm_classifier.predict_proba(X_test), multi_class=
    'ovo')
print(f"AUC: {auc}")
```

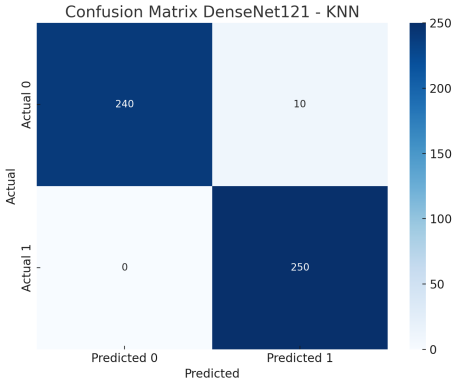
Listing 6.5: AUC python code

6.2.6 Πίνακας σύγχυσης

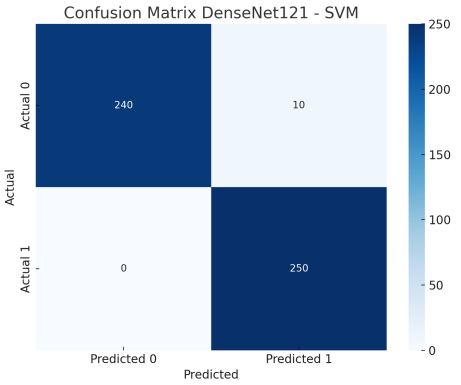
Ο πίνακας σύγχυσης αποτελεί βασικό εργαλείο για την αξιολόγηση της απόδοσης του συστήματος ανίχνευσης πλαστογραφίας υπογραφής. Παρέχει λεπτομερή ανάλυση των προβλέψεων του μοντέλου, εμφανίζοντας τον αριθμό των αληθώς θετικών (γνήσιες υπογραφές που ταξινομήθηκαν σωστά), των αληθώς αρνητικών (πλαστές υπογραφές που ταξινομήθηκαν σωστά), των ψευδώς θετικών (γνήσιες υπογραφές που ταξινομήθηκαν εσφαλμένα ως πλαστές) και των ψευδώς αρνητικών (πλαστές υπογραφές που ταξινομήθηκαν εσφαλμένα ως γνήσιες). Αυτός ο πίνακας προσφέρει εικόνα των συγκεκριμένων τύπων σφαλμάτων ταξινόμησης που κάνει το μοντέλο, επιτρέποντας τη βαθύτερη κατανόηση των δυνατών και αδύνατων σημείων του.



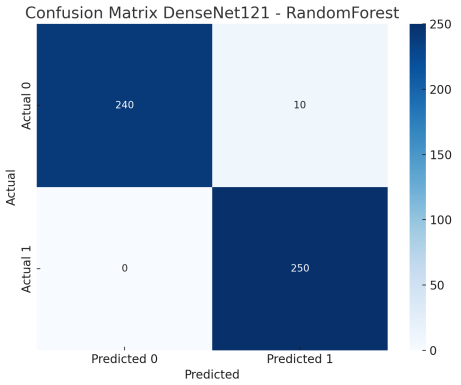
(α′) Confusion Matrix of DenseNet121 - DecisionTree.



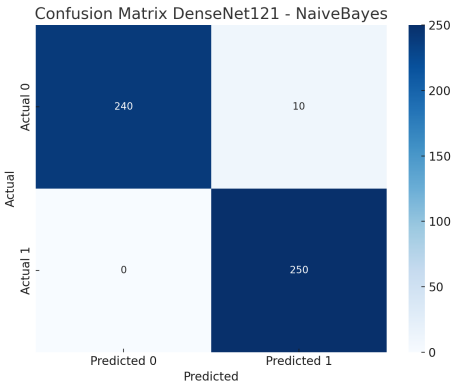
(β′) Confusion Matrix of DenseNet121 - KNN.



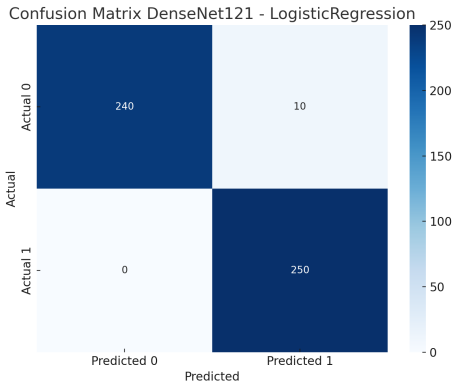
(γ′) Confusion Matrix of DenseNet121 - SVM.



(δ′) Confusion Matrix of DenseNet121 - Random Forest.

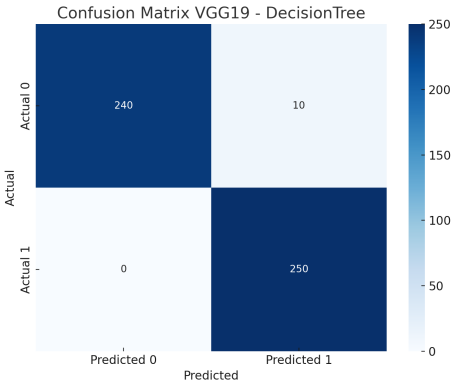


(ε′) Confusion Matrix of DenseNet121 - Naive Bayes.

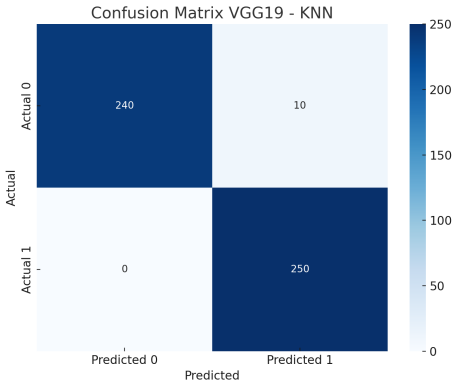


(ς′) Confusion Matrix of DenseNet121 - Logistic Regression.

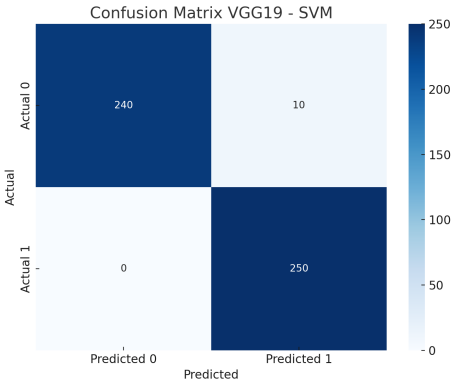
Σχήμα 6.9: Comparison of Different Confusion Matrices for DenseNet121 Model's Classifiers.



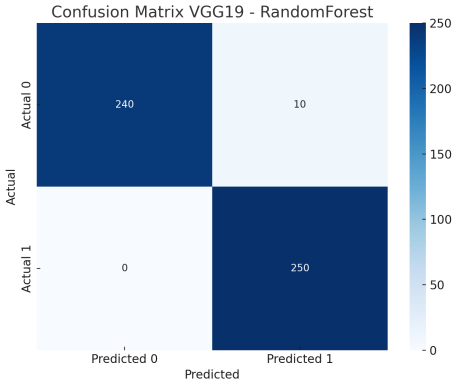
(α′) Confusion Matrix of VGG19 - DecisionTree.



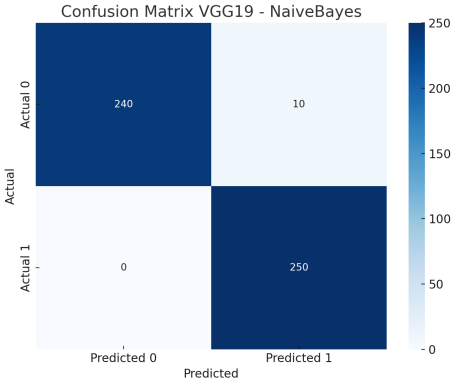
(β′) Confusion Matrix of VGG19 - KNN.



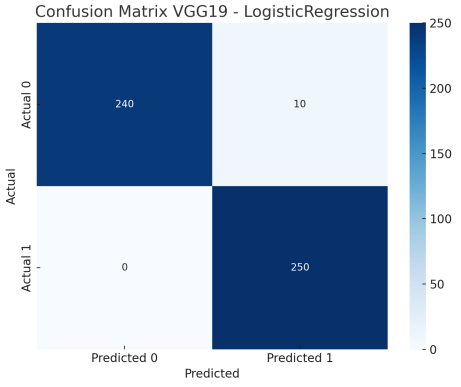
(γ′) Confusion Matrix of VGG19 - SVM.



(δ′) Confusion Matrix of VGG19 - Random Forest.



(ε′) Confusion Matrix of VGG19 - Naive Bayes.



(ϛ′) Confusion Matrix of VGG19 - Logistic Regression.

Σχήμα 6.10: Comparison of Different Confusion Matrices for VGG19 Model's Classifiers.

6.2.7 Σύνοψη των αποτελεσμάτων

Οι πειραματικές μετρήσεις αποκάλυψαν ότι η υβριδική προσέγγιση που συνδυάζει την εξαγωγή χαρακτηριστικών βαθιάς μάθησης με την παραδοσιακή ταξινόμηση με μηχανική μάθηση πέτυχε ισχυρές επιδόσεις σε όλες τις μετρήσεις. Η ακρίβεια του συστήματος ήταν σταθερά υψηλή σε πολλαπλούς ταξινομητές, με τις μηχανές διανυσμάτων υποστήριξης (SVM) και τους ταξινομητές Random Forest να επιδεικνύουν ιδιαίτερα ισχυρές επιδόσεις. Οι βαθμολογίες ακρίβειας και ανάκλησης ήταν επίσης ισορροπημένες, υποδεικνύοντας ότι το σύστημα ήταν αποτελεσματικό τόσο στον εντοπισμό πλαστών εγγράφων όσο και στην ελαχιστοποίηση των ψευδώς θετικών αποτελεσμάτων.
Οι βαθμολογίες F1 επιβεβαίωσαν την ικανότητα του συστήματος να διατηρεί μια καλή ισορροπία μεταξύ ακρίβειας και ανάκλησης, καθιστώντας το μια στιβαρή λύση για τον εντοπισμό πλαστογραφιών σε σενάρια πραγματικού κόσμου. Επιπλέον, οι βαθμολογίες AUC υπογράμμισαν τη συνολική ικανότητα του μοντέλου να διακρίνει μεταξύ γνήσιων και πλαστών υπογραφών σε διαφορετικά όρια απόφασης, υπογραμμίζοντας την ευελιξία και την αξιοπιστία του συστήματος σε διαφορετικά πλαίσια.

Model	Classifier	AUC Score	Accuracy	Precision (Original)	Precision (Forged)
VGG19	SVM	0.9893	0.9090	0.9748	0.8546
VGG19	KNN	0.9371	0.8693	0.8456	0.9
VGG19	LogisticRegression	0.9998	0.9905	0.9856	0.996
VGG19	DecisionTree	0.9483	0.9488	0.9428	0.9556
VGG19	RandomForest	0.9992	0.9905	0.9856	0.9969
VGG19	NaiveBayes	0.7130	0.7102	0.7242	0.6953
VGG19	Deep Learning	0.9913	0.9261	0.8831	0.9863
VGG16	SVM	0.9921	0.92424	0.9644	0.8872
VGG16	KNN	0.9487	0.8825	0.8790	0.8866
VGG16	LogisticRegression	0.9996	0.9886	0.9820	0.9959
VGG16	DecisionTree	0.9376	0.9375	0.9448	0.9296
VGG16	RandomForest	0.9998	0.9886	0.9855	0.9920
VGG16	NaiveBayes	0.7065	0.7045	0.7228	0.6858
VGG16	Deep Learning	0.9243	0.6193	0.9868	0.5575
DenseNet121	SVM	0.9999	0.9791	0.9615	1
DenseNet121	KNN	0.9940	0.9583	0.9884	0.9293
DenseNet121	LogisticRegression	0.9997	0.9867	0.9751	1
DenseNet121	DecisionTree	0.9195	0.9204	0.9087	0.9341
DenseNet121	RandomForest	0.9975	0.9734	0.9547	0.9958
DenseNet121	NaiveBayes	0.8761	0.8712	0.8683	0.8744
DenseNet121	Deep Learning	1	1	1	1
DenseNet169	SVM	0.9999	0.9829	0.9683	1
DenseNet169	KNN	0.9935	0.9678	0.9886	0.9469
DenseNet169	LogisticRegression	1	0.9981	0.9963	1
DenseNet169	DecisionTree	0.9283	0.9280	0.9405	0.9150
DenseNet169	RandomForest	0.9992	0.9791	0.9680	0.9918
DenseNet169	NaiveBayes	0.8633	0.8617	0.8412	0.8879
DenseNet169	Deep Learning	0.9985	0.9791	0.9714	0.9879
DenseNet201	SVM	1	0.9905	0.9821	1
DenseNet201	KNN	0.9858	0.9621	0.9811	0.9429

DenseNet201	LogisticRegression	0.9999	0.9962	0.9927	1
DenseNet201	DecisionTree	0.9051	0.9053	0.9090	0.9011
DenseNet201	RandomForest	0.9984	0.9772	0.9614	0.9958
DenseNet201	NaiveBayes	0.8605	0.8598	0.8654	0.8537
DenseNet201	Deep Learning	1	1	1	1
MobileNet	SVM	0.9821	0.8844	0.9652	0.8221
MobileNet	KNN	0.9347	0.8446	0.7969	0.9211
MobileNet	LogisticRegression	0.9942	0.9848	0.9750	0.9959
MobileNet	DecisionTree	0.8051	0.8049	0.8208	0.7884
MobileNet	RandomForest	0.9786	0.9318	0.9226	0.9428
MobileNet	NaiveBayes	0.7383	0.7367	0.7575	0.7159
MobileNet	Deep Learning	1	0.9962	1	0.9921
MobileNetV2	SVM	0.9905	0.9071	0.8531	0.9903
MobileNetV2	KNN	0.9650	0.9034	0.9552	0.8581
MobileNetV2	LogisticRegression	0.9989	0.9886	0.9786	1
MobileNetV2	DecisionTree	0.8198	0.8200	0.8284	0.8110
MobileNetV2	RandomForest	0.9891	0.9393	0.9175	0.9662
MobileNetV2	NaiveBayes	0.7312	0.7310	0.7418	0.7193
MobileNetV2	Deep Learning	0.4642	0.4791	0.8181	0.4791
Xception	SVM	0.9879	0.8996	0.8468	0.9807
Xception	KNN	0.9758	0.8977	0.9473	0.8540
Xception	LogisticRegression	0.9980	0.9829	0.9854	0.9803
Xception	DecisionTree	0.8589	0.8598	0.8551	0.8653
Xception	RandomForest	0.9834	0.9204	0.8870	0.9647
Xception	NaiveBayes	0.6966	0.7007	0.6756	0.7435
Xception	Deep Learning	0.5	0.5208	0.5208	0.9090
EfficientNetV2S	SVM	0.9018	0.8560	0.8540	0.8582
EfficientNetV2S	KNN	0.8949	0.8106	0.7868	0.8430
EfficientNetV2S	LogisticRegression	0.9249	0.875	0.8591	0.8945
EfficientNetV2S	DecisionTree	0.6970	0.6969	0.7153	0.6781
EfficientNetV2S	RandomForest	0.8973	0.8162	0.8111	0.8223
EfficientNetV2S	NaiveBayes	0.6533	0.6590	0.6368	0.7016

EfficientNetV2S	Deep Learning	1	1	1	1

Πίνακας 6.1: Metrics for each Model and their classifiers

Model	Classifier	Recall (Original)	Recall (Forged)	F-score (Original)	F-score (Forged)
VGG19	SVM	0.8472	0.9762	0.9066	0.9114
VGG19	KNN	0.9169	0.8181	0.8795	0.8571
VGG19	LogisticRegression	0.9963	0.9841	0.9909	0.9900
VGG19	DecisionTree	0.96	0.9367	0.9513	0.9461
VGG19	RandomForest	0.9963	0.9841	0.9909	0.9900
VGG19	NaiveBayes	0.7163	0.7035	0.7202	0.6994
VGG19	Deep Learning	0.9890	0.8577	0.9331	0.9175
VGG16	SVM	0.8872	0.9644	0.9242	0.9242
VGG16	KNN	0.8981	0.8656	0.8884	0.876
VGG16	LogisticRegression	0.9963	0.9802	0.9891	0.9880
VGG16	DecisionTree	0.9345	0.9407	0.9396	0.9351
VGG16	RandomForest	0.9927	0.9841	0.9891	0.9880
VGG16	NaiveBayes	0.7018	0.7075	0.7121	0.6964
VGG16	Deep Learning	0.2727	0.9960	0.4273	0.7148
DenseNet121	SVM	1	0.9565	0.9803	0.9777
DenseNet121	KNN	0.9309	0.9881	0.9588	0.9578
DenseNet121	LogisticRegression	1	0.9723	0.9874	0.9859
DenseNet121	DecisionTree	0.9418	0.8972	0.925	0.9153
DenseNet121	RandomForest	0.9963	0.9486	0.9750	0.9716
DenseNet121	NaiveBayes	0.8872	0.8537	0.8776	0.864
DenseNet121	Deep Learning	1	1	1	1
DenseNet169	SVM	1	0.9644	0.9838	0.9818
DenseNet169	KNN	0.9490	0.9881	0.9684	0.9671
DenseNet169	LogisticRegression	1	0.9960	0.9981	0.9980
DenseNet169	DecisionTree	0.92	0.9367	0.9301	0.9257
DenseNet169	RandomForest	0.9927	0.9644	0.9802	0.9779
DenseNet169	NaiveBayes	0.9054	0.8142	0.8721	0.8494
DenseNet169	Deep Learning	0.9890	0.9683	0.9801	0.9780
DenseNet201	SVM	1	0.9802	0.9909	0.9900
DenseNet201	KNN	0.9454	0.9802	0.9629	0.9612

DenseNet201	LogisticRegression	1	0.9920	0.9963	0.9960
DenseNet201	DecisionTree	0.9090	0.9011	0.9090	0.9011
DenseNet201	RandomForest	0.9963	0.9565	0.9785	0.9758
DenseNet201	NaiveBayes	0.8654	0.8537	0.8654	0.8537
DenseNet201	Deep Learning	1	1	1	1
MobileNet	SVM	0.8072	0.9683	0.8792	0.8892
MobileNet	KNN	0.9418	0.7391	0.8633	0.8201
MobileNet	LogisticRegression	0.9963	0.9723	0.9856	0.984
MobileNet	DecisionTree	0.8	0.8102	0.8103	0.7992
MobileNet	RandomForest	0.9490	0.9130	0.9354	0.9277
MobileNet	NaiveBayes	0.7272	0.7470	0.7421	0.7311
MobileNet	Deep Learning	0.9927	1	0.9963	0.9960
MobileNetV2	SVM	0.9927	0.8142	0.9176	0.8937
MobileNetV2	KNN	0.8545	0.9565	0.9021	0.9046
MobileNetV2	LogisticRegression	1	0.9762	0.9892	0.988
MobileNetV2	DecisionTree	0.8254	0.8142	0.8269	0.8126
MobileNetV2	RandomForest	0.9709	0.9051	0.9434	0.9346
MobileNetV2	NaiveBayes	0.7418	0.7193	0.7418	0.7193
MobileNetV2	Deep Learning	0.9	1	0.8571	0.6478
Xception	SVM	0.9854	0.8063	0.9109	0.8850
Xception	KNN	0.8509	0.9486	0.8965	0.8988
Xception	LogisticRegression	0.9818	0.9841	0.9836	0.9822
Xception	DecisionTree	0.88	0.8379	0.8673	0.8514
Xception	RandomForest	0.9709	0.8656	0.9270	0.9125
Xception	NaiveBayes	0.8181	0.5731	0.7401	0.6473
Xception	Deep Learning	1	0.8333	0.6849	0.6849
EfficientNetV2S	SVM	0.8727	0.8379	0.8633	0.848
EfficientNetV2S	KNN	0.8727	0.7430	0.8275	0.7899
EfficientNetV2S	LogisticRegression	0.9090	0.8379	0.8833	0.8653
EfficientNetV2S	DecisionTree	0.6945	0.6996	0.7047	0.6887
EfficientNetV2S	RandomForest	0.8436	0.7865	0.8270	0.8040
EfficientNetV2S	NaiveBayes	0.8036	0.5019	0.7106	0.5852

EfficientNetV2S	Deep Learning	1	1	1	1

Πίνακας 6.2: Metrics for each Model and their classifiers

Συνολικά, οι μετρικές επιδόσεων του συστήματος επιβεβαίωσαν την ικανότητά του να ανιχνεύει με ακρίβεια και αποτελεσματικότητα πλαστές υπογραφές, καθιστώντας το πολύτιμο εργαλείο για εφαρμογές που απαιτούν υψηλή ακρίβεια στην επαλήθευση της γνησιότητας των υπογραφών.

6.3 Συζήτηση

Τα πειραματικά αποτελέσματα αναδεικνύουν τα δυνατά σημεία και τους περιορισμούς του συστήματος ανίχνευσης πλαστογραφίας υπογραφών, παρέχοντας πληροφορίες σχετικά με την απόδοσή του σε διάφορες μετρήσεις και ρίχνοντας φως σε πιθανές βελτιώσεις. Το σύστημα, το οποίο ενσωματώνει τη βαθιά μάθηση για την εξαγωγή χαρακτηριστικών και την παραδοσιακή μηχανική μάθηση για την ταξινόμηση, επέδειξε ισχυρές επιδόσεις στη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών.
Ένα από τα κύρια πλεονεκτήματα του συστήματος ήταν η ικανότητά του να αξιοποιεί τα εκπαιδευμένα νευρωνικά δίκτυα συνελίξεων (CNN) για την αυτόματη εξαγωγή σύνθετων χαρακτηριστικών από εικόνες υπογραφών.Μοντέλα όπως το VGG16, το DenseNet121 και το MobileNetV2 ήταν αποτελεσματικά στον εντοπισμό λεπτών λεπτομερειών, όπως μοτίβα γραφής, υφή και δομή υπογραφής. Αυτά τα χαρακτηριστικά ήταν ζωτικής σημασίας για να μπορέσουν οι ταξινομητές μηχανικής μάθησης να διακρίνουν με ακρίβεια τις γνήσιες από τις πλαστές υπογραφές.
Οι παραδοσιακοί αλγόριθμοι μηχανικής μάθησης, όπως οι μηχανές διανυσμάτων υποστήριξης (SVM) και τα τυχαία δάση, είχαν σταθερά καλή απόδοση όταν εφαρμόστηκαν στα διανύσματα χαρακτηριστικών που εξήχθησαν από τη βαθιά μάθηση. Οι SVM και Random Forest, ειδικότερα, επέδειξαν υψηλή ακρίβεια, ακρίβεια, ανάκληση και βαθμολογία F1 σε διάφορα πειράματα. Αυτοί οι ταξινομητές αποδείχθηκαν αξιόπιστοι στο χειρισμό των εξαχθέντων χαρακτηριστικών και στη μετατροπή τους σε ακριβείς προβλέψεις. Οι υψηλές βαθμολογίες AUC επιβεβαίωσαν περαιτέρω την ικανότητα των μοντέλων να διακρίνουν μεταξύ των δύο κατηγοριών (γνήσιες και πλαστές υπογραφές) σε διαφορετικά κατώφλια.
Ωστόσο, το σύστημα αντιμετώπισε ορισμένες προκλήσεις, ιδίως όσον αφορά τη μεταβλητότητα της ποιότητας των υπογραφών και το περιορισμένο μέγεθος του συνόλου δεδομένων. Το σύνολο δεδομένων αποτελούνταν από υπογραφές με διαφορετική ανάλυση και σαφήνεια, γεγονός που δημιουργούσε δυσκολίες για τα μοντέλα σε ορισμένες περιπτώσεις. Επιπλέον, οι πλαστογραφίες που έμοιαζαν πολύ με τις γνήσιες υπογραφές αποδείχθηκε πιο δύσκολο να εντοπιστούν, ιδίως όταν οι διαφορές μεταξύ τους ήταν πολύ λεπτές.
Ενώ η χρήση της μάθησης μεταφοράς μετρίασε σε κάποιο βαθμό το ζήτημα των περιορισμένων δεδομένων, το σχετικά μικρό σύνολο δεδομένων περιόρισε την ικανότητα των μοντέλων βαθιάς μάθησης να αξιοποιήσουν πλήρως τις δυνατότητές τους.Αυτός ο περιορισμός πιθανώς συνέβαλε στις περιστασιακές λανθασμένες ταξινομήσεις του συστήματος, ιδίως όταν επρό-

κειτο για εξαιρετικά επιδέξιες πλαστογραφίες ή υπογραφές που παρουσίαζαν σημαντική μεταβλητότητα εντός του γραφικού χαρακτήρα του ίδιου ατόμου.
Παρά τις προκλήσεις αυτές, το σύστημα επέδειξε ισχυρή ικανότητα γενίκευσης σε αόρατα δεδομένα. Αυτό είναι ζωτικής σημασίας για εφαρμογές στον πραγματικό κόσμο, όπου το σύστημα πρέπει να χειριστεί μια ποικιλία υπογραφών από διαφορετικά άτομα υπό διαφορετικές συνθήκες. Τα στιβαρά βήματα προεπεξεργασίας, σε συνδυασμό με την υβριδική προσέγγιση της εξαγωγής χαρακτηριστικών βαθιάς μάθησης και της παραδοσιακής ταξινόμησης με μηχανική μάθηση, επέτρεψαν στο σύστημα να αποδώσει αξιόπιστα σε ένα ευρύ φάσμα υπογραφών. Συνοψίζοντας, η πειραματική μελέτη επιβεβαίωσε την αποτελεσματικότητα του υβριδικού συστήματος ανίχνευσης πλαστογραφίας υπογραφών. Ο συνδυασμός της βαθιάς μάθησης και της παραδοσιακής μηχανικής μάθησης επέτρεψε μια ισχυρή και ευέλικτη προσέγγιση για την επαλήθευση υπογραφών. Ενώ παρατηρήθηκαν προκλήσεις που σχετίζονται με τη μεταβλητότητα των δεδομένων και το μέγεθος του συνόλου δεδομένων, η συνολική απόδοση του συστήματος υποδηλώνει ότι είναι κατάλληλο για εφαρμογές στον πραγματικό κόσμο, όπου η ακρίβεια και η αξιοπιστία είναι υψίστης σημασίας για την ανίχνευση πλαστών υπογραφών.

Κεφάλαιο 7

Συμπεράσματα και μελλοντική έρευνα

Στο κεφάλαιο αυτό παρουσιάζονται τα βασικά συμπεράσματα που προέκυψαν από την ανάπτυξη και την πειραματική μελέτη του συστήματος ανίχνευσης πλαστογραφίας υπογραφών. Επιπλέον, περιγράφει πιθανές κατευθύνσεις για μελλοντική έρευνα με σκοπό την περαιτέρω ενίσχυση των δυνατοτήτων του συστήματος.

7.1 Συμπεράσματα

Ο πρωταρχικός στόχος της παρούσας πτυχιακής εργασίας ήταν η ανάπτυξη ενός αξιόπιστου και ακριβούς συστήματος για την ανίχνευση πλαστών υπογραφών με την αξιοποίηση των πλεονεκτημάτων της βαθιάς μάθησης και των παραδοσιακών αλγορίθμων μηχανικής μάθησης. Μέσω της υβριδικής προσέγγισης, η οποία συνδύαζε την εξαγωγή χαρακτηριστικών με τη χρήση προεκπαιδευμένων νευρωνικών δικτύων συνελικτικής μάθησης (CNN) με την ταξινόμηση μέσω παραδοσιακών αλγορίθμων μηχανικής μάθησης, το σύστημα κατάφερε να επιτύχει υψηλή ακρίβεια στη διάκριση γνήσιων υπογραφών από πλαστές.
Τα μοντέλα βαθιάς μάθησης, συμπεριλαμβανομένων των VGG16, DenseNet121 και MobileNetV2, ήταν ιδιαίτερα αποτελεσματικά στην αυτόματη εκμάθηση σύνθετων και διαφοροποιημένων χαρακτηριστικών από εικόνες υπογραφών. Χρησιμοποιώντας τη μάθηση μεταφοράς, τα μοντέλα αυτά προσάρμοσαν την προϋπάρχουσα γνώση τους στην εργασία ανίχνευσης πλαστογραφίας υπογραφών, βελτιώνοντας σημαντικά τη συνολική απόδοση του συστήματος. Στη συνέχεια, τα εξαγόμενα διανύσματα χαρακτηριστικών ταξινομήθηκαν με τη χρήση αλγορίθμων μηχανικής μάθησης, όπως οι Μηχανές Διανυσμάτων Υποστήριξης (SVM), τα Τυχαία Δάση και οι K-Nearest Neighbors (KNN), οι οποίοι επέδειξαν ισχυρές επιδόσεις όσον αφορά την ακρίβεια, την ακρίβεια, την ανάκληση και την AUC.
Η πειραματική μελέτη επικύρωσε την αποτελεσματικότητα της υβριδικής προσέγγισης, με τα αποτελέσματα να δείχνουν σταθερά ισχυρή ακρίβεια ταξινόμησης και αξιόπιστη απόδοση σε διάφορες μετρικές. Παρά τις προκλήσεις, όπως το περιορισμένο μέγεθος του συνόλου δεδομέ-

νων και η μεταβλητότητα στην ποιότητα των υπογραφών, το σύστημα αποδείχθηκε ικανό να γενικεύει καλά σε νέα, αθέατα δεδομένα, καθιστώντας το κατάλληλο για πρακτικές εφαρμογές σε διάφορα σενάρια του πραγματικού κόσμου, όπως τραπεζικές συναλλαγές, επαλήθευση νομικών εγγράφων και πιστοποίηση ταυτότητας.
Η παρούσα πτυχιακή εργασία απέδειξε ότι ο συνδυασμός της βαθιάς μάθησης και της παραδοσιακής μηχανικής μάθησης σε έναν αρθρωτό και κλιμακούμενο αγωγό παρέχει μια ισχυρή λύση για την ανίχνευση πλαστότητας υπογραφών. Η ευελιξία, η προσαρμοστικότητα και οι υψηλές επιδόσεις του συστήματος το καθιστούν ένα πολλά υποσχόμενο εργαλείο για χρήση σε περιβάλλοντα ασφάλειας και επαλήθευσης όπου η ακριβής επαλήθευση υπογραφής είναι κρίσιμη.

7.2 Μελλοντική έρευνα

Ενώ το τρέχον σύστημα αποδίδει καλά, υπάρχουν αρκετές ευκαιρίες για μελλοντική έρευνα και βελτιώσεις που θα μπορούσαν να ενισχύσουν περαιτέρω την αποτελεσματικότητά του και να διευρύνουν την εφαρμογή του.

7.2.1 Επέκταση του συνόλου δεδομένων

Ένας από τους πιο σημαντικούς δρόμους για τη μελλοντική έρευνα έγκειται στην επέκταση του συνόλου δεδομένων που χρησιμοποιείται για την εκπαίδευση και τη δοκιμή του συστήματος ανίχνευσης πλαστογραφίας υπογραφών. Το τρέχον σύνολο δεδομένων, αν και επαρκές για την επίδειξη της αποτελεσματικότητας του συστήματος, έχει περιορισμούς όσον αφορά το μέγεθος και την ποικιλομορφία. Η επέκταση του συνόλου δεδομένων θα εισήγαγε μεγαλύτερη μεταβλητότητα σε στυλ γραφής, πλαστογραφίες και συνθήκες υπογραφής, επιτρέποντας στο σύστημα να γενικεύει καλύτερα σε ένα ευρύτερο φάσμα σεναρίων.
Ένα μεγαλύτερο και πιο ποικιλόμορφο σύνολο δεδομένων θα επέτρεπε στα μοντέλα βαθιάς μάθησης να μάθουν πιο σύνθετα μοτίβα και λεπτές αποχρώσεις στις υπογραφές, βελτιώνοντας τελικά την ικανότητά τους να ανιχνεύουν πλαστογραφίες, ιδίως σε περιπτώσεις όπου οι πλαστογράφοι μιμούνται στενά τις γνήσιες υπογραφές. Η ενσωμάτωση υπογραφών από διαφορετικούς πληθυσμούς, πολιτισμικά υπόβαθρα και γλώσσες θα ενίσχυε επίσης την ανθεκτικότητα του συστήματος, καθιστώντας το εφαρμόσιμο σε παγκόσμιες περιπτώσεις χρήσης, όπου τα χαρακτηριστικά του γραφικού χαρακτήρα μπορεί να διαφέρουν σημαντικά[25].

7.2.2 Προηγμένες τεχνικές επαύξησης δεδομένων

Για να αντιμετωπιστούν οι προκλήσεις των περιορισμένων δεδομένων, η μελλοντική έρευνα θα μπορούσε να διερευνήσει πιο προηγμένες τεχνικές επαύξησης δεδομένων. Αυτό θα μπορούσε να περιλαμβάνει τη δημιουργία συνθετικών πλαστογραφιών ή την εφαρμογή μετασχη-

ματισμών σε υπάρχουσες εικόνες υπογραφών για την προσομοίωση διαφορετικών τύπων παραμορφώσεων και παραλλαγών. Η επαύξηση των δεδομένων όχι μόνο θα διευρύνει το σύνολο δεδομένων αλλά και θα εισάγει νέες προκλήσεις για τα μοντέλα, ενθαρρύνοντάς τα να μάθουν πιο ισχυρά χαρακτηριστικά.
Οι συνήθεις τεχνικές επαύξησης δεδομένων, όπως η περιστροφή, η κλιμάκωση, η μετάφραση και η αναστροφή, μπορούν να εφαρμοστούν σε εικόνες υπογραφών για τη δημιουργία νέων παραλλαγών των υφιστάμενων υπογραφών χωρίς να μεταβάλλονται τα βασικά χαρακτηριστικά τους. Αυτοί οι μετασχηματισμοί εισάγουν μεταβλητότητα στα δεδομένα υπογραφών, βοηθώντας το μοντέλο να γίνει πιο ανθεκτικό σε μικρές αλλαγές στο στυλ, τον προσανατολισμό ή το μέγεθος του γραφικού χαρακτήρα, οι οποίες είναι συνηθισμένες σε πραγματικές περιπτώσεις.
Πέρα από τους βασικούς μετασχηματισμούς, οι πιο προηγμένες τεχνικές επαύξησης θα μπορούσαν να περιλαμβάνουν τη δημιουργία συνθετικών πλαστογραφιών με τη χρήση αντιπολιτευτικών μεθόδων ή γενετικών μοντέλων, όπως τα Generative Adversarial Networks (GAN). Αυτές οι συνθετικές πλαστογραφίες θα μπορούσαν να εισάγουν νέες προκλήσεις για το μοντέλο, ενθαρρύνοντάς το να μάθει πιο εξελιγμένα χαρακτηριστικά που διακρίνουν τις γνήσιες υπογραφές από τις ιδιαίτερα πειστικές πλαστογραφίες.
Με την εφαρμογή αυτών των στρατηγικών ενίσχυσης, το σύστημα θα μπορούσε να βελτιώσει την ικανότητά του να ανιχνεύει πλαστογραφίες, ακόμη και σε περιπτώσεις όπου οι διαφορές μεταξύ γνήσιων και πλαστών υπογραφών είναι ανεπαίσθητες. Η επαύξηση όχι μόνο θα βελτίωνε την απόδοση του μοντέλου σε μικρότερα σύνολα δεδομένων, αλλά θα μείωνε επίσης την πιθανότητα υπερπροσαρμογής, με αποτέλεσμα ένα πιο ισχυρό και προσαρμόσιμο σύστημα επαλήθευσης υπογραφών[35][36].

7.2.3 Εξερευνώντας νέους αλγορίθμους

Η μελλοντική έρευνα θα μπορούσε να επικεντρωθεί στη διερεύνηση πιο προηγμένων αλγορίθμων για την περαιτέρω βελτίωση των επιδόσεων του συστήματος ανίχνευσης πλαστογραφίας υπογραφών. Ενώ η τρέχουσα εφαρμογή ενσωματώνει επιτυχώς παραδοσιακούς ταξινομητές μηχανικής μάθησης, όπως οι μηχανές διανυσμάτων υποστήριξης (SVM), τα τυχαία δάση και οι K-Nearest Neighbors (KNN), με μοντέλα βαθιάς μάθησης για την εξαγωγή χαρακτηριστικών, υπάρχουν ακόμη σημαντικές δυνατότητες βελτίωσης της ακρίβειας και της ευρωστίας με τον πειραματισμό με εναλλακτικούς αλγορίθμους.
Μια πολλά υποσχόμενη κατεύθυνση είναι η διερεύνηση της χρήσης μεθόδων συνόλου, οι οποίες συνδυάζουν τις προβλέψεις πολλαπλών ταξινομητών για την επίτευξη καλύτερης συνολικής απόδοσης. Τεχνικές όπως η στοίβαξη, το boosting (π.χ. XGBoost, AdaBoost) και το bagging θα μπορούσαν να εφαρμοστούν στα εξαγόμενα διανύσματα χαρακτηριστικών, παρέχοντας μια πιο ολοκληρωμένη προσέγγιση στην ταξινόμηση με την αξιοποίηση των πλεονεκτημάτων των διαφορετικών μοντέλων. Οι μέθοδοι ensemble είναι ιδιαίτερα αποτελεσματικές στη μείωση της

υπερπροσαρμογής και στη βελτίωση της γενίκευσης, ιδίως σε πολύπλοκες εργασίες όπως η ανίχνευση πλαστογραφίας.
Ένας άλλος τομέας ενδιαφέροντος είναι η εξερεύνηση πιο προηγμένων αρχιτεκτονικών βαθιάς μάθησης. Για παράδειγμα, τα μοντέλα που βασίζονται στην προσοχή, όπως οι μετασχηματιστές, έχουν επιδείξει αξιοσημείωτη επιτυχία σε διάφορους τομείς, επιτρέποντας στο μοντέλο να εστιάζει στα πιο σημαντικά τμήματα των δεδομένων εισόδου. Η ενσωμάτωση μηχανισμών προσοχής θα μπορούσε να επιτρέψει στο σύστημα να συλλάβει καλύτερα τις βασικές λεπτομέρειες στις εικόνες υπογραφών που είναι ενδεικτικές των πλαστογραφιών. Επιπλέον, τα επαναλαμβανόμενα νευρωνικά δίκτυα (RNN) και τα δίκτυα μακράς βραχυπρόθεσμης μνήμης (LSTM) θα μπορούσαν να διερευνηθούν για την ανάλυση δυναμικών πληροφοριών σε δεδομένα υπογραφών, ιδίως σε περιπτώσεις όπου τα χρονικά μοτίβα ή οι ακολουθίες γραφής παίζουν σημαντικό ρόλο στη διάκριση μεταξύ γνήσιων και πλαστών υπογραφών.
Τέλος, ο πειραματισμός με βαθιά νευρωνικά δίκτυα σχεδιασμένα ειδικά για μικρά σύνολα δεδομένων, όπως η εκμάθηση λίγων λήψεων ή οι τεχνικές μετα-μάθησης, θα μπορούσαν να επιτρέψουν στο σύστημα να προσαρμόζεται ταχύτερα σε νέους τύπους υπογραφών και πλαστογραφιών με περιορισμένα παραδείγματα εκπαίδευσης. Αυτές οι προσεγγίσεις επικεντρώνονται στην εκπαίδευση μοντέλων που μπορούν να γενικεύσουν καλά από λίγα μόνο δείγματα, καθιστώντας τα ιδανικά για εργασίες επαλήθευσης υπογραφών όπου η απόκτηση μεγάλων ποσοτήτων επισημασμένων δεδομένων μπορεί να είναι δύσκολη[37][38].

7.2.4 Επαλήθευση υπογραφών σε πραγματικό χρόνο

Μια πολλά υποσχόμενη κατεύθυνση για μελλοντική έρευνα είναι η βελτιστοποίηση του συστήματος ανίχνευσης πλαστότητας υπογραφής για επαλήθευση υπογραφής σε πραγματικό χρόνο. Επί του παρόντος, το σύστημα είναι ικανό να επεξεργάζεται και να ταξινομεί υπογραφές με μεγάλη ακρίβεια, αλλά η βελτίωση της ταχύτητας και της απόκρισης θα του επέτρεπε να αναπτυχθεί σε εφαρμογές που απαιτούν άμεση επαλήθευση, όπως τερματικά πώλησης, υπογραφή νομικών εγγράφων ή συστήματα ελέγχου πρόσβασης.
Για την επίτευξη επεξεργασίας σε πραγματικό χρόνο, οι μελλοντικές εργασίες θα μπορούσαν να επικεντρωθούν στον εξορθολογισμό της αρχιτεκτονικής του συστήματος. Αυτό θα μπορούσε να περιλαμβάνει τη βελτιστοποίηση του αγωγού προεπεξεργασίας για τη μείωση της καθυστέρησης, όπως η απλούστευση των μετασχηματισμών εικόνας ή η χρήση αποδοτικότερων αλγορίθμων για την εξαγωγή χαρακτηριστικών. Επιπλέον, η αξιοποίηση αποδοτικότερων εκδόσεων μοντέλων βαθιάς μάθησης, όπως το MobileNetV3 ή κβαντισμένων μοντέλων, θα επέτρεπε ταχύτερη εξαγωγή χαρακτηριστικών χωρίς να θυσιάζεται η ακρίβεια.
Η υλοποίηση επαλήθευσης σε πραγματικό χρόνο απαιτεί επίσης τη βελτιστοποίηση των ταξινομητών μηχανικής μάθησης για ταχύτητα. Τεχνικές όπως το κλάδεμα του μοντέλου, όπου οι λιγότερο σημαντικές παράμετροι αφαιρούνται από το μοντέλο, και η κβάντιση, η οποία μειώνει

την ακρίβεια των βαρών και των ενεργοποιήσεων του μοντέλου, θα μπορούσαν να βοηθήσουν στη μείωση του υπολογιστικού φόρτου και του χρόνου εξαγωγής συμπερασμάτων. Αυτές οι βελτιστοποιήσεις θα μπορούσαν να επιταχύνουν σημαντικά το στάδιο της ταξινόμησης, επιτρέποντας στο σύστημα να επαληθεύει υπογραφές σε κλάσματα του δευτερολέπτου.
Επιπλέον, η μετάβαση του συστήματος για να λειτουργήσει σε συσκευές άκρων ή σε πλατφόρμες που βασίζονται στο νέφος θα μπορούσε να επιτρέψει ταχύτερη, αποκεντρωμένη επεξεργασία. Αυτό θα επέτρεπε την επαλήθευση σε πραγματικό χρόνο σε καταστάσεις όπου η συνδεσιμότητα στο διαδίκτυο ή οι κεντρικοί πόροι επεξεργασίας μπορεί να είναι περιορισμένοι, καθιστώντας το σύστημα πιο προσιτό και προσαρμόσιμο σε διάφορα περιβάλλοντα του πραγματικού κόσμου[39][40].

7.2.5 Διατροπική επαλήθευση υπογραφής

Ένας άλλος πολλά υποσχόμενος τομέας για μελλοντική έρευνα είναι η διερεύνηση της διατροπικής επαλήθευσης υπογραφών, η οποία θα περιλαμβάνει το συνδυασμό στατικής ανάλυσης υπογραφών βάσει εικόνας με δυναμικά βιομετρικά δεδομένα. Στα παραδοσιακά συστήματα επαλήθευσης υπογραφών, η εστίαση γίνεται κυρίως σε στατικά χαρακτηριστικά, όπως μοτίβα κινήσεων, μεταβολές πίεσης και συνολική δομή της υπογραφής. Ωστόσο, η ενσωμάτωση δυναμικών δεδομένων υπογραφής -όπως η ταχύτητα, ο χρόνος και η πίεση που ασκείται κατά τη διαδικασία υπογραφής- θα μπορούσε να βελτιώσει σημαντικά την ικανότητα του συστήματος να ανιχνεύει πλαστογραφίες.
Η δυναμική επαλήθευση υπογραφών περιλαμβάνει την καταγραφή των μοναδικών χαρακτηριστικών συμπεριφοράς της διαδικασίας υπογραφής ενός ατόμου. Τα δεδομένα αυτά μπορούν να συλλεχθούν μέσω εξειδικευμένων συσκευών, όπως οι ταμπλέτες ψηφιοποίησης, οι οποίες καταγράφουν τα χρονικά χαρακτηριστικά της υπογραφής κατά τη διάρκεια της γραφής της. Με την ενσωμάτωση τόσο των στατικών οπτικών χαρακτηριστικών όσο και των δυναμικών δεδομένων συμπεριφοράς, το σύστημα θα μπορούσε να αξιοποιήσει μια πολυτροπική προσέγγιση που συλλαμβάνει πιο ολοκληρωμένες πληροφορίες, καθιστώντας ακόμη πιο δύσκολο για τους πλαστογράφους να αντιγράψουν τόσο την εμφάνιση όσο και τη διαδικασία της γνήσιας υπογραφής.
Η ενσωμάτωση διατροπικών δεδομένων θα απαιτούσε την προσαρμογή της αρχιτεκτονικής του συστήματος ώστε να μπορεί να φιλοξενήσει πολλαπλούς τύπους δεδομένων. Για παράδειγμα, τα νευρωνικά δίκτυα συνελίξεων (CNN) θα μπορούσαν να συνεχίσουν να επεξεργάζονται τα στατικά δεδομένα εικόνας, ενώ τα επαναλαμβανόμενα νευρωνικά δίκτυα (RNN) ή τα δίκτυα μακράς βραχυπρόθεσμης μνήμης (LSTM) θα μπορούσαν να χρησιμοποιηθούν για την ανάλυση της διαδοχικής φύσης των δυναμικών δεδομένων. Η συγχώνευση αυτών των ροών δεδομένων θα μπορούσε να επιτευχθεί μέσω πολυτροπικών τεχνικών βαθιάς μάθησης, με αποτέλεσμα ένα πιο ισχυρό σύστημα επαλήθευσης υπογραφών που είναι πιο δύσκολο να

εξαπατηθεί[41][42].

7.2.6 Θέματα ασφάλειας και προστασίας προσωπικών δεδομένων

Καθώς το σύστημα ανίχνευσης πλαστογραφίας υπογραφών προχωρά προς την ανάπτυξη στον πραγματικό κόσμο, η αντιμετώπιση των προβλημάτων ασφάλειας και προστασίας της ιδιωτικής ζωής θα είναι ζωτικής σημασίας. Το σύστημα ασχολείται με ευαίσθητα βιομετρικά δεδομένα, γεγονός που καθιστά απαραίτητη τη διασφάλιση της προστασίας των δεδομένων αυτών από μη εξουσιοδοτημένη πρόσβαση και κατάχρηση. Η μελλοντική έρευνα θα πρέπει να επικεντρωθεί στην ενίσχυση της ασφάλειας του συστήματος, προστατεύοντας τόσο τα δεδομένα όσο και τα μοντέλα από πιθανές απειλές.
Μια σημαντική ανησυχία είναι η προστασία του συστήματος από εχθρικές επιθέσεις, όπου οι επίβουλοι παραποιούν τις υπογραφές εισόδου για να εξαπατήσουν τα μοντέλα ανίχνευσης. Η έρευνα θα μπορούσε να διερευνήσει την εφαρμογή τεχνικών εκπαίδευσης με αντίπαλο τρόπο, όπου τα μοντέλα εκπαιδεύονται σε διαταραγμένα δεδομένα για να γίνουν πιο ανθεκτικά σε τέτοιου είδους επιθέσεις. Η διασφάλιση ότι το σύστημα μπορεί να αντέξει τις προσπάθειες των αντιπάλων είναι ιδιαίτερα σημαντική σε περιβάλλοντα με υψηλό ρίσκο, όπως ο τραπεζικός ή ο νομικός έλεγχος, όπου η επιτυχής πλαστογράφηση μπορεί να έχει σοβαρές συνέπειες.
Μια άλλη κρίσιμη πτυχή είναι το απόρρητο των βιομετρικών δεδομένων που χρησιμοποιούνται στο σύστημα. Τα δεδομένα υπογραφής είναι μια μορφή προσωπικών πληροφοριών και η συλλογή, αποθήκευση και επεξεργασία τους πρέπει να συμμορφώνεται με τους κανονισμούς προστασίας δεδομένων, όπως ο GDPR ή η CCPA. Θα πρέπει να χρησιμοποιούνται τεχνικές κρυπτογράφησης και ασφαλούς αποθήκευσης για να διασφαλίζεται ότι τα δεδομένα υπογραφής παραμένουν εμπιστευτικά και προστατεύονται από παραβιάσεις[43][44][45].

7.2.7 Προσαρμογή σε διαφορετικές γλώσσες και σενάρια

Ένας σημαντικός τομέας για μελλοντική έρευνα είναι η προσαρμογή του συστήματος ανίχνευσης πλαστότητας υπογραφών για την επαλήθευση υπογραφών σε διαφορετικές γλώσσες και γραφές. Επί του παρόντος, το σύστημα είναι προσαρμοσμένο για υπογραφές γραμμένες σε λατινικές γραφές, αλλά οι υπογραφές σε μη λατινικές γραφές - όπως η αραβική, η κινεζική, η κυριλλική και άλλες - δημιουργούν μοναδικές προκλήσεις λόγω των διαφορετικών συμβάσεων γραφής, των δομών των χαρακτήρων και των καλλιγραφικών στυλ.
Οι μη λατινικές γραφές έχουν συχνά διακριτά μοτίβα, κατευθύνσεις και πολυπλοκότητες που διαφέρουν σημαντικά από τις υπογραφές που βασίζονται στα λατινικά. Για παράδειγμα, στις αραβικές γραφές, οι χαρακτήρες συχνά συνδέονται και η ροή της γραφής είναι συνήθως από δεξιά προς τα αριστερά, σε αντίθεση με τις λατινικές γραφές, οι οποίες είναι από αριστερά προς τα δεξιά. Ομοίως, οι κινεζικοί χαρακτήρες αποτελούνται από περίπλοκες πινελιές και ρίζες που απαιτούν διαφορετικές τεχνικές εξαγωγής χαρακτηριστικών. Αυτές οι παραλλαγές

απαιτούν εξειδικευμένα μοντέλα και τεχνικές προεπεξεργασίας για την ακριβή αποτύπωση των αποχρώσεων κάθε γραφής[46].

7.3 Κατακλείδα

Εν κατακλείδι, ενώ το τρέχον σύστημα αποτελεί ένα σημαντικό βήμα προόδου στον τομέα της ανίχνευσης πλαστογραφίας υπογραφών, υπάρχουν πολλά περιθώρια για περαιτέρω διερεύνηση και καινοτομία. Με την επέκταση του συνόλου δεδομένων, τη διερεύνηση νέων αλγορίθμων και τη βελτιστοποίηση του συστήματος για χρήση σε πραγματικό χρόνο, η μελλοντική έρευνα μπορεί να βασιστεί στα θεμέλια που δημιουργήθηκαν στην παρούσα πτυχιακή εργασία, για την ανάπτυξη ακόμη πιο ισχυρών και ευέλικτων εργαλείων για την επαλήθευση υπογραφών και την ανίχνευση πλαστογραφίας.

Βιβλιογραφία

[1] D. Choi and other authors, "Uav-driven structural crack detection and location determination using convolutional neural networks," *ResearchGate*, 2021. Accessed: 2024-08-20.

[2] R. Rasti *et al.*, "Breast cancer screening using convolutional neural network and follow-up digital mammography," *ResearchGate*, 2018. Accessed: 2024-08-20.

[3] N. Radwan *et al.*, "Leveraging sparse and dense features for reliable state estimation in urban environments," *ResearchGate*, 2019. Accessed: 2024-08-20.

[4] S. K. S. Madipally *et al.*, "Fine-tuned densenet-169 for breast cancer metastasis prediction using fastai and 1-cycle policy," *ResearchGate*, 2022. Accessed: 2024-08-20.

[5] R. Mahum *et al.*, "A novel framework for potato leaf disease detection using an efficient deep learning model," *ResearchGate*, 2022. Accessed: 2024-08-20.

[6] M. U. Asad *et al.*, "Efficient approach towards detection and identification of copy move and image splicing forgeries using mask r-cnn with mobilenet v1," *ResearchGate*, 2022. Accessed: 2024-08-20.

[7] J. Martínez *et al.*, "Architecture of mobilenetv2." Image from: Facial Recognition System for People with and without Face Mask in Times of the COVID-19 Pandemic, 2021. Accessed: 2024-08-20.

[8] E. Westphal *et al.*, "A machine learning method for defect detection and visualization in selective laser sintering based on convolutional neural networks," *ResearchGate*, 2021. Accessed: 2024-08-20.

[9] L. Aldakhil *et al.*, "Multi-fruit classification and grading using a same-domain transfer learning approach," *ResearchGate*, 2024. Accessed: 2024-08-20.

[10] Y. Wang, H. Zheng, Y. Xia, H. Wang, Q. Li, and J. Zhang, "Convolutional neural network based features for motor imagery eeg signals classification in brain-computer interface system," *Journal of Neuroscience Methods*, vol. 337, p. 108651, 2020.

[11] H. Bhardwaj, A. Verma, S. Kumar, and J. Basak, "Target detection using supervised machine learning algorithms for gpr data," *International Journal of Remote Sensing*, vol. 41, no. 14, pp. 5423–5446, 2020.

[12] R. Elnadree *et al.*, "Performance investigation of features extraction and classification approaches for sentiment analysis systems," *ResearchGate*, 2021. Accessed: [Date of Access].

[13] V. Kanade, "What is decision tree?," 2022. Accessed: August 29, 2024.

[14] Z. Yang, Y. Chen, X. Luo, and L. Ma, "Pre-evacuation time estimation-based emergency evacuation simulation in urban residential communities," *International Journal of Environmental Research and Public Health*, vol. 16, no. 22, p. 4538, 2019.

[15] S. Bhattacharyya, "Introduction to naïve bayes classifier," 2019. Accessed: 2024-08-20.

[16] X. Zhang, R. Kumar, R. Sharma, and X. Wang, "A review - signature verification system using deep learning: A challenging problem," *ResearchGate*, 2021.

[17] S. Elliott, "The challenge of forgeries and perception of dynamic signature verification," in *Proceedings of the 2002 International Workshop on Frontiers in Handwriting Recognition (IWFHR)*, pp. 122–127, IEEE, 2002.

[18] H. Wang, M. Xu, Y. Liu, and Q. Chen, "Robust offline handwritten signature verification and forgery detection via hybrid deep learning," *Multimedia Tools and Applications*, vol. 81, no. 20, pp. 29541–29559, 2022.

[19] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 1800–1807, 2017.

[20] E. A. Soelistio, R. E. Hananto Kusumo, Z. V. Martan, and E. Irwansyah, "A review of signature recognition using machine learning," in *2021 1st International Conference on Computer Science and Artificial Intelligence (ICCSAI)*, vol. 1, pp. 219–223, 2021.

[21] A. G. Howard, M. Zhu, B. Chen, D. Kalenichenko, W. Wang, T. Weyand, M. Andreetto, and H. Adam, "Mobilenets: Efficient convolutional neural networks for mobile vision applications," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017.

[22] M. Tan and Q. V. Le, "Efficientnet: Rethinking model scaling for convolutional neural networks," in *Proceedings of the 36th International Conference on Machine Learning*, pp. 6105–6114, PMLR, 2019.

[23] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Writer-independent feature learning for offline signature verification using deep convolutional neural networks," in *2016 International Joint Conference on Neural Networks (IJCNN)*, pp. 2576–2583, IEEE, 2016.

[24] J. A. P. Lopes, B. Baptista, N. Lavado, and M. Mendes, "Offline handwritten signature verification using deep neural networks," *Energies*, vol. 15, no. 20, p. 7611, 2022.

[25] T. Jadhav, "Handwritten signature verification using local binary pattern," *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 4, pp. 579–584, 2019.

[26] F. Pedregosa, G. Varoquaux, A. Gramfort, V. Michel, B. Thirion, O. Grisel, M. Blondel, P. Prettenhofer, R. Weiss, V. Dubourg, J. Vanderplas, A. Passos, D. Cournapeau, M. Brucher, M. Perrot, and E. Duchesnay, "Scikit-learn: Machine learning in python," *Journal of Machine Learning Research*, vol. 12, pp. 2825–2830, 2011.

[27] W. McKinney, "Data structures for statistical computing in python," in *Proceedings of the 9th Python in Science Conference (SciPy 2010)*, pp. 56–61, Austin, TX, 2010.

[28] F. Chollet, *Deep Learning with Python*. Shelter Island, NY: Manning Publications Co., 2018.

[29] C. R. Harris, K. J. Millman, S. J. van der Walt, R. Gommers, P. Virtanen, D. Cournapeau, E. Wieser, J. Taylor, S. Berg, N. J. Smith, R. Kern, M. Picus, S. Hoyer, M. H. van Kerkwijk, M. Brett, A. Haldane, J. Fernández del Río, M. Wiebe, P. Peterson, P. Gérard-Marchant, K. Sheppard, T. Reddy, W. Weckesser, H. Abbasi, C. Gohlke, and T. E. Oliphant, "Array programming with numpy," *Nature*, vol. 585, no. 7825, pp. 357–362, 2020.

[30] J. D. Hunter, "Matplotlib: A 2d graphics environment," *Computing in Science & Engineering*, vol. 9, no. 3, pp. 90–95, 2007.

[31] Q. Huang, C. Zhou, and G. Zhang, "Color code structure design and recognition using opencv," in *2022 2nd International Conference on Computer Graphics, Image and Virtualization (ICCGIV)*, pp. 28–33, IEEE, 2022.

[32] T. E. Oliphant, "Python for scientific computing," *Computing in Science & Engineering*, vol. 9, no. 3, pp. 10–20, 2007.

[33] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY: Springer, 2006.

[34] C. D. Manning, P. Raghavan, and H. Schütze, *Introduction to Information Retrieval*. Cambridge University Press, 2008.

[35] C. Shorten and T. M. Khoshgoftaar, "Data augmentation for deep learning: A survey," *Journal of Big Data*, vol. 6, no. 1, p. 60, 2019.

[36] S. Ghosh, S. Chakraborty, and A. Chakrabarti, "Synthetic data generation for machine learning: An introduction," *Journal of Machine Learning Research*, vol. 21, pp. 1–25, 2020.

[37] Z.-H. Zhang, *Ensemble Methods: Foundations and Algorithms*. CRC Press, 2012.

[38] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, . Kaiser, and I. Polosukhin, "Attention is all you need," in *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.

[39] U. Pal, A. Malik, and S. Singh, "Real-time handwriting signature verification using deep learning techniques," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, no. 5, 2021.

[40] I. Hubara, M. Courbariaux, D. Soudry, R. El-Yaniv, and Y. Bengio, "Quantized neural networks: Training neural networks with low precision weights and activations," *Journal of Machine Learning Research*, 2017.

[41] A. Ross and A. Jain, "Multimodal biometric systems: A comparative study," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 1019–1033, 2004.

[42] M. Diaz, M. A. Ferrer, and A. Morales, "Dynamic signature verification: Fusion of discriminative static and dynamic features," *Pattern Recognition*, vol. 93, pp. 178–189, 2019.

[43] B. Biggio and F. Roli, "Adversarial machine learning at scale," *IEEE Intelligent Systems*, vol. 33, no. 3, pp. 26–38, 2018.

[44] C. Rathgeb, C. Busch, and A. Dantcheva, "Privacy and security in biometric systems: Threats and countermeasures," *IET Biometrics*, vol. 9, no. 3, pp. 91–103, 2020.

[45] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric security: A modern approach," *IEEE*

Communications Magazine, vol. 50, no. 8, pp. 43–51, 2012.

[46] R. Plamondon and S. N. Srihari, "Online and offline handwriting recognition: A comprehensive survey," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 1, pp. 63–84, 2000.