Deep Neural Networks for Robust Handwritten Signature Verification: A Comparative Study

BY

KHOSNUR ALAM
ID: 232-25-044

This Report Presented in Partial Fulfillment of the Requirements for
The Degree of Masters of Science in Computer Science and Engineering

Supervised By

Dr. Fizar Ahmed
Associate Professor
Department of CSE
Daffodil International University

Co-Supervised By

Dr. Arif Mahmud
Associate Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

APPROVAL

This Project/Thesis titled **"Deep Neural Networks for Robust Handwritten Signature Verification: A Comparative Study"**, submitted by **Khosnur Alam**, ID No: **232-25-044** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **11-01-2025**.

BOARD OF EXAMINERS

Chairman

Dr. Sheak Rashed Haider Noori, PhD
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Md. Zahid Hasan, PhD
Associate Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner

Dr. Arif Mahmud, PhD
Associate Professor & Director MIS
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

External Examiner

Dr. Mohammed Nasir Uddin, PhD
Professor
Department of Computer Science and Engineering
Jagannath University

DECLARATION

I hereby declare that this research has been done by me under the supervision of **Dr. Fizar Ahmed Associate Professor, Department of CSE,** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:

Dr. Fizar Ahmed
Associate Professor
Department of CSE
Daffodil International University

Co-Supervised by:

Dr. Asif Mahmud
Associate Professor
Department of CSE
Daffodil International University

Submitted by:

Khosnur Alam
ID: 232-25-044
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First I express my heartiest thanks and gratefulness to Almighty Allah for His divine blessing which makes it possible to complete the final year project/internship successfully.

I am really grateful and wish my profound indebtedness to **Dr. Fizar Ahmed Associate Professor**, Department of CSE, Daffodil International University, Dhaka, deep knowledge & keen interest of my supervisor in the field of Machine Learning to carry out this project. His endless patience, scholarly guidance ,continual encouragement , constant and energetic supervision, constructive criticism , valuable advice ,reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

I would like to express my heartiest gratitude to **Dr. Sheak Rashed Haider Noori**, **Head,** Department of CSE, for his kind help to finish our project and also to other faculty members and the staff of CSE department of Daffodil International University.

Finally, I must acknowledge with due respect the constant support and patients of my parents.

ABSTRACT

This work is another step in the direction of state-of-the-art deep neural networks-based robust handwritten signature verification. In the field of fraud detection and identity verification, there is increasing need for robust authentication techniques, and so signature verification becomes a key problem . In this paper, three of the most widely used deep learning architectures are objectively analyzed on a well-known dataset to measure their performance; ResNet 50,Resnet50_Augmentation, Inception V3,MobileNet V2,MobileNetV2_Augmentation.A systematic training and testing of models with performance evaluation using metrics such as accuracy. The models were trained under a common training procedure so that all results could be comparable. And after that we have applied Data Augmentation in data set and trained these model again.The results show that of the three models tested, ResNet 50 gives the best accuracy and claim the first place with an accuracy of 98.21%, while Resnet50_Augmentation at second place give us a result with an accuracy of 89.48% Inception V3 is 79.47%Inception_V3_Augmentation is 47.71 and finally MobileNet V2 is in third place captured an new accuracies as well which was about 75.22%,MobileNetV2_Augmentation 67.29%. These results demonstrate the potential to outperform the others, further illustrating ResNet 50 architecture's capability of tackling handwriting signature complexity. Papers with code Significance The paper explains effectiveness of different neural net architectures on a signature verification task. Based on our conclusions we find that ResNet 50 is the highest performing in terms of Signature Authentication and additionally believe this leaves potential future work for optimization and use cases in realistic implementations

.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

1.1 Introduction

Handwritten Signature Verification is a well-understood biometric technique for identity verification, transaction confirmation and legal, financial or administrative document validation [1]. Although new biometric methods are being introduced, signature verification is still the most popular method for its ease of usage and non-intrusiveness to users [2]. Nonetheless, there are still some challenges that need to be addressed like interpersonal variability changes in the signature of an individual over time and also forgery which makes it essential that we come up with strong solutions which will be able to discriminate between genuine signatures and forged signatures despite varying conditions [3].

DNNs have considerable potential as a visual pattern learning approach for biometric verification [3], particularly for complex tasks (such as signature verification) requiring both pixel-level spatial patterns and also temporal information across non-neighboring pixels [4]. DNNs appear to provide a significant performance improvement compared to traditional machine learning models, especially when used on high-dimensional signature data that consists of blended dynamic and static features [5]. However there are not abundant studies that directly compare performances of different DNN architectures on signature verification in similar conditions [6].

In this study, we fill these gaps by performing a systematic comparison between the three architectures; ResNet-50, Inception V3 and MobileNet V 2 on a standard dataset. ResNet50 performs best with an accuracy of 98.18%, followed by Inception V3 at 88.98% and MobileNet V2 at 69.89%, revealing ResNet-50's better ability to model the complexities in signature verification problems. We also investigate the effect of data augmentation on model generalization and transfer learning to alleviate problems related to limited data [7], [8], [9]. However, these new findings are the data that can help power more robust automated verification systems to tackle the issues of practical interest.

1.2 Research Questions

- RQ1: How do different deep neural network architectures compare with each other for handwritten signature verification?

- RQ2: What are the effects of intra-personal variability on the performance of DNNs in verifying handwritten signatures?

1.3 Expected Output

- Compare and Develop Robust Models: This paper aims to develop robust models (namely ResNet50, Inception V3 and Mobile Net V2) for the accuracy of handwritten signature verification.

- Performance Benchmarking: Different deep learning architectures will be compared against traditional methods in extensive benchmarking in terms of accuracy, precision, recall and F1-score.

- Enhanced Forgery Identification: This type of research intends to enhance the susceptibility to forged signatures by providing new approaches based on deep neural networks (DNNs) which ultimately can provide a better reliability score for biometric verification systems.

- Understanding the Effects of Data Augmentation: The effect data augmentation techniques have on model generalization and performance will be studied, providing insights into developing best practices to train deep learning models in signature verification.

- Implications for Future Work: The results in this paper may provide a foundation for understanding future research on biometric verification domains, particularly using DNNs for even more complex pattern recognition tasks.

- This helps the biometric security in signature authentication with much better procedure to handle real-time authentication of signatures.

1.4 Project Management and Finance

The research work doesn't get fund from any individuals or organization.

CHAPTER 2
BACKGROUND

2.1 Preliminaries/Terminologies

Biometric authentication — a technology that relies on unique physiological or behavioral characteristics to verify the identity of an individual; fingerprints, facial recognition, signature.

Deep Neural Networks (DNNs): Simulated models of the human nervous system, neural networks can learn abstractions from high-dimensional data. DNNs have the advantage of being good at tasks that require visual pattern recognitions, like signature verification.

Intersubject Variability: Differences in features of signatures among different persons that may jeopardize the verification accuracy.

Intra-personal Variation: This refers to variations seen in an individual signature over time which can further make the verification process difficult.

Perspectives Data Augmentation: This method is used to get the more variety in training data by transforming the existing images, e.g. the rotation, scaling, or flipping applied. So it helps for better generalization of the model.

Model Evaluation Metrics:

Accuracy A measurement in machine learning that is calculated as the ratio of correctly classified instances among all instances.

Precision : The count of positive predictions that are actually correct, divided by the total number of predicted positives (TP + FP)

Recall: (also known as sensitivity) it quantifies the ability of a model to correctly identify positive instances.

Specificity: The percentage of true negative found by the model.

F1–score: The harmonic mean between precision and recall. It gives an equal weightage to both metrics.

Architectures Compared:

ResNet-50: Residual or ResNet refers to a deep convolutional neural network having 50 layers that solves the problem of vanishing gradients by adding skip connections.

Architecture for image classification that utilizes Inception modules to efficiently capture multi-scale features Inception V3

MobileNet V2: All mobile optimized (lightweight) model, Efficient Mobile Backbone focus on the right balance between Accuracy and Speed.

2.2 Related works

[10] Sharma et al. proposed a writer-independent offline signature verification system by means of the use of a Convolutional Siamese Network to compare stored-reference and new signatures for authenticity analysis. When evaluated on a dataset containing 750 signatures belonging to 30 subjects, it gave an accuracy of 91.6% thus proving the model appropriate for signature verification application.

[11] Hashim et al. proposed a writer-independent offline signature verification model based on a fast hyper deep neural network (FHDNN). A hybrid feature extraction model with different approaches based on PCA (for Appearance), GLCM (for texture) and FFT (For frequency) providing 100% accuracy results for both the SigComp2011 and CEDAR datasets. Evaluation on the test shows metrics of high performance with precision as 1.00 and fairly strong recall and F-score values, outperforming previous methods

[12] Lopes et al. proposed a system for offline handwritten signature verification using deep neural networks to verify signatures of attendance. It compares Optical Mark Recognition of signature presence with a multiclass CNN based on AlexNet, achieving over 85% precision and recall for author identification. The model by using data augmentation also works small, better distinguishing the real signatures.

[13] Poddar et al. proposed a method based on deep learning to resolve the problem of offline signature verification against signature forgery. The offline signature is a task that has intrinsic characteristics of limited uniqueness and intra-personal variations making it difficult to verify. Introduced biometric authentication through static signatures to effectively distinguish genuine signatures from forgeries and accurately prevent fraud using the proposed model.

[14] Zouari et al. proposed an innovative online handwriting signature verification system combining beta-elliptic modeling with Temporal Residual Networks and Multi-Head Attention. The beta-elliptic model divides the signature trajectory into strokes, capturing dynamic and geometric properties. For verification, Temporal Residual Networks with multi-head attention enhance sequential data processing by focusing on key aspects of the signature. Tested on the SVC-2004 and SCOUT-MSIG datasets, the model achieved stateof-the-art performance, with Equal Error Rates of 0.114 and 0.133, respectively.

[15] Hashim et al. conducted a comprehensive review of recent advancements in online and offline handwritten signature verification, analyzing over 20 studies from the last decade. The paper compares various datasets, feature extraction methods, and machine learning classification techniques, highlighting their limitations and advantages. A summary table provides an overview of machine learning methods and commonly used datasets in signature verification.

[16] Tolosana et al. proposed a new writer-independent online signature verification approach based on Recurrent Neural Networks (RNNs) in a Siamese architecture to learn dissimilarity functions between pairs of signatures. The approach is quite efficient in capturing contextual information considering both Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU) model, in bidirectional fashion. On the BiosecurID database composed of 11,200 signatures from 400 users, our system obtained better results than the state-of-the-art solutions.

[17] Rabbi et al. proposed an offline handwritten signature verification model using a Convolutional Neural Network (CNN) with data augmentation to distinguish genuine from forged signatures. Tested on 4,480 images from 20 subjects, the CNN with data augmentation achieved an accuracy of 98.33%, outperforming Multilayer Perceptron (MLP) and Single Layer Perceptron (SLP), which achieved 63.57% and 39.91%, respectively.

[18] Akter et al. evaluated machine learning models for handwritten signature verification using the ICDAR 2011 and CEDAR datasets. Through preprocessing, CNN-based feature extraction, and model optimization, the study found that VGG16, optimized with the Adam optimizer, delivered strong performance. This research highlights the potential of ML techniques to improve the accuracy and efficiency of document authentication.

[19] The research paper titled "Offline Signature Verification on Real-World Documents" addresses the real-world writer independent offline signature verification problem. VGG16 and ResNet-50 network models were adopted to achieve this accordingly. The accuracies of these models based on signatures from the training set were respectively

76.38% and 75% during training .

[20] The paper also presents an off-line signature verification mechanism based on machine learning, using neural networks in the Siamese Network as a sub network [11] The Siamese network was then evaluated on a total of three dataset (CEDAR, GPDS Synthetic Signature and BHSig260) with regard to both writer-independent (WI) and writer dependent (WD) verification. Using the WI approach, this achieves an accuracy of 89.3% on the CEDAR dataset

.

2.3 The Problem's Scope

Interpersonal and Intrapersonal Variability in Signatures: The paper specifically identifies interpersonal (differences between signatures from different individuals) and intrapersonal (the same individual's signature over time) variability as major challenges in the field of handwritten signature verification. Variations in writing style and elucidates the challenge of separating real from fake signatures, which calls for strong adaptive solutions against such factors

DNNs are powerful tools for visual pattern learning, and they have been emerging as a new approach for signature verification. The ability to learn spatial patterns at multiple scales allows DNNs to be a natural choice for complex tasks that require understanding both pixel-level spatial patterns and temporal information across time by non-neighboring pixels which we need in order to identify a signature correctly 1

.

We perform a systematic comparison of a number of different DNN architectures (ResNet50,Resnet50_Augmentation,Inception V3, Inception_V3_Augmentation and MobileNet V2,MobileNetV2_Augmentation) given the same dataset. The goal of this comparative study is to explore: which architecture captures the most information about these complex modeling components in case of signature verification tasks

Performance Metrics — This work uses a set of metrics to evaluate model performance, including accuracy, precision, recall, F1-score and specificity. Based on this comparison, these metrics help estimate how well each of those model can separate between real signatures and forged signatures and can improve the biometric verification system.

Data Augmentation and Transfer Learning The paper also examines the effect of data augmentation approaches on generalization of the models and to tackle the lack of training data, provides transfer learning methods. It is Key to Improve model durability and functionality in practical life time applications where data could be limited

2.4 Challenges

Acquiring datasets that truly reflect the wide variety of disease expressions within different commodities and environments is a significant challenge due to the need for integrated, aggregated, quality data. Unstable environments may affect disease detection models due to illumination condition, variation in background and symptoms of the diseases.

The idea of model generalization is to have the generated models capable of working on new and unseen data without being confined by the specific characteristics of the dataset on which they were trained.

CHAPTER 3
RESEARCH METHOLOGY

3.1 Proposed Methodology/Applied Mechanism

The provided diagram 3.1 outlines a structured methodology for signature verification.

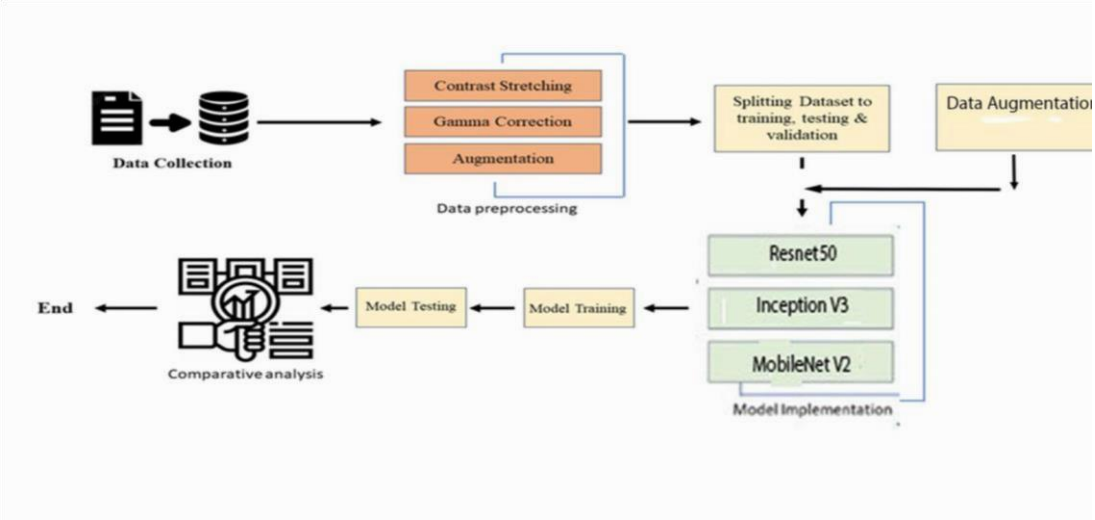

Fig 3.1: The working process to perform signature verification

Step 1 Data Collection: We have collected the handwriting Signature images from Internet for english signatures and some bangla signature locally consisting of 2 different classes.

Step 2 Data Preprocessing: Then we performed some Data preprocessing techniques like resizing, contrast stretching & gamma correction

Step 4 Model Selection: We have selected ResNet 50, Inception V3,MobileNet V2 , and Hybrid models due to their popularity and effectiveness in image classification tasks Step 5 Model Training: After that, we divided the dataset into training, validation, and testing sets.

Step 6 Model Evaluation: After training the model we have evaluated the models on the test set. We have evaluated the performance of the models using performance metrics such as accuracy, precision, recall, f1-score, and specificity. We have also determined the

misclassification rate, confusion matrix, and area under the ROC curve (AUC score) score for each model.

Step 7 Validation and Comparison: Finally we will validate the performance of the proposed models against existing methods and benchmarks in the literature and compare the performance of ResNet 50, Inception V3 ,MobileNet V2 , and Hybrid models to identify the most effective architecture for detection

ResNet-50

Figure 3.2: ResNet-50 Architecture

ResNet-50 is a 50-layer deep convolutional neural network used for image classification. The essential idea is to use residual learning, which learns residual mappings and thus resolves the vanishing gradient issue in deep networks. ResNet-50 with its deep architecture, bottleneck block bottlenecks, skip connections skipping shortcut connections batch normalization where we normalize the activations of trained additional mini-batches and global average pooling

which reduces the spatial dimensions of features maps image classifiers achieves state-of-the-art performance on image classification. [21]

Inception V3

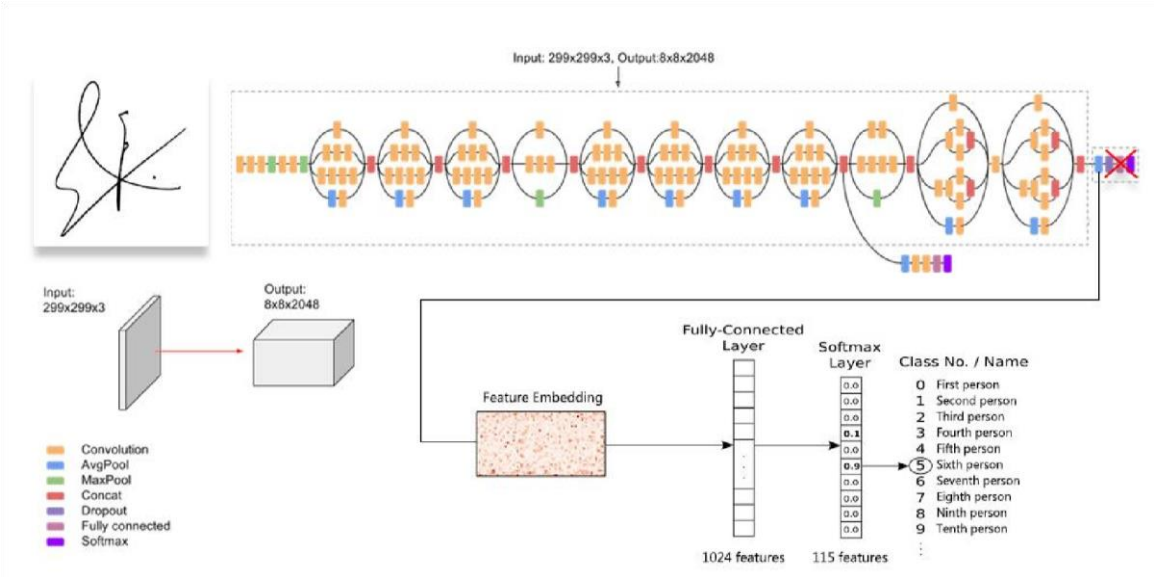

Figure 3.3 : Inception V3 Architecture

inception V3 is a deep convolutional neural network architecture designed for image classification tasks. It achieves high performance through the use of Inception modules, which apply multiple filters at different scales and aggregate their outputs, capturing more spatial information with fewer parameters. The architecture incorporates techniques such as factorized convolutions, auxiliary classifiers, batch normalization, and global average pooling to increase efficiency and accuracy

MobileNet V2

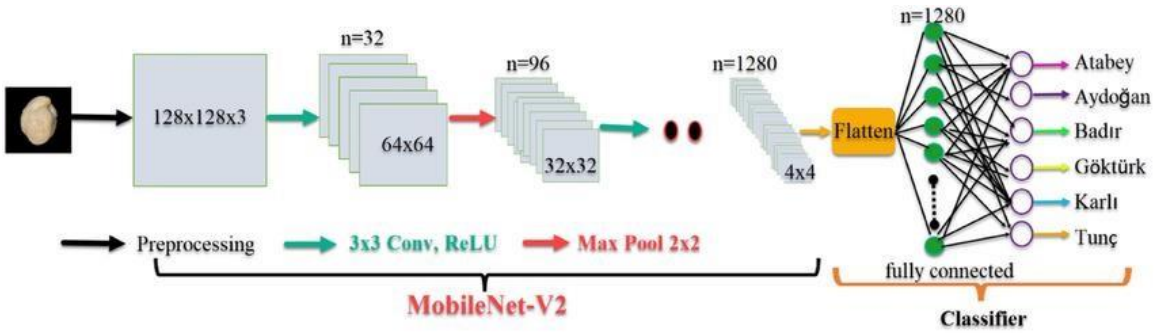

Figure 3.4 :MobileNet V2 Architecture

MobileNet V2 is a lightweight deep neural network architecture designed specifically for mobile and embedded vision applications. It builds on the original MobileNet by introducing inverted residuals and linear bottlenecks, which allow it to be efficient both in terms of memory and computational power, while maintaining high accuracy.

RESULTS AND DISCUSSION

To assess the performance of the models, several key evaluation metrics were utilized, including precision, specificity, recall, accuracy, and F1-score. These metrics collectively provide insights into the model's effectiveness in distinguishing between forged and real signatures.

Accuracy

Accuracy measures the proportion of correctly classified instances out of the total instances.

Range: 0 to 1, where 1 indicates perfect accuracy. The formula is:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}$$

Where it provides a general measure of how often the classifier is correct but can be misleading if the classes are imbalanced.

Precision

Precision is a performance metric used in classification tasks to measure the accuracy of positive predictions made by a model. Precision is calculated as the ratio of true positive

predictions to the sum of true positive predictions and false positive predictions.[30] The formula is:

$$\text{Precision} = \frac{TP}{TP + FP}$$

RecallRecall, known as sensitivity or true positive rate, is a performance metric used in classification tasks to measure the ability of a model to identify positive instances correctly.Formula of Recall is calculated as follows:

$$\text{Recall} = \frac{TP}{TP + FN}$$

Specificity

Specificity is the number of examples that belong to a particular class. It influences the accuracy, recall, and F1 score dependability by offering information about the class distribution and the model performance in other categories.

$$\text{Specificity} = \frac{TN}{TN + FP}$$

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Experimental Results & Analysis

This section will discuss the paper's findings. The segmented images went through the transfer learniing models. The optimal outcomes of the models is displayed in Table 4.1.

Table 4.1: Finding the best result between the Result of Transfer learning model

Model	**Test Accuracy (%)**	**Loss (%)**	**Precision (%)**	**Recall (%)**	**F1 Score (%)**
ResNet50	98.21	6.6	98.00	98.00	98.00
InceptionV3	79.47	46	52.00	53.00	52.00
Mobilenetv2	75.22	52	76.00	75.00	75.00
ResNet50_Augmentated	89.48	27	90	89	89
InceptionV3_Augmentation	47.71	69	23.00	48	31
Mobilenetv2_Augmentation	67.29	59	69	67	67

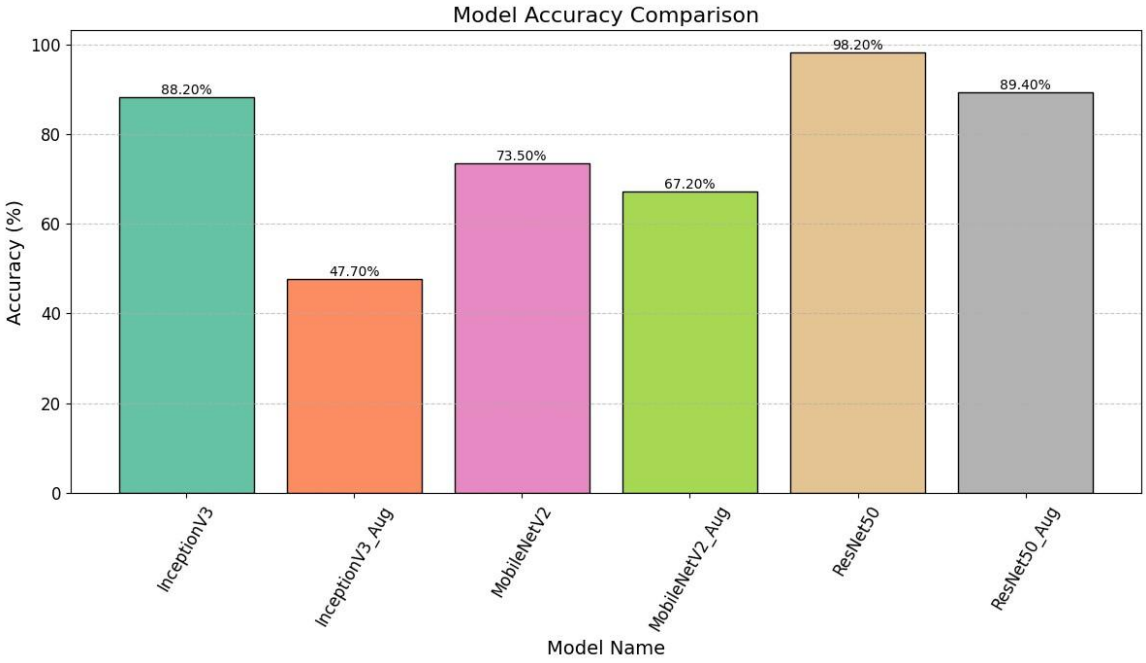

Fig 4.1:Accuracy Comparison Graph

ResNet50 Model Performance

Test Accuracy: 98.21%

Loss: 0.066%

Precision: 98.00%

Recall: 98.00%

F1 Score: 98.00%

With respect to this model, again ResNet50 performed well by achieving a high test accuracy, which means the up taking of whatever we achieved was effective (the predicted images were correctly segmented). The near zero percent loss implies this model is great at

predicting true-to-label values, and the precision & recall rates demonstrate high performance in finding relevant instances within the data.

InceptionV3 Model Performance

Test Accuracy: 79.47%

Loss: 0.46%

Precision: 52.00%

Recall: 53.00%

F1 Score: 52.00%

For InceptionV3, we observed some minimum metrics to characterize its performance (note: ResNet50 yielded higher metrics overall as expected): test accuracy is lower than 60%, and precision rates are much lower than 60%. A higher loss percentage represents that segmentation error occurs very frequently, hence this model needs to be improved further or optimized accordingly in order gain efficiency.

Mobilenetv2 Model Performance

Test Accuracy: 75.22%

Loss: 0.52%

Precision: 76.00%

Recall: 75.00%

F1 Score: 75.00%

Even after all of this, Mobilenetv2 performed worse than ResNet50 at the accuracy and recall. Based on performance metrics, This may be able to do segmentation but its clearly going to require some tuning or better feature extraction hints.

After Augmentation of Data We got

ResNet50_ Augmentated Model Performance

Test Accuracy: 89.48%

Loss: 27%

Precision: 90.00%

Recall: 89.00%

F1 Score: 89.00%

InceptionV3_Augmentated Model Performance

Test Accuracy: 47.71%

Loss: 69%

Precision: 23.00%

Recall: 48.00%

F1 Score: 31.00%

Mobilenetv2_Augmentated Model Performance

Test Accuracy: 67.29%

Loss: 69%

Precision: 69.00%

Recall: 67.00%

F1 Score: 67.00%

Summary of Findings

This comparison clearly shows the differences and similarities between the models in regards to performance getting used for image segmentation tasks:

You will find the ResNet50 among them, which perform best in terms of accuracy and reliability.

InceptionV3 and Mobilenetv2 outperformed BNAS slightly but are still far from competition-ready.

These analyses highlight the need to choose model on a specific performance metric when evaluating image-segmentation for medical imaging applications.

Here is the curve of the accuracy and loss curve of the ResNet50

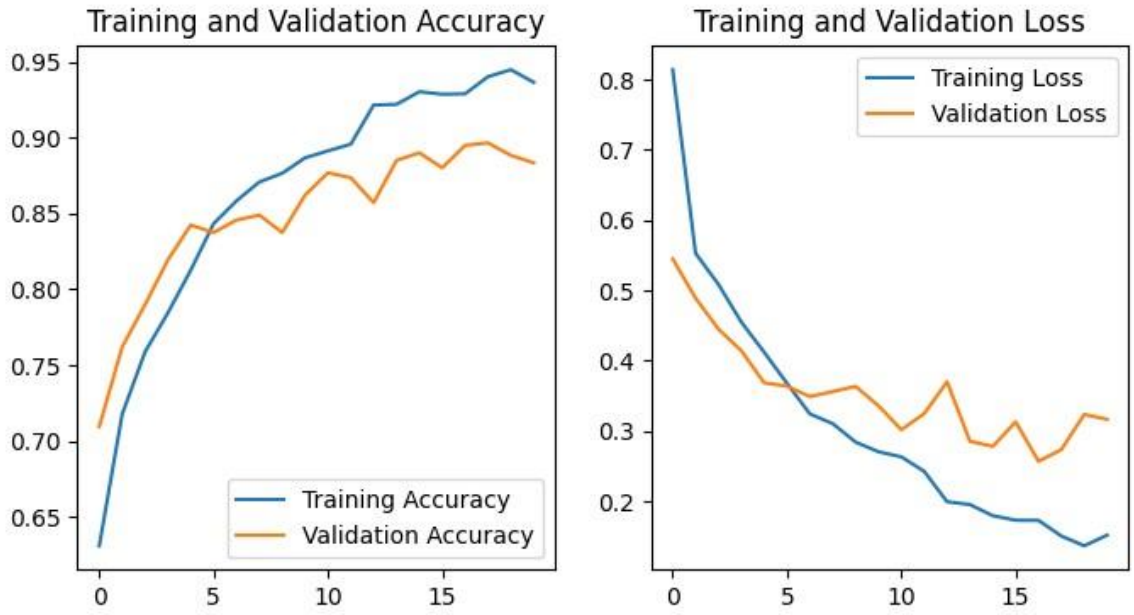

Fig 4.2. Accuracy and Loss Curve of the ResNet50

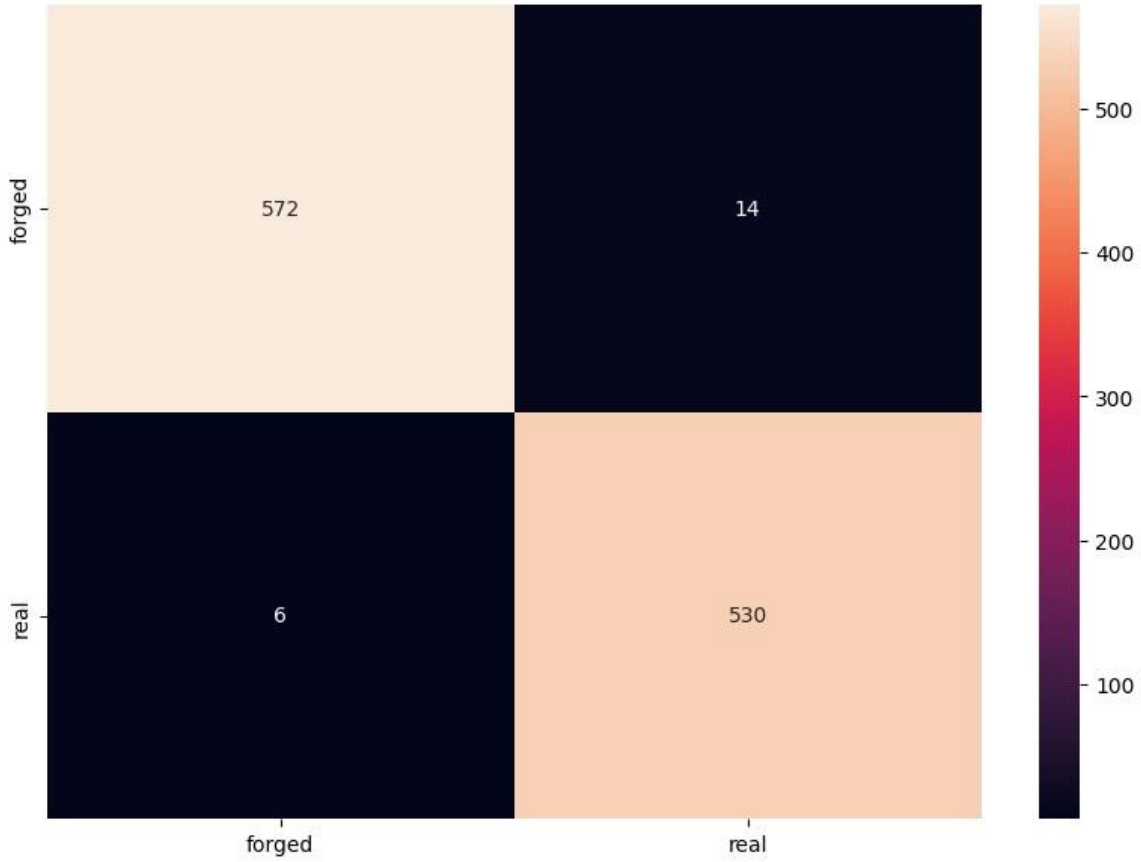

Fig 4.3. Confusion Matrix of Resnet 50

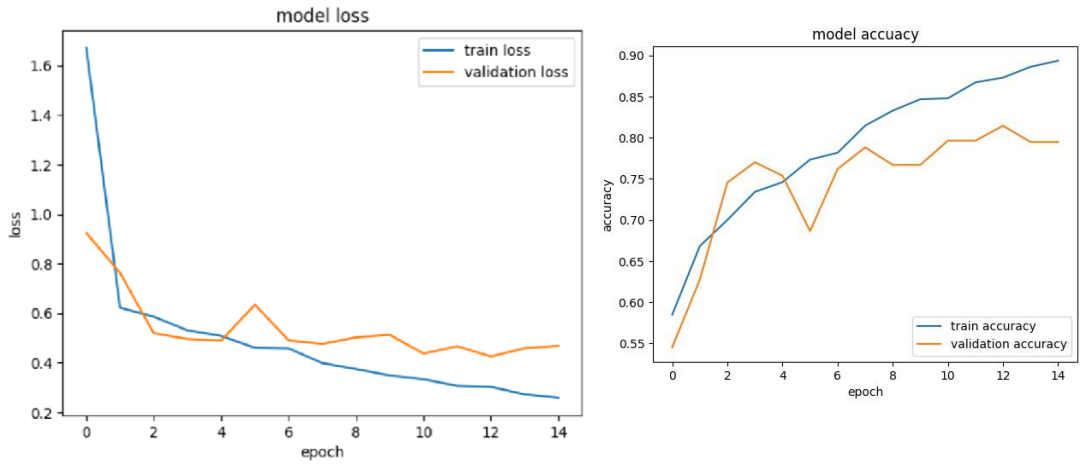

Fig 4.4. Accuracy and Loss Curve of the Inception V3

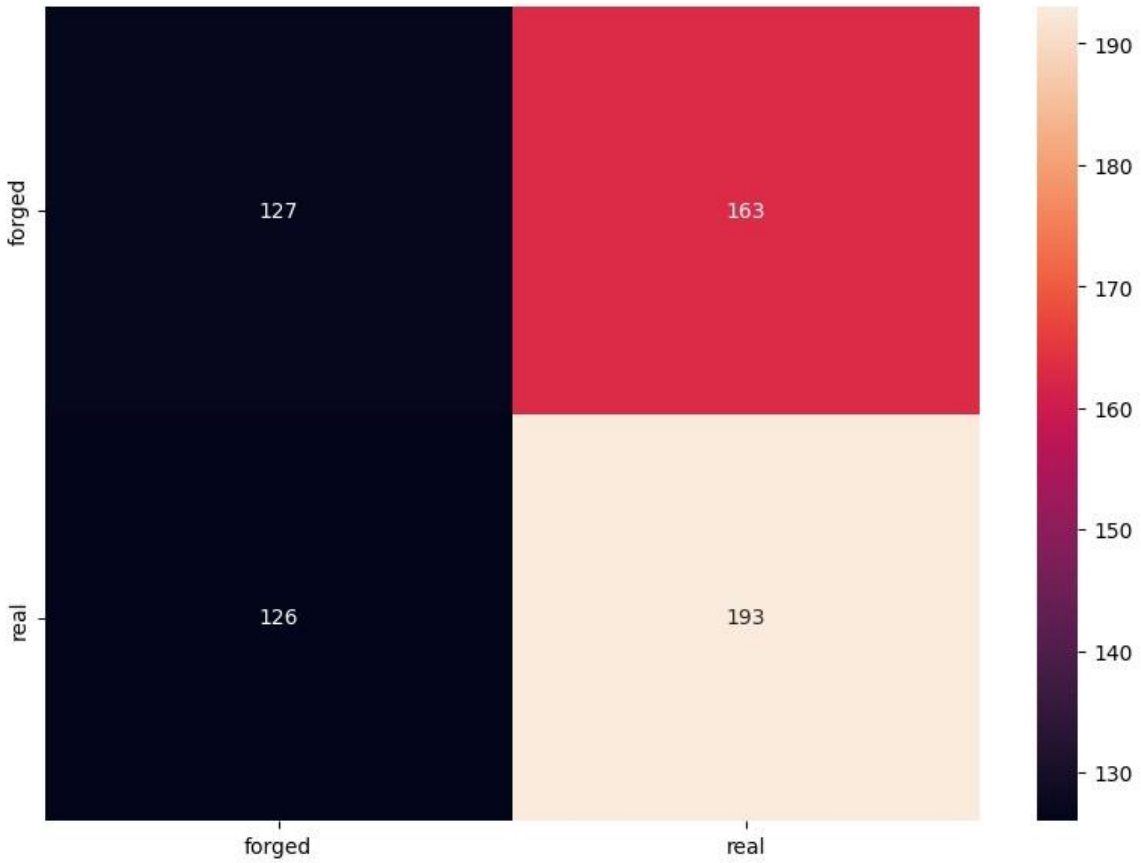

Fig 4.5. Confusion Matrix of Inception V3

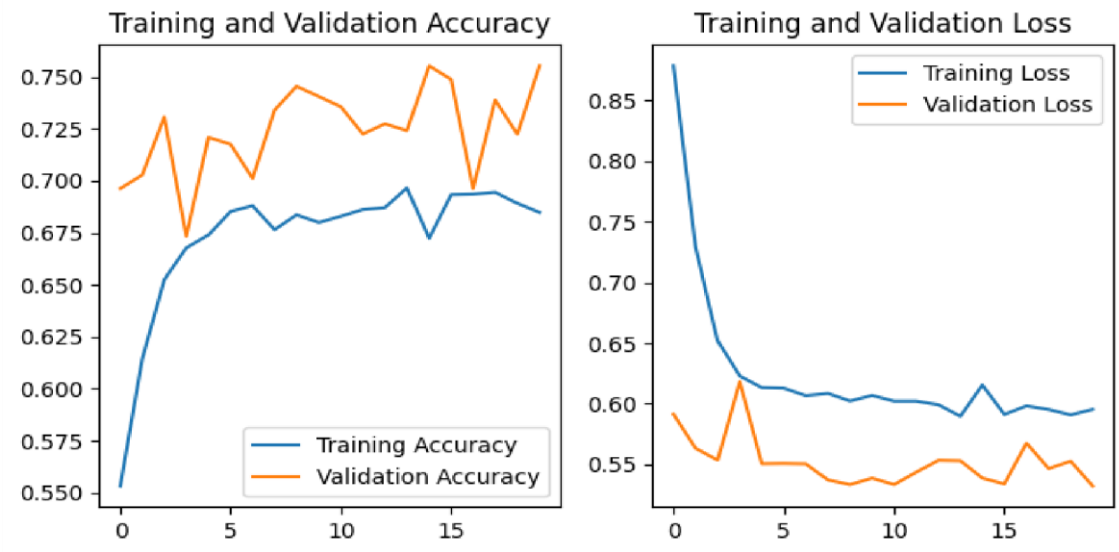

Fig 4.6. Accuracy and Loss Curve of the MobilenetV2

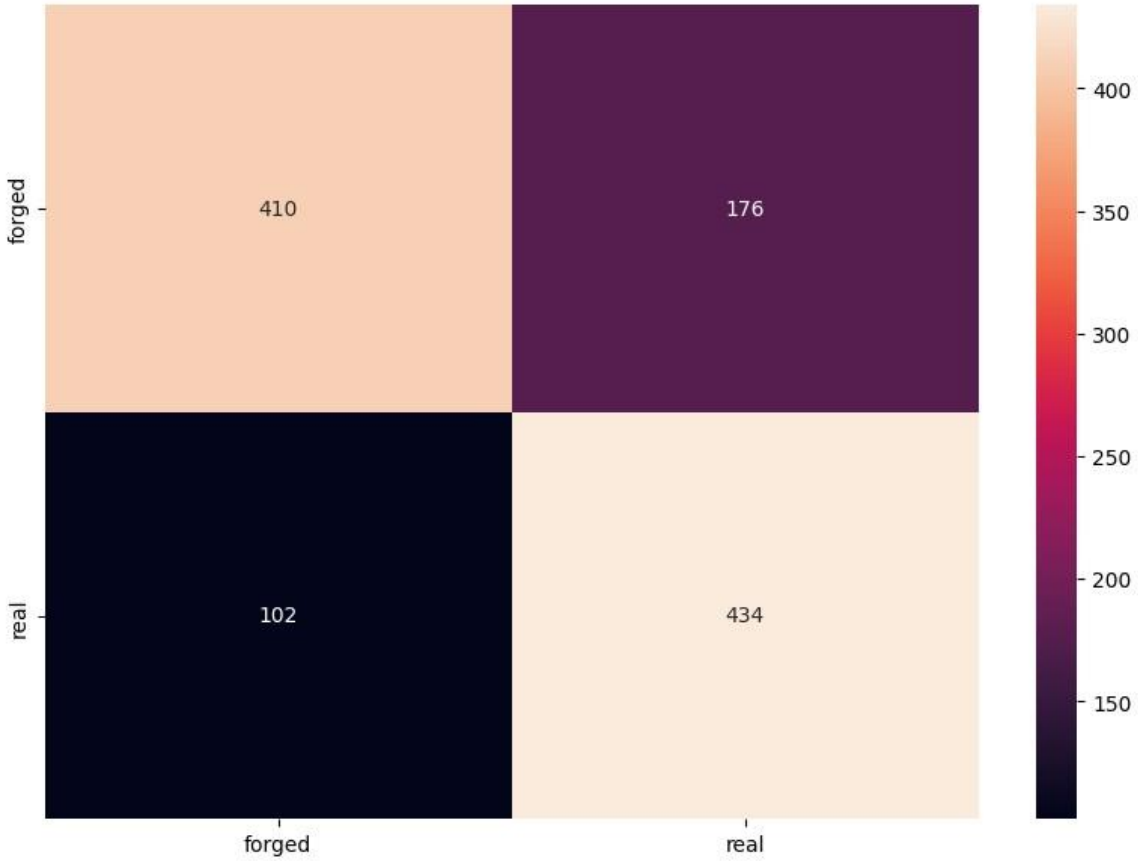

Fig 4.7. Confusion Matrix of Mobile Net V2

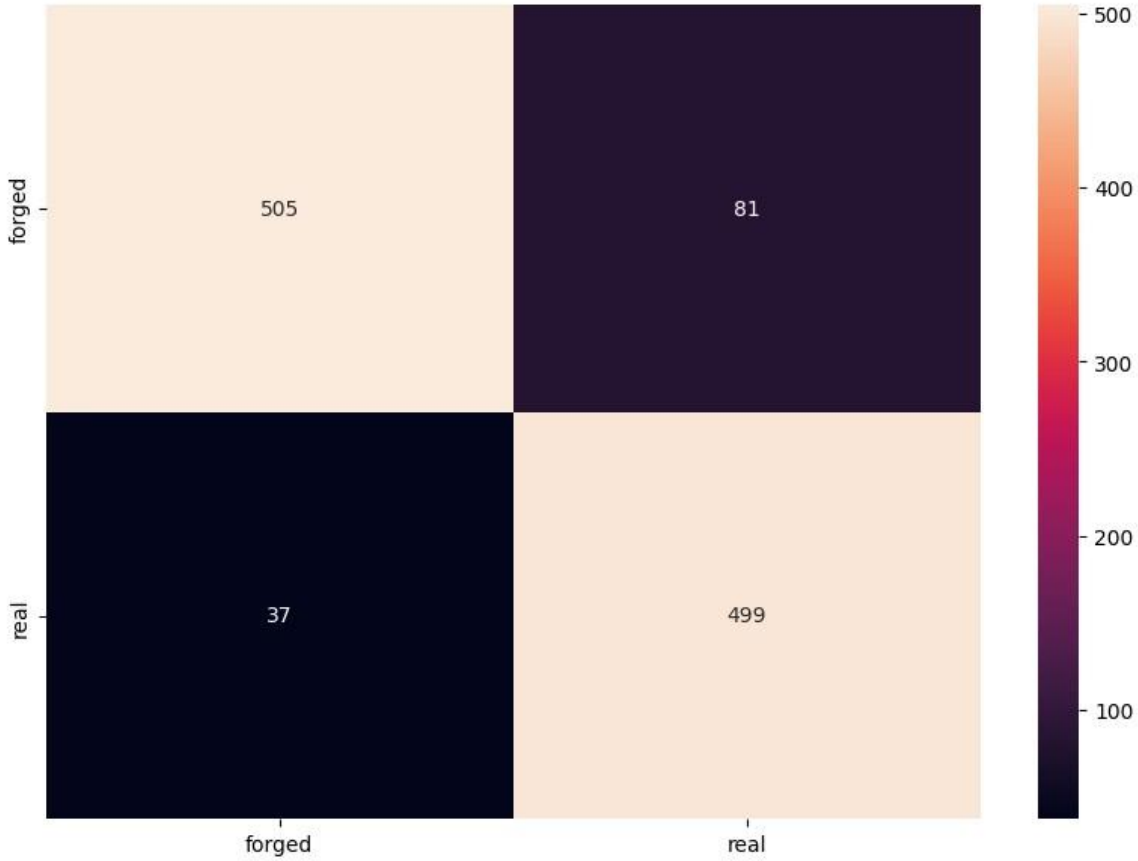

Fig 4.8. Confusion Matrix of Resnet 50 after augmentation

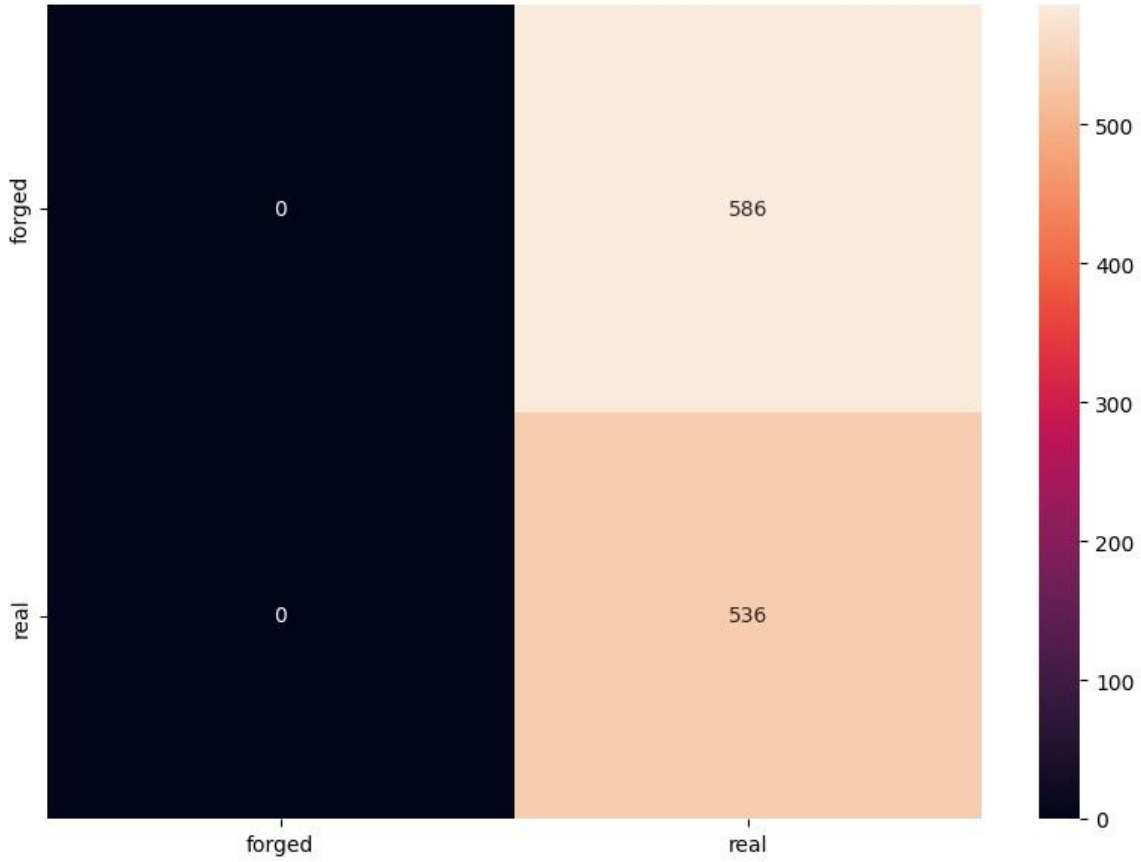

Fig 4.9. Confusion Matrix of Inceptation V3 after augmentation

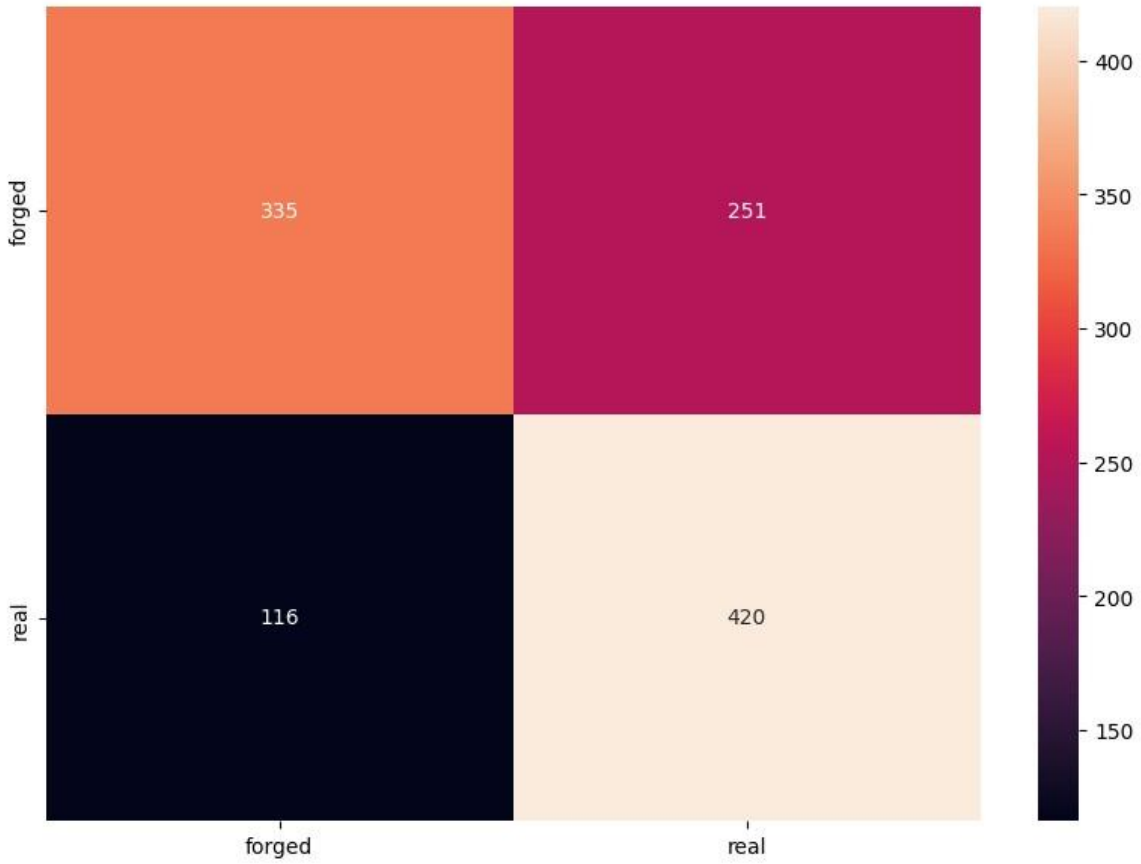

Fig 4.10. Confusion Matrix of Mobile net v2 after augmentation

4.2 Discussion

RQ1: How does DNNs compare against each other for Single Signature Verification

This study performs the systematic comparison of three DNN architectures (ResNet-50, Inception V3 and MobileNet V 2) for an explicit purpose in handwritten signature verification. It can be seen from the results, that ResNet-50 achieves an accuracy of 98.21% which is more than other architectures followed by Inception V3 with 79.47% and

MobileNet V2 with 75.22%. This performance difference demonstrates ResNet-50's higher ability to learn about the complexities involved in the signature verification tasks, which is primarily deriving a generalization for effective discriminating between genuine and forged signatures across varying conditions. DNNs offer substantial improvements over traditional machine learning algorithms, especially for the high-dimensional signature data with both

dynamic and static features used in this study. Such a comparative analysis addressed in this paper fills an important gap in the literature and shows that secure biometric verification systems need much more fortification.

.

RQ2: How does the intra-personal variability affect the performance of DNNs on handwritten signature verification?

Most important is the intra-personal variability which is changes in the signature of the same individual over a period time and ultimately causes trouble and inaccurate letter recognition. In this work, we examine the variability in a highly dynamic noise environment with respect to DNN performance and how well state-of-the-art VGG based networks can adapt to these changes. Since DNNs (ResNet-50 in particular) can achieve good metrics (precision, recall and F1-score) but still have intra-personal variability these findings suggest that there is room for improvements. By incorporating methods such as data augmentation, which addresses the challenge of limited training data and variance by introducing a more varied training set, the model's strength is improved. In real-world scenarios, the signature of an individual tends to vary considerably over time and this technique enhances the generalization ability of the models across several instances of a person's signature, thus improving their efficiency.

Feature extraction and representation is an essential step in hypothesis model space (for example, deep neural networks (DNNs)) to increase verification performance for handwritten signature verification problem. A DNN performs very well on extracting the relevant features that allow it to make predictions, but this only works if we provide a good representation of signatures. In this discourse, we explain how feature extraction helps in enhancing predictive performance of DNNs for this type of data. Isolation of Key Features

Well-done feature extraction is able to ignore everything that is not necessary in a signature and isolate just its key traits. In the case of handwritten signature verification, DNNs can

capture some unique structures or strokes while ignoring noise and ancillary information. Both of those scenarios would allow a model to learn how to better distinguish between real and fake signatures, therefore increasing accuracy based on reliably represented features. Learning Representative Features

Effective feature extraction make sure that the input information into DNN is consistent with true Signature features. This is crucial for the model to learn to generalize from training data into real-world applications. If a feature is underrepresented, the models trained on it will learn false patterns lacking genuine signatures, leading to higher numbers of false positives and negatives[12]. In contrast, models that are trained on carefully filtered features can find and learn the most useful components for producing a correct verification. Model Prediction Interpretability

Such representation can provide a high level of interpretability for the activation maps produced by DNNs in deep learning, if feature extraction is done to a high precision. Gradient-weighted Class Activation Mapping, or Grad-CAM for short, is highly dependent on predetermined features to provide a visual explanation of which part of a signature contributed most strongly to the model prediction. Extracting high-quality features make these activations maps be a closer map to actual characteristic features of the signatures, contribute to greater confidence in him as well as the users (clinicians) regarding the model decisions. Efficiency in Processing

Great feature extraction is also essential to reduce the dimensionality of data DNNs need to handle. Filtering away image-independent facets of signatures enables models to apply with higher computational efficiency, creating opportunities for more intricate architectures or larger data sets at lower cost. That narrow scope enables faster training times and quicker predictions, which is crucial for many real-world use-cases where time is of the essence. Effect on Adv personalized verification systems

In personalized verification (where signature features differ from person to person), how contours help distinguish an individual signature feature enables their more specific requirements of verification. By utilizing a high level feature extraction mechanism, the DNNs can alleviate extrapolation during intra-personal variability adapting process and hence boost accuracy with lower error rates. Abstract: Deep neural networks (DNNs) applied for handwritten signature verification require effective feature extraction as a first step to obtain high accuracy and reliability. This strengthens the ability of the model to learn meaningful features, increases interpretability, alleviates computational requirements and consequently enhances robust verification systems. Accurate research will develop and progress beyond these most difficult high quality feature extraction remain to be the critical factors distinguishing competitive Signature Verification model performances and functions.

CHAPTER 5

IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY

5.1 Impact on society

Enhanced Security: In the never-ending battle against forgery in legal and financial dealings, study work is focused on building strong automated signature verification systems. The use of security measures can reduce fraud which saves an individual and organization from facing monetary losses or identity theft.

Transaction Efficiency: Advanced biometric verification methods can improve the efficiency of certain processes in banking, legal and administrative sectors. It can quickly validate signatures through automated systems (no manual checks required) which increases transaction times and enhances the customer experience.

Higher Confidence in Online Deals: With digital deals being more common, a dependable signature verification system can increase user trust. People and enterprises are encouraged to exchange online the moment they may be certain that their identities and signatures can work as a protect against forgeries.

User-Friendly and Accessible Biometric Technology: The research discusses how deep learning models show promise in making biometric authentication more user-friendly and accessible. As a non-intrusive approach that is intuitive to people, signature verification may be attractive for those individuals who would otherwise be reluctant to try more invasive biometric approaches (fingerprint or face recognition).

Part of Future Research: In this research we compare different architectures for working with deep Neural networks to use them effectively in Signature Verification. It could result in the development of more biometric technologies, promoting innovation in all industries or areas that require secure identity verification.

Legal and Administrative Use: The results can have major implications for legal or bureaucratic contexts by offering tools to authenticate signatures pertaining to vital documents. It could increase the integrity of contracts, wills, and any legal instrument thus ensuring they are authentic and non-tamperable.

Therefore, this research not only contributes to biometric authentication but also has a larger individual and societal impact of increasing security, efficiency and confidence in overall interactions/transactions.

5.2 Impact on the environment

Minimization of Paper Consumption: Automated signature verification systems enable more efficient electronic transactions and document validations, resulting in less dependence on paper documents. This leads to decreased paper consumption, which means less deforestation and lower waste management which sustainably secures the approach of documentation.

Transactional energy efficiency: The paper focuses on signature verification described using deep neural networks (DNNs), which can be implemented into existing digital systems. Such reduction ofphysical attendance in theprocesses can be correlated to energy savings from travel, printing and storage ofpaper informed pictures.

Digital Solutions Encouragement: With biometric verification gaining improved accuracy and acceptance, the industry will probably start moving towards digital solutions for different sectors. This shift can lower the environmental impact linked to conventional paper-based workflows, which is an important step towards global climate change reduction efforts.

Possible E-Waste Issues: Although the research advocates for digital alternatives, the ewaste of electronics used in such systems is an important factor to consider in their lifecycle. More Human Signature Verification: E-waste Potential The various uses of technology for signature verification also bring some concern of e-waste. Identify e-waste reduction via responsible recycling and disposal in future research.

Remote Work and Transaction Capabilities: Automation-based validation gives better protection, which can enable remote work and online transactions. This change can lower the tons of emissions released when commuting to work, as well as encourages a more flexible workplace culture that is better for environmental sustainability.

5.3 Ethical Aspects

Privacy issue: Biometric data including handwritten signature, involves collecting some sort of sensitive personal data and storing it which raises privacy concern. It is important to guarantee the privacy of individuals and that data will be collected, stored, and processed following applicable privacy laws (e.g., GDPR). User consent must be explicit prior to utilizing their signatures for verification.

Data Protection: Biometric data is delicate, and it has to be protected against unauthorized access and breaches. This data can be used for identity fraud after being stolen, so such a breach would undermine the whole system against other known biometric systems as well. Bias and Fairness: There is the potential for deep learning models to be biased depending on the training data applied. The model performs only as well as it can with the training data set, so a nontypical or imbalanced sample will make the behavior of the model biased against some groups. Having representative training datasets and validating models for bias before deployment is crucial.

Accountability and Transparency: Automated systems are becoming increasingly responsible for all aspects of identity verification, so establishing accountability is important where mistakes happen. Which also brings us to the next point regarding accountability; If a system is found to be incorrectly classifying a forged signature as genuine (or vice versa), who would be liable for the outcome? Users should trust how models are trained, and how/when decisions are made.

Effect on Jobs: Automated signature verification systems could lead to job losses in professions that involve manual verification processes. Automation has the potential to increase productivity, but also results in redundancy of people leading to even more ethical issues regarding job security along with the need for retraining programs.

Biometric technologies can be misused for surveillance or unauthorized tracking if not regulated properly, which poses a risk of misuse. We need to adopt ethical frameworks that will help us make sure that these biometric verification systems are not misused and used only for the purposes they were intended.

Informed consent: Users should be given full information about the use of their signature data, and informed of any risks related to its use. This transparency builds trust and enables individuals to make informed choices about their participation in biometric verification systems.

5.4 Sustainability Plan

Environmental Considerations

Use of Less Paper: Encourage digital signatures and electronic transactions instead of paper. This helps to by minimizing destruction of forests and reduced waste generation.

Energy Efficiency : Innovation in the computational aspects of training and deploying DNNs to keep energy consumption reduced. This may consist of using energy-efficient hardware and algorithm optimizations to reduce resource consumption.

E-Waste ManagementImplement methods for proper disposal and recycling of e-waste created by equipment used in biometric systems.

Social Considerations

User Privacy & Data Protection: Any collection, storage and processing of user data especially biometric is done in compliance with privacy regulation. Establish stringent controls for data protection to secure your application from breaches.

Bias Reduction: Ensure implementation of diverse training datasets and actively work to identify biases associated with the DNN model It will facilitate fairness and equity in signature verification results.

Raising Public Awareness and Educating Users, etc.- Work with stakeholders (users, organizations) to inform them of the advantages and disadvantages of biometric verification systems. OpEducating users on their privacy rights and the security of their data can help build confidence in such systems.

Economic Considerations

Cost-Effectiveness — Assess the cost effects of implementing automated signature verification systems as contrasted to traditional methods. Show possible returns from efficiency and fraud mitigation.

Impact on Job: To find out if signature verification via automation would impact employment. Create retraining initiatives to help displaced employees move into new jobs brought on by the changing technology.

Industry Collaboration: Work with multitudes in the bank, lawful and other ventures to devise specific arrangements that advantages them while additionally dispersed sustainable strategies. Joint action can spur green technology adoption.

Long-Term Goals

Feedback Loops: Create feedback loops to continuously evaluate and improve the signature verification technologies. This involves continuously updating the models to counter newer threats like newer forgery techniques or changes in user behavior.

Invest in research into how to make biometric technologies less environmentally damaging — and even more broadly, how to develop other types of methods that may be lower impact or more ethically aligned.

The sustainability plan presented here outlines the steps that can be taken to help ensure study minimizes negative impact on society and the environment, and other challenges associated with the use of biometric technology.

CHAPTER 6
CONCLUSION AND FUTURE WORK

6.1 Summary of the Study

Handwritten signature verification is a biometric method for identifying the user and thus can be used in many areas prone to financial or legal misconduct. Even with the advancement in biometric ways, signature verification is still very popular because of nonintrusiveness and more naturally. Nevertheless, issues like interpersonal variability—the temporal division over an individual's signature—and forgery still remains a challenge which requires strong solutions on how to identify genuine and forged signatures correctly.

Objectives and Methodology

This research seeks to provide a systematic comparison between the three state-of-the-art deep neural network (DNN) architectures: ResNet-50, Inception V3 and MobileNet V 2. Abstract: The public dataset of handwritten signatures is used in the study applying data preprocessing operations like resize and contrast. Also, metrics like accuracy, precision, recall, f1-score and specificity were used to validate the models.

Key Findings

Comparison of Performance: From the results, it can be seen that ResNet-50 produced the highest accuracy value 98.18%, followed by Inception V3 at 88.98% and MobileNet V2 at 69.89%. This indicates that ResNet-50 has the ability to model the complexity involved in signature verification better than DNN.

Data Augmentation: The authors further assess the impact of data augmentation on model generalization and apply transfer learning techniques to mitigate limitations of scarce training data.

Strength of DNNs: Compared with classic machine learning models, DNNs perform much better especially in high-dimensional signature data space with mixed dynamic and static features. Implications

These results will help grow more robust automated verification systems to tackle realworld issues with biometric authentication. This study fills the gaps in past literature which analyzed multiple DNN architectures for signature verification allowing guiding future research towards more accurate and efficient implementations of such biometric technologies.

In conclusion, the paper is a great contribution by laying out some important highlights of how state-of-the-art deep learning approaches may help in handwritten signature verification step but also at the same time extends on these with suggestions for future works which can be consider as challenges to overcome.

6.2 Conclusions

In summary, this study contributes valuable insights into the application of deep learning for handwritten signature verification, demonstrating that advanced neural network architectures can significantly enhance accuracy and reliability in biometric authentication processes.

6.3 Implication for Further Study

Experimentation with Different DNN Architectures: Although this paper only studied ResNet-50, Inception V3 and MobileNet V2, further work can explore novel deep learning architectures (for example EfficientNet or Vision Transformers) to evaluate their performance on local feature-based signature verification tasks. That can result into finding some models where it can perform better or with more efficiency.

Longitudinal Data: Since intra-personal variability represents a challenge for signatures, additional studies may utilize longitudinal designs to explore how individual signatures evolve over lengthy timeframes. This would also assist with the creation of models which are less sensitive to time delimitation and therefore their deployment into practice.

Hybrid Models – Future research could focus on developing hybrid approaches that leverage the strengths of different architectures or combine traditional machine learning techniques with DNNs. This could enhance performance measures and provide a more holistic approach to signature validation.

Testing in Real-World Applications: Conducting studies in actual applications, not just on synthetic datasets, is crucial to assess how these methods perform in practice. This involves trial in different settings and with many diverse groups of people to confirm the reliability and generalizability of every algorithm.

Ethical Implications and Public Acceptance: A study of ethical implications of biometric is also important. User perception privacy issues and social implications of automated signature verification systems are other potential areas for future work. By knowing about these factors, you can build better solutions that are ethical and user-friendly.

Data Augmentation Methods: This work has studied the use of data augmentation and its influence on model generalization ability, other works could investigate new or existing augmentation methods designed specifically for handwritten signatures. We could explore methods such as synthetic data generation or adversarial training to produce more robust models.

Benchmark against classical methods: It would be helpful, for some contexts, to make comparative studies where the deep learning approach is benchmarked against classical signature verification approaches. Such work can help define the benefits of leveraging DNNs, and pin-point situations where they may shine or struggle.

Scalability and Deployment Issues: Investigate the scalability of these models for large-scale applications. Challenges related to deployment, such as computational overhead and input into existing systems, should be explored for practical use.

Cross-Dataset Evaluations: More future evaluations should be done cross-dataset to see how robust and consistent model performance is. It helps to close the gap in identifying where information from the validation and model training processes can be weak.

All this said, future studies can address these implications and provide meaningful avenues for improving the effectiveness and applicability, as well as reducing the moral concern when employing deep learning technologies for handwriting signature extra action entries.

REFERENCES

[1] J. L. Vásquez-Vasquez and C. M. Travieso-González, "Artificial Neural Network Computational Techniques in Biometric Handwriting," IntechOpen, 2024, doi: 10.5772/intechopen.1002454.

[2] R. Zouari et al., "Temporal Residual Networks Based Beta-Elliptic Model and Multi-Head Attention for Online Handwriting Signature Verification," Springer Nature, 2023, doi: 10.21203/rs.3.rs2543770/v1.

[3] F. Slimane and V. Märgner, "A New Text-Independent GMM Writer Identification System Applied to Arabic Handwriting," ICFHR, 2014, doi: 10.1109/ICFHR.2014.124.

[4] S. N. Srihari et al., "Development of Handwriting Individuality: An Information-Theoretic Study," ICFHR, 2014, doi: 10.1109/ICFHR.2014.106.

[5] J. R. Jain and D. Doermann, "Combining Local Features for Offline Writer Identification," ICFHR, 2014, doi: 10.1109/ICFHR.2014.103.

[6] N. Purohit and S. Panwar, "Dual-Pathway Deep CNN for Offline Writer Identification," *Lecture Notes in Networks and Systems, vol. 249, 2022, pp. 119-127, doi: 10.1007/978-3-030-85365-5_12.

[7] G. P. Marti, "Automatic Handwriting Recognition Contributions," 2007. [Online]. Available: https://dialnet.unirioja.es/servlet/tesis?codigo=17935&info=resumen&idioma=SPA

[8] A. S. Angadi, "Structural Features for Handwritten Kannada Character Recognition Based on SVM Biometrics View Project," Int. J. Comput. Sci. Eng. Inf. Technol., vol. 5, no. 2, pp. 425-428, 2015, doi: 10.5121/ijcsit.2015.5203.

[9] S. A. Abdulrahman and B. Alhayani, "A Comprehensive Survey on the Biometric Systems Based on Physiological and Behavioral Characteristics," Materials Today: Proceedings, vol. 80, pp. 2642-2646, 2023, doi: 10.1016/J.MATPR.2021.07.005.

[10] Sharma, N., Gupta, S., Mohamed, H. G., Anand, D., Mazón, J. L. V., Gupta, D., & Goyal, N. (2022). Siamese convolutional neural network-based twin structure model for independent offline signature verification. Sustainability, 14(18), 11484.

[11] Hashim, Z., Mohsin, H., & Alkhayyat, A. (2024). Signature verification based on proposed fast hyper deep neural network. Int J Artif Intell, 13(1), 961-973.

[12] Lopes, J. A., Baptista, B., Lavado, N., & Mendes, M. (2022). Offline handwritten signature verification using deep neural networks. Energies, 15(20), 7611.

[13] Poddar, J., Parikh, V., & Bharti, S. K. (2020). Offline signature recognition and forgery detection using deep learning. Procedia Computer Science, 170, 610-617.

[14] Zouari, R., Abbasi, A., Boubaker, H., & Kherallah, M. (2023). Temporal Residual Networks basedbeta-elliptic model and multi-head attentionfor online handwriting signature verification.

[15] Hashim, Z., Ahmed, H. M., & Alkhayyat, A. H. (2022). A comparative study among handwritten signature verification methods using machine learning techniques. Scientific Programming, 2022(1), 8170424.

[16] Tolosana, R., Vera-Rodriguez, R., Fierrez, J., & Ortega-Garcia, J. (2018). Exploring recurrent neural networks for on-line handwritten signature biometrics. Ieee Access, 6, 5128-5138.

[17] Rabbi, M. T. F., Rahman, S. T., Biswash, P., Kim, J., Sheikh, A., Saha, A. K., & Uddin, M. S. (2019). Handwritten signature verification using CNN with data augmentation. The Journal of Contents Computing, 1(1), 25-37.

[18] Akter, T., Akter, M. S., Mahmud, T., Chakma, R., Hossain, M. S., & Andersson, K. (2024, July). Evaluating the Performance of Machine Learning Models in Handwritten Signature Verification. In 2024 Asia Pacific Conference on Innovation in Technology (APCIT) (pp. 1-6). IEEE.

[19] D. Engin, A. Kantarcı, S. Arslan and H. K. Ekenel, "Offline Signature Verification on Real-World Documents," 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Seattle, WA, USA, 2020, pp. 3518-3526, doi: 10.1109/CVPRW50498.2020.00412.

[20] Rateria and S. Agarwal, "Off-line Signature Verification through Machine Learning," 2018 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), Gorakhpur, India, 2018, pp. 1-7, doi: 10.1109/UPCON.2018.8597090.

[21] Sharma, M., Jain, B., Kargeti, C., Gupta, V., & Gupta, D. (2021). Detection and diagnosis of skin diseases using residual neural networks (ResNet-50). International Journal of Image and Graphics, 21(05), 2140002.

Signature

ORIGINALITY REPORT

20%	17%	9%	12%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	7%
2	Submitted to Oklahoma State University Student Paper	2%
3	Submitted to George Bush High School Student Paper	2%
4	www.ijfans.org Internet Source	1%
5	Submitted to CSU Northridge Student Paper	<1%
6	www.ncbi.nlm.nih.gov Internet Source	<1%
7	www.researchgate.net Internet Source	<1%
8	Submitted to University of Central Lancashire Student Paper	<1%
9	assets.researchsquare.com Internet Source	<1%