IJMSIT

International Journal of Multidisciplinary Studies and Innovative Technologies

e-ISSN: 2602-4888
dergipark.org.tr/en/pub/ijmsit
Research Article

2025, 9 (1), 74-82
DOI: 10.36287/ijmsit.9.1.11
Received: June 11, 2025; Accepted: June 27, 2025

Performance Evaluation of Transfer Learning Techniques and Machine Learning Methods in Signature Verification

Yasin Ozkan[1*],

[1*] *Department of Computer Technologies, Zonguldak Bulent Ecevit University, Zonguldak, Turkey (yasin.ozkan@beun.edu.tr) (ORCID: 0000-0002-2029-0856)*

Abstract –Signature verification plays an important role in biometric security systems and traditional methods can lead to limitations in verification accuracy. However, traditional signature verification techniques work with limited data and features, which can negatively affect the accuracy of verification processes. In this study, we investigate the performance improvement in signature verification by combining transfer learning and machine learning algorithms. In the experiments performed on signatures from the BHSig260 Hindi dataset, the transfer learning models (ResNet50, MobileNetV2, VGG16, InceptionV3, EfficientB7, DenseNet169) achieved high accuracy rates on their own, especially the VGG16 model performed the best with 93.77% accuracy. In the later stages of the study, machine learning algorithms such as K-nearest neighbor (KNN), Support Vector Machines (SVM) and Random Forest were added to the transfer learning models to further improve the validation performance. The combination of EfficientB7 + Random Forest achieved the highest performance with 95.24% accuracy. The results show that the integration of transfer learning techniques with machine learning algorithms significantly improves the accuracy of signature verification tasks. This combination stands out as an effective method that significantly improves the reliability and efficiency of biometric security systems. The findings of the study will provide an important reference for the future development of signature verification systems, contributing to the development of more accurate and reliable solutions in this field.

Keywords *–Signature verification, Machine learning, Transfer Learning,CNN, Biometric Security, Hindi Signature Dataset*

Citation: Ozkan, Y. (2025). Performance Evaluation of Transfer Learning Techniques and Machine Learning Methods in Signature Verification. International Journal of Multidisciplinary Studies and Innovative Technologies, 9(1): 74-82.

I. Introduction

Signature verification fulfills an important function as one of the key components of authentication and security in both digital and physical environments. In particular, digital signature verification plays a critical role in enabling secure and fraud-proof communication and transactions in the electronic environment. While traditional signatures are known to be used to verify a person's identity and approve transactions performed with his/her permission, digital signatures are technologies that fulfill this function in an internet-based environment [1]. Digital signature systems not only provide authentication, but also protect the integrity, security and confidentiality of data [2].

The legal validity of digital signatures is directly related to the security of signature verification systems. In many countries, digital signatures and verification systems have been established in a legal framework for secure electronic transactions. The effectiveness of electronic signature verification algorithms is critical in ensuring the security of data in areas such as financial transactions, e-commerce and government services. In this context, signature verification systems not only ensure secure communication, but also guarantee the legal binding and validity of transactions [3] . Digital signature verification is an indispensable tool not only for security but also for ensuring the legal and commercial validity of transactions. Therefore, the security of digital signature verification technologies remains important in the face of ever-evolving cyber threats and research in this field continues [4].

The security of digital signature verification systems is continuously improving with advancing technologies. Traditional signature verification methods usually use template-based approaches and algorithms. However, these methods may be insufficient to deal with challenging situations such as forged signature detection. In recent years, the integration of artificial intelligence techniques such as machine learning and deep learning has made significant progress in the field of digital signature verification. These techniques make the signature verification process more secure and accurate, while at the same time providing a more flexible solution against next-generation forgery attempts. Machine learning algorithms, especially by training using labeled data, increase accuracy rates in the verification process and improve the ability to detect forged signatures [5].

Deep learning is being integrated into digital signature verification, especially with structures such as Convolutional Neural Networks (CNNs). CNNs are networks that are generally used in the processing of visual data and can achieve high accuracy rates thanks to their multilayer structure. CNNs play an important role in improving the accuracy of digital signatures because they can perform in-depth analysis on the shape and dynamic properties of the signature. The geometric properties of the signature, time-varying features such as speed and compression strength can be learned by CNNs to determine whether the signature is authentic or not [6]. In this context, deep learning algorithms overcome the limitations of traditional methods and enable the development of more flexible and powerful verification systems. Moreover, these algorithms minimize forgery risks by ensuring that the signature is analyzed correctly.

Signature verification is a widely used biometric method to securely verify the identity of individuals in a digital environment. It plays an important role especially in security areas such as personal data protection and fraud prevention. Using signature as a biometric feature can provide high levels of security in verification processes by taking into account the variability and uniqueness of individuals' signatures over time. In the literature, various algorithms and technologies have been developed for signature verification, and this field has made significant progress in recent years with innovative methods such as deep learning and machine learning.

In [7], we focus on dynamic (online) verification methods instead of static (offline) signature verification to improve the efficiency of online biometric personal verification systems. The study aims to improve the signature verification process by using a CNN model built in Python for online signature verification. After training and validation, an accuracy rate of 99.70% was achieved on test data.

In [8], 24 original and 30 forged signatures of 1000 users were classified using GPDS Synthetic Signature Database for handwritten signature verification. In the experiments with Inception-v1 and Inception-v3 CNN architectures, Inception-v1 performed better with 83% accuracy. The Equal Error Rate (EER) was 17 for Inception-v1 and 24 for Inception-v3. Inception-v1 outperformed Inception-v3 with faster training time and lower number of operations.

In [9], a model is proposed using VGG-19 pre-trained CNN to automate the signature verification process. The model is tested on common datasets such as ICDAR, CEDAR, and Kaggle and achieves 100%, 88%, and 94.44% accuracy rates, respectively. The analysis shows that the proposed model can correctly classify forged signatures, but it may have difficulty with samples that are very similar to the original signature.

In [10], a new model for offline signature verification is proposed that can better capture signature features and reduce the complexity of the network. In this model, CNN and Capsule Neural Network (CapsNet) are combined to better understand the spatial features of signature features and improve the feature extraction process. Furthermore, a new training mechanism is developed in which two images at the same level are trained simultaneously with a single network. This hybrid model, called CBCapsNet, outperforms existing signature verification methods by increasing accuracy rates.

In [11], the importance of the feature extraction phase of online signature verification systems is emphasized. In this study, CNN and Histogram of Oriented Gradients (HOG) are used for feature extraction from signature images and key features are identified with decision trees. Finally, CNN and HOG methods are combined and the effectiveness of the model is evaluated with long-short-term memory (LSTM), support vector machines (SVM) and K-nearest neighbor (K-NN) classifiers. The experimental results showed that the model was successful with 95.4%, 95.2% and 92.7% accuracy rates for the UTSig dataset and 93.7%, 94.1% and 91.3% accuracy rates for the CEDAR dataset, respectively.

In [12], a Recurrent Neural Network (RNN) based method is proposed for online signature verification. This method is analyzed with LSTM and bidirectional LSTM (BLSTM) models by extracting structural and directional features from different people's signatures. The proposed model is tested on GPDS synthetic (93.24%), GPDS-300 (94.18%), MCYT-75 (94.42%), CEDAR (95.31%), BHSig260 Hindi (95.12%) and BHSig260 Bengali (95.19%) datasets. Experimental results show that the proposed RNN-based system achieves high accuracy rates and outperforms existing CNN-based methods.

In [13], a deep learning based method is proposed for handwritten signature verification. Inception V3 transfer learning model is developed to distinguish between forged and genuine signatures and fine-tuned by adding Flatten, Dense, Dropout layers. The model achieved the highest performance with 88% accuracy compared to pre-trained models such as VGG 16, ResNet and MobileNet. This work contributes to the development of more effective CNN-based models for online signature verification.

In [14], CNN is used for feature extraction and SVM for verification for online signature verification. CNN is trained to extract features from signature data and these features are evaluated using SVM to classify them as forged or genuine signatures. The model was tested on the GPDS signature dataset. The dataset contains signatures of 960 users, each containing 24 real signatures and 30 forged signatures. The CNN was trained with 300 users and the signatures of 400 users were used for feature learning. These 400×20×25 signatures were applied to the SVM classifier for 90% training and 10% testing.

In [15], an application of DAG-CNN is presented to classify and verify the accuracy of online signatures of 3 users. For the study, two datasets were created, including the signatures of 3 users and forged signatures of 115 other users that were modified by these users. After the network was trained, validation and testing phases were performed and accuracy rates of 99.4% and 99.3% were obtained respectively. The results confirm the features learned by the network and the usability of this neural network in online signature verification and identification applications.

In [16], CNN architectures such as AlexNet, GoogleNet, ResNet, MobileNet and DenseNet are investigated and compared for signature verification. In the study, a fine-tuned transfer learning approach is used for verification and identification of offline signature images. Experiments on the UTSig dataset show that the DenseNet architecture performs better than other CNN architectures. The proposed model achieved 98.87% accuracy with the fine-tuned approach.

In [17], a Cycle-GAN based data augmentation method is proposed for offline handwritten signature verification. To overcome the lack of data, the proposed method is tested on four different CNN architectures, VGG16, VGG19, ResNet50 and DenseNet121. The results show that the proposed data augmentation method achieves significant success for all CNN architectures, and especially shows the best effect on DenseNet121. According to the results, in the validation tests with the data augmentation method, the highest accuracy is achieved on the MCYT dataset and the second best accuracy is achieved on the GPDS dataset. The verification accuracy obtained with the proposed method was 96.9% for VGG16, 96.9% for VGG19, 97.0% for DenseNet121 and 96.5% for ResNet50.

In [18], a CNN model is used to verify the accuracy of handwritten signatures. In tests on a dataset of signatures from 16 volunteers, the model achieved 91.35% accuracy. With five-fold cross-validation, the accuracy increased to 98%, while adversarial attacks reduced the accuracy of the model to 80%.

In [19], a CNN-based automatic feature extraction and learning method for signature verification is proposed. The method consists of three steps: preprocessing, feature extraction and classification. The system was tested on the CEDAR dataset and achieved 89.2% accuracy.

In [20], CNN followed by Recurrent Neural Network (RNN) is used to detect forged signatures in the signature verification process. The study was tested with SVC 2004 and SigComp2009 online datasets and achieved 97.05% accuracy.

In [21], the importance of signature verification is emphasized in areas where handwritten signatures are still used instead of digital signatures. This study aims to identify real signatures using deep learning technique. CNN based deep learning model is used for image processing, classification and segmentation. VGG16, Inception v3 and CNN models with three to four convolution layers were trained for this verification. A dataset was created by collecting 50 signatures from 10 different users, out of 500 signatures, 400 were used for training and 100 for testing. In two different cases, the Inception v3 model achieved 95% accuracy with preprocessed images, but only 88% accuracy with unprocessed images.

In this study, signature verification was performed on Hindi signatures in the BHSig260 dataset using ResNet50, MobileNetV2, VGG16, InceptionV3, EfficientB7 and DenseNet169 transfer learning models. In the first stage, the validation performance of these models was evaluated. In the second stage, the K-nearest neighbor (KNN) algorithm was added to each transfer learning model to examine their performance. In the third stage, Support Vector Machines (SVM) were integrated and in the last stage, Random Forest algorithm was used to improve the validation performance. As a result of these four steps, the effects of integrating transfer learning models with machine learning algorithms on signature verification performances are evaluated.

These studies provide valuable contributions to the field to improve the efficiency and accuracy of signature verification processes. In particular, the integration of machine learning and deep learning methods makes signature verification systems more reliable and faster. Moreover, these innovative approaches provide important opportunities for systems to work more effectively in real-world situations.

II. MATERIALS AND METHOD

Signature verification has made significant progress thanks to the integration of artificial intelligence (AI) and machine learning, especially deep learning. While traditional signature verification methods often rely on manually extracted features, deep learning techniques make this process more automated and accurate. Artificial intelligence has the potential to minimize human error in verification processes by learning signature patterns from large data sets. Deep learning, especially through architectures such as CNN, can learn the geometric and dynamic properties of signatures with high accuracy. Machine learning, on the other hand, effectively utilizes these features learned from signature data in classification and verification processes. This makes signature verification systems more flexible, faster and more reliable, while increasing the ability to detect forgery. In particular, the use of transfer learning techniques enables high performance with limited data and enables systems to operate more efficiently.

In this section, we propose an innovative approach to improve signature verification performance. The dataset used, the transfer learning architectures implemented and the machine learning techniques integrated are discussed in detail. The flowchart of the proposed methodology is presented in Figure 1.

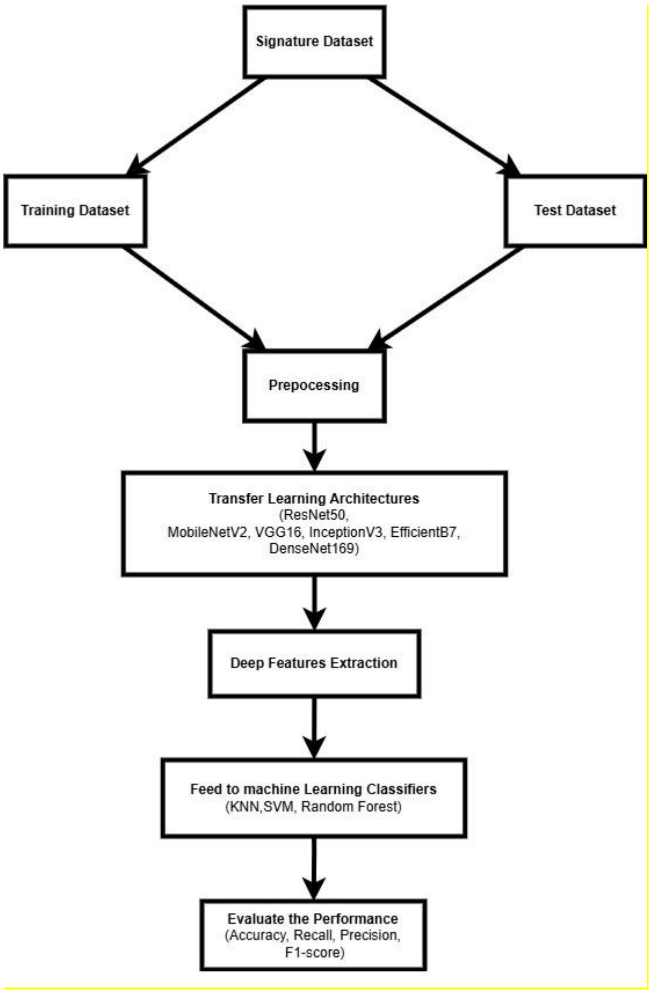

Figure 1. Flow diagram of the proposed methodology

A. Dataset

The BHSig260 dataset is an important resource, especially for signature recognition and verification. The BHSig260 dataset contains the signatures of 260 different individuals, 100 of which are represented by Bengali signatures and the rest by Hindi signatures. In total, there are 6240 real signatures and 7800 forged signatures in this dataset. For each person, there are 24 real and 30 forged signature samples. This results in 3840 real signatures and 4800 forged signatures per 160 people for Bengali signatures and 2400 real signatures and 3000 forged signatures per 100 people for Hindi signatures [22]. Figure 2. shows examples of Hindi signatures.

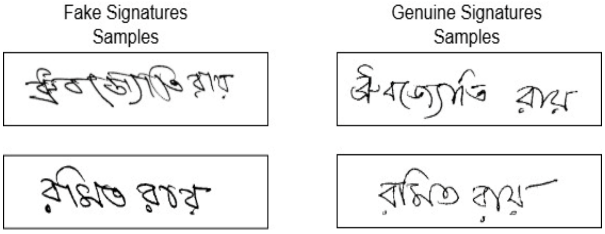

Figure 2. BHsig260 Hindi dataset genuine and fake signatures examples

In this study, only Hindi signatures are used for training and testing purposes. The Hindi dataset is divided into three independent subsets for training, validation and evaluation of the model. In this context, 64% of the total signatures are allocated to the training set, 16% to the validation set and 20% to the test set. This partitioning strategy maintains the initial approach of using 80% of the data for training and validation, while ensuring that the validation set is not derived from the training data and is completely independent. Thus, the validation and test sets are separated as independent sets that are not involved in the training process.

B. Model Development

Signature verification is critical in the field of biometric authentication and can be defined as a process that recognizes and verifies the individual characteristics of written signatures. In this field, the increasing use of machine learning and deep learning techniques is improving the accuracy and security of signature verification. While machine learning methods typically utilize feature engineering, classification algorithms and other statistical methods to recognize patterns in signature data, deep learning achieves successful results in signature verification tasks, especially with its ability to learn more complex relationships in large data sets [23]. At this point, the strong performance of deep learning methods plays an important role in making signature verification systems more accurate and reliable.

The splitting ratios chosen for the Turkey dataset used in the study are in line with data separation standards widely adopted in the field of deep learning [24]. In addition, a validation set that is completely independent from the training data and of sufficient size was created to be used in processes such as hyperparameter optimization, early stopping and prevention of overlearning. However, by ensuring that the test data was not used in the training process in any way, the overall performance of the model was evaluated in a statistically significant and reliable way. Keeping the training and validation sets at 80% in total is designed to preserve the model's performance in the learning process. Finally, by setting the test set at 20%, the performance of the model on real-world data could be analyzed more robustly. In addition, different CNN architectures such as ResNet50, MobileNetV2, VGG16, InceptionV3, EfficientNetB7 and DenseNet169, which are pre-trained on ImageNet, are used for deep feature extraction. In these models, the classification layers are removed, and the outputs of the final convolutional block are directly converted into vectors by flattening to preserve low-level textural and curvilinear information, which is especially important in structurally rich images such as signatures. In the transfer learning process, weights were frozen in all models and only the extracted features were used for subsequent classifiers. In the transfer learning phase, Adam optimization algorithm, learning rate 0.0001, batch size 32, maximum 50 epochs and early stopping criterion if the validation loss does not improve for 7 consecutive epochs were used as common hyperparameters. The resulting deep features were classified by the classical machine learning algorithms KNN (K=5), SVM (RBF kernel, C=1.0) and RF (20 trees). In order to prevent the model from overlearning, the training, validation and test datasets were created completely independently from each other and the training process was controlled by early stopping method. In this way, the generalization capacity of the models was increased. The proposed hybrid approach combines the powerful feature extraction capabilities of deep learning architectures with the low computational cost and explainable structures of classical machine learning algorithms, enabling high performance even under limited data conditions. While in the literature, either only deep learning or only classical methods are usually used, this study offers an innovative and effective solution by combining the advantages of both methods.

Deep learning techniques, especially with network structures such as CNN and Recurrent Neural Networks (RNN), provide efficient results in signature verification processes. CNN has a strong performance in learning visual features and is effective in recognizing the geometric features of the signature, while RNN is successful in discovering relationships in time-dependent data. These network structures allow for a deeper understanding of the evolution of signatures over time and their individual characteristics. In particular, CNN is effective in learning the shape and drawing dynamics of the signature, while RNN can further improve accuracy by modeling changes in the writing style and speed of the signature over time [25]. Therefore, the combination of these deep learning methods results in a more powerful system, improving accuracy and reliability in the signature verification process.

In recent years, the combination of deep learning and machine learning techniques has enabled signature verification systems to become more accurate and reliable. The integration of these two approaches plays an important role in the development of signature verification systems. The combination of deep learning and machine learning combines the advantages of both technologies, resulting in more advanced and powerful models. Another important development that makes this integration possible is the transfer learning technique. Transfer learning allows a model to use the knowledge it has acquired in another task in a new and different task. It provides great efficiency in terms of time and resources, especially in training deep learning models based on large data sets [26]. Thus, transfer learning techniques allow training powerful models with smaller data sets in the field of signature verification.

The use of transfer learning techniques in signature verification allows the knowledge learned from previous models to be reused on smaller and more specific data sets. This not only reduces the training time of the model, but also improves its performance. Especially when working with limited data sets, transfer learning plays a critical role in improving the accuracy of the model. This advantage helps signature verification systems to become more efficient, while at the same time making it possible to achieve high accuracy rates with low data. Another important factor that increases the effectiveness of transfer learning is the integration of machine learning techniques into this process. In particular, classical machine learning algorithms such as KNN, SVM and RF, when supported by transfer learning, allow for more powerful and flexible models. This combination enables the development of more advanced and reliable systems in the field of signature verification.

C. Transfer Learning Architectures Used in the Study

Transfer learning is an important technique that allows a model to use the knowledge it has already learned in another task in a new task. This method offers significant advantages in training models based on large data sets, especially in the field of deep learning [27]. Especially in biometric authentication tasks, such as signature verification, transfer learning techniques are frequently preferred in order to build stronger models with limited data sets. Deep learning models learn complex relationships, often by training on very large datasets, and are able to transfer this learned knowledge to smaller, more specific datasets. Thus, a robust and generalizable model can be obtained even when training with more limited data. In this context, transfer learning architectures such as MobileNetV2, ResNet50, DenseNet169, InceptionV3 and EfficientB7 make significant contributions in terms of efficiency, accuracy and speed in tasks such as signature verification. Each model, with its specific advantages and architectural differences, improves performance in such tasks. The structure and features of each model are briefly described below.

MobileNetV2 is a deep learning model optimized for mobile and low-power devices. This model was developed specifically for platforms with limited computational power, such as mobile and embedded systems. Using a technique called “depthwise separable convolutions”, MobileNetV2 achieves efficient results with fewer parameters and processing power. In the context of transfer learning, MobileNetV2 has been successfully used in biometric verification tasks such as signature verification, offering high accuracy rates and low computational costs, especially when working with small data sets [28].

ResNet50 is a widely used model in deep learning networks. It has a 50-layer structure and facilitates the training of deeper networks by using the “Residual Learning” method. An important advantage of this model is that it can eliminate the vanishing gradient problem encountered in deep networks. In the context of transfer learning, ResNet50 is highly effective in tasks such as signature verification, because the layers in the deep structure have the ability to better learn the complex and detailed features of signatures. The success of this model becomes especially evident in signature verification tasks based on large datasets [29].

DenseNet169 is a model that preserves all connections between each layer and enables more efficient feature learning using dense connections. This architecture enables each layer to receive more information from the previous layers, resulting in deeper and more efficient learning processes. DenseNet169 can perform effectively in signature verification tasks, especially in environments with small data sets. When supported by transfer learning, it enables faster and more accurate results based on previously trained models. This is especially advantageous in biometric verification applications where data sets are limited [30].

InceptionV3 is a deep learning model developed by Google and is particularly known for its high accuracy rates. This model uses the “inception module” to learn features at different resolutions in parallel. This structure enables richer and more comprehensive feature learning by combining multiple filters. With its transfer learning technique, InceptionV3 becomes an effective model for tasks such as signature verification. Especially trained on large datasets, this model can achieve successful results even on small datasets and provides high security in the field of signature verification [31].

EfficientNetB7 is an architecture that has become popular in the field of deep learning in recent years and optimizes the model size to achieve more efficient results. The EfficientNet series aims to learn the relationship between each layer more efficiently while optimizing the number of parameters of the model. EfficientNetB7, when integrated with transfer learning, is particularly effective with large data sets and complex tasks such as signature verification. The high accuracy rates of the model are especially evident when trained on large datasets and provide reliable results in biometric authentication applications such as signature verification [32].

D. Classical Machine Learning Methods Used in the Study

Transfer learning allows a deep learning model to use the knowledge it has already learned in a different task in a new and specific task. This technique is often used to enable the model to learn quickly on limited data sets. The combination of transfer learning architectures and classical machine learning methods provides a great advantage, especially in biometric authentication applications such as signature verification. In this study, a powerful and flexible model is created by combining transfer learning architectures and classical machine learning algorithms. Transfer learning allows deep learning networks to be applied effectively on smaller and more specific datasets, while classical machine learning algorithms (such as K-nearest neighbor, Support Vector Machines and Random Forest) act as additional elements that improve the accuracy of the model. The structure and characteristics of each method are briefly described below.

KNN algorithm is one of the unsupervised learning methods and is often used for classification problems. When determining the class of a new data set, KNN uses the k closest instances in the data set and makes a decision based on the classes of these instances. KNN is particularly effective for achieving high accuracy on small data sets. When combined with transfer learning, the features learned by deep learning models previously trained on large data sets can be used with the KNN algorithm for accurate classification on smaller data sets. This combination enables successful results in tasks such as signature verification, even when working with limited data [33].

SVM is one of the supervised learning algorithms and is particularly effective for nonlinear classification problems. SVM determines the classification boundaries between data by transforming the data into a high-dimensional space. This algorithm is particularly successful when data points are close to each other. When SVM is combined with transfer learning, the features obtained from the deep learning model are used to make more accurate and precise classifications. Transfer learning improves the classification capacity of SVM and helps to achieve more robust and reliable results in biometric tasks such as signature verification [34].

Random Forest is one of the ensemble learning methods and allows many decision trees to come together to form a stronger and more stable model. Each tree is trained on a random subset of the data and the final decision is determined by a majority vote of these trees. Random Forest is specifically used to reduce the overfitting problem and make more robust predictions. Combined with transfer learning, Random Forest allows for a more detailed evaluation of the features learned from the deep learning model. In this way, in biometric applications such as signature verification, more accurate classifications can be made and high accuracy rates can be achieved even with low data sets [35].

This study has demonstrated that transfer learning architectures combined with classical machine learning algorithms such as KNN, SVM and RVM are highly effective for improving the accuracy and reliability of signature verification.

III. RESULTS AND DISCUSSION

Recent advances in biometric authentication have been made possible by the integration of artificial intelligence techniques. These developments play a critical role in increasing security and improving fraud detection, especially in applications such as signature verification. Signature verification has become an area that requires increasingly sophisticated methods to accurately analyze changes over time and individual signature characteristics. Deep learning and machine learning techniques offer important contributions to biometric verification systems, making it possible to overcome these challenges.

Deep learning techniques enable the development of models that can extract detailed features of signatures and understand how they change over time. This enables high accuracy rates in verification processes. Furthermore, methods such as transfer learning allow for efficient utilization of the information obtained from deep learning models, especially on small data sets [36]. The main reason why transfer learning is so effective in biometric verification systems is that the knowledge gained from larger data sets can be used in smaller data sets. This is a great advantage when data is limited and helps to maintain the accuracy of the model [37].

Machine learning techniques combine with transfer learning to strengthen the validation process. In systems working with small data sets, classical machine learning algorithms offer significant advantages. These algorithms can quickly recognize patterns in the data set and contribute to higher accuracy rates in the classification process. Combining the features obtained by transfer learning with classical machine learning methods increases the accuracy of verification systems and provides more robust and reliable results [35].

The combination of deep learning and machine learning techniques allows to more successfully manage the complexity of data in biometric verification and security systems, while significantly improving accuracy rates. This integration plays an important role in the development of more reliable and robust verification systems for biometric tasks such as signature verification.

In this work, various transfer learning models are used for signature verification. These models include ResNet50, MobileNetV2, VGG16, InceptionV3, EfficientB7 and DenseNet169. First, these six different transfer learning architectures are tested on the BHSig260 Hindi dataset. The performance of each model on the signature verification task is evaluated with specific performance metrics. These metrics were used to measure the performance of each model with respect to important criteria such as accuracy, precision, specificity and F1 score. The results obtained are extensively analyzed to compare the validation performance of these models on the BHSig260 Hindi dataset. Table 1 presents the performance metrics obtained for each model in detail. The accuracy and loss graphs of the VGG16 architecture, which gives the most successful verification result, are presented in Figure 3.

Table 1. Verification performance metrics of transfer learning architectures for signatures on the BHSig260 Hindi dataset

Transfer Learning	Accuracy (%)	Recall (%)	Precision (%)	F1-score (%)
ResNet50	88.27	82.08	86.15	88.27
MobileNetV2	87.02	88.03	86.03	87.02
VGG16	92.77	91.58	93.25	92.42
Inceptionv3	79.38	85.95	91.70	71.77
EfficientB7	83.66	78.20	83.94	80.97
DenseNet169	83.14	72.70	87.25	79.31

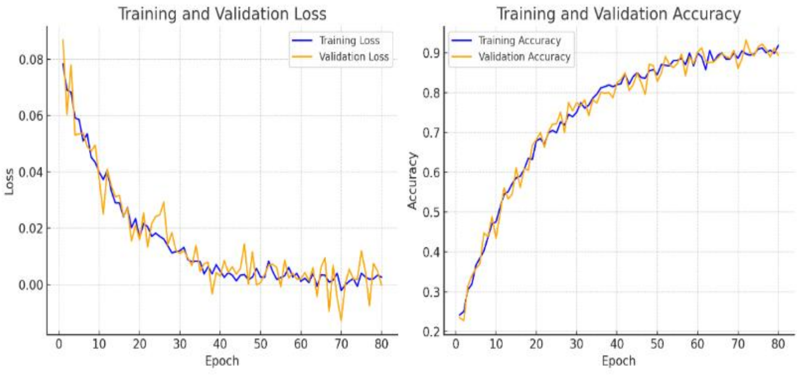

Figure 3. VGG16 architecture accuracy and loss graphs

Performance metrics used to evaluate the effectiveness of signature verification systems play a critical role in understanding the accuracy and reliability of the model. In this study, the success of the models is measured by four key metrics: accuracy, recall, precision and F1 score. Accuracy is the proportion of all instances correctly classified by the model and indicates overall success. Precision measures the ratio of the model's true positive predictions (TP - True Positive) to all positive predictions (TP + FP - False Positive), while recall is the ratio of the model's true positive predictions (TP) to all true positive predictions (TP + FN - False Negative). These two metrics are important in assessing the model's ability to detect forgery and authenticate correctly. Finally, the F1 score measures the model's ability to achieve overall balance by taking the harmonic mean of precision and recall. The F1 score aims to both increase true positives (TP) and minimize false positives (FP) and false negatives (FN), especially in cases of imbalance between classes. These metrics provide a more comprehensive performance analysis by assessing both the model's ability to provide accurate results and its capacity to minimize false positives and negatives. The mathematical formulas of performance metrics are essential tools for assessing the accuracy and reliability of the model. The formulas for calculating these metrics are presented in Equations (1), (2), (3) and (4) respectively. These formulas allow to calculate the accuracy, precision, recall and F1 score, taking into account the correct and misclassifications (TP, TN, FP, FN) of the model.

$$Accuracy = \frac{(\mathrm{TP+TN})}{(\mathrm{TP+TN+FP+FN})} \quad (1)$$

$$\mathrm{Precision} = \frac{\mathrm{TP}}{(\mathrm{TP + FP})} \quad (2)$$

$$\mathrm{Recall} = \frac{\mathrm{TP}}{(\mathrm{TP + FN})} \quad (3)$$

$$\mathrm{F1 - Score} = 2\,\mathrm{x}\,\frac{\mathrm{Precision\ x\ Recall}}{(\mathrm{Precision + Recall})} \quad (4)$$

According to the results in Table 1, the VGG16 model achieved the highest performance with an accuracy of 92.77%. It also showed the best overall verification performance with high precision (93.25%) and recall (91.58%). ResNet50 (88.27% accuracy) and MobileNetV2 (87.02% accuracy) stood out with high accuracy rates, and both models provided balanced metrics. Although the InceptionV3 model lags behind the other models with 79.38% accuracy, it shows a strong performance in forgery detection with high recall (85.95%) and good precision (91.70%). EfficientB7 and DenseNet169 achieved similar results with 83.66% and 83.14% accuracy, respectively, but their recall rates were lower than the other models. Overall, VGG16 exhibited the highest accuracy and best overall performance, while the other models also achieved strong results in specific metrics. These results suggest that each model offers different advantages in signature verification tasks.

In the second part of the study, in addition to the transfer learning models, the KNN method was also used and tested on the same dataset. In Table 2, the verification performance metrics of the KNN method added to each transfer learning model are presented in detail.

Table 2. Verification performance metrics of signatures in BHSig260 dataset with transfer learning architectures and KNN method

Transfer Learning+KNN	**Accuracy (%)**	**Recall (%)**	**Precision (%)**	**F1-score (%)**
ResNet50+KNN	89.69	80.08	96.05	87.34
MobileNetV2+KNN	90.76	85.125	93.50	89.11
VGG16+KNN	88.72	82.16	91.59	86.62
Inceptionv3+KNN	87.00	82.58	87.46	84.95
EfficicientB7+KNN	86.72	78.95	89.93	84.09
DenseNet169+KNN	93.09	87.75	96.38	91.86

According to the results in Table 2, the combination of DenseNet169 + KNN shows the highest validation performance with 93.09% accuracy and 91.86% F1 score. This model achieves superior results in both precision and recall metrics and offers the best overall performance. The MobileNetV2 + KNN model showed a strong validation performance with an accuracy of 90.76% and an F1 score of 89.11%, especially notable for its high recall rate (85.12%). ResNet50 + KNN (89.69% accuracy) and VGG16 + KNN (88.72% accuracy) models also achieved good results with high accuracy rates and balanced metrics. However, EfficientB7 + KNN (86.72% accuracy) and InceptionV3 + KNN (87.00% accuracy) models have lower accuracy and F1 score values compared to other combinations and lag behind in terms of performance.

In the third part of the study, in addition to the transfer learning models, the SVM method was also used and tested on the same dataset. In Table 3, the verification performance metrics of the SVM method added to each transfer learning model are presented in detail.

Table 3. Verification performance metrics of signatures on the BHSig260 Hindi dataset with transfer learning architectures and SVM method

Transfer Learning+SVM	**Accuracy (%)**	**Recall (%)**	**Precision (%)**	**F1-score (%)**
ResNet50+SVM	92.85	92.00	91.92	91.96
MobileNetV2+SVM	91.15	90.72	90.84	90.78
VGG16+SVM	92.04	91.66	91.22	91.44
Inceptionv3+SVM	92.53	92.54	90.83	91.68
EfficicientB7+SVM	94.44	93.66	93.74	93.82
DenseNet169+SVM	93.81	93.70	92.47	93.08

According to Table 3, the EfficientB7 + SVM combination performed the best with 94.44% accuracy and 93.82% F1 score. This model is characterized by high precision (93.74%) and recall (93.66%). DenseNet169 + SVM achieved a high performance with 93.81% accuracy and 93.08% F1 score. ResNet50 + SVM (92.85% accuracy) and InceptionV3 + SVM (92.53% accuracy) models also provided effective results with high accuracy and balanced metrics. VGG16 + SVM performed strongly with an accuracy of 92.04% and an F1 score of 91.44%. These findings show that the combination of transfer learning and SVM provides high accuracy and reliability in signature verification.

In the third part of the study, in addition to the transfer learning models, the Random Forest method was also used and tested on the same dataset. In Table 4, the verification performance metrics of the SVM method added to each transfer learning model are presented in detail.

Table 4. Verification performance metrics of signatures on the BHSig260 Hindi dataset with transfer learning architectures and Random Forest method

Transfer Learning+Random Forest	Accuracy (%)	Recall (%)	Precision (%)	F1-score (%)
ResNet50+ Random Forest	93.75	91.41	94.36	92.86
MobileNetV2+ Random Forest	94.22	91.95	94.88	93.39
VGG16+ Random Forest	93.77	90.79	94.98	92.84
Inceptionv3+ Random Forest	93.48	92.20	93.06	92.63
EfficicientB7+ Random Forest	95.24	94.83	94.47	94.65
DenseNet169+ Random Forest	94.61	92.25	95.47	93.83

The results in Table 4 show that the EfficientB7 + Random Forest combination performed the best with 95.24% accuracy and 94.65% F1 score. This model is characterized by high recall (94.83%) and precision (94.47%). DenseNet169 + Random Forest offers a similarly strong verification performance with 94.61% accuracy and 93.83% F1 score. MobileNetV2 + Random Forest and ResNet50 + Random Forest models also achieved effective results with 94.22% and 93.75% accuracy rates, respectively. The VGG16 + Random Forest and InceptionV3 + Random Forest models perform less well with 93.77% and 93.48% accuracy rates, respectively, but still contribute to the overall success. These results show that the combination of transfer learning models and the Random Forest algorithm provides strong and reliable performances in the signature verification task.

In this study, we observe that machine learning algorithms added to transfer learning approaches contribute significantly to signature verification performance. First, the results obtained with transfer learning models only showed that the overall verification performance was high. However, the validation performance of these models is significantly improved when combined with machine learning methods such as K-nearest neighbor (KNN), Support Vector Machines (SVM) and Random Forest. For example, the combination of DenseNet169 + KNN achieved 93.09% accuracy and 91.86% F1 score, outperforming the accuracy of the transfer learning model alone. Similarly, the EfficientB7 + SVM combination achieved an F1 score of 93.82%, improving on the 94.44% accuracy achieved by transfer learning alone. The most remarkable result was seen in the EfficientB7 + Random Forest combination. This combination achieved the highest verification performance in all stages with 95.24% accuracy and 94.65% F1 score. These findings clearly demonstrate that combining the powerful features of transfer learning techniques with the classification capabilities of machine learning algorithms leads to higher accuracy, precision and overall performance in signature verification tasks. Therefore, the integration of transfer learning and machine learning algorithms enables the development of more robust and reliable verification systems by utilizing the advantages of both methods

IV. CONCLUSION

Signature verification plays a critical role in security and fraud detection in biometric authentication systems. While traditional methods have limited verification performance, deep learning and machine learning techniques provide more accurate and reliable results. In particular, transfer learning increases the success in this field by enabling the transfer of information from large data sets even with limited data. In this study, we investigate the performance of signature verification using a combination of transfer learning models and machine learning algorithms. First, we verify with transfer learning models (ResNet50, MobileNetV2, VGG16, InceptionV3, EfficientB7, DenseNet169) and find that the VGG16 model has the highest performance with 93.77% accuracy. In the second stage, KNN algorithm was added to the transfer learning architectures and the combination of DenseNet169 + KNN achieved the highest performance with 93.09% accuracy. In the third stage, SVM algorithm was added to the transfer learning architectures and EfficientB7 + SVM model provided the best results with 94.44% accuracy. In the fourth stage, the EfficientB7 + Random Forest model achieved the highest success with 95.24% accuracy and 94.65% F1 score as a result of the integration of transfer learning architectures with Random Forest. As a result, the integration of transfer learning and machine learning algorithms has significantly improved the performance of signature verification. These methods have laid a strong foundation for the development of reliable and highly accurate verification systems.

Statement of Conflicts of Interest

There is no conflict of interest between the authors.

Statement of Research and Publication Ethics

The authors declare that this study complies with Research and Publication Ethics

REFERENCES

[1] Stauffer, M., Maergner, P., Fischer, A., & Riesen, K. (2020). A survey of state of the art methods employed in the offline signature verification process. *New trends in business information systems and technology: digital innovation and digital business transformation*, 17-30.

[2] Mohammed, Q. A. A. S., Joudah, M., & Mohammed, H. (2024, October). A survey on digital signature schemes. In *AIP Conference Proceedings* (Vol. 3232, No. 1). AIP Publishing.

[3] Saripan, H., & Hamin, Z. (2011). The application of the digital signature law in securing internet banking: Some preliminary evidence from Malaysia. *Procedia Computer Science*, *3*, 248-253.

[4] Vatambeti, R., Divya, N. S., Jalla, H. R., & Gopalachari, M. V. (2022). Attack Detection Using a Lightweight Blockchain Based Elliptic Curve Digital Signature Algorithm in Cyber Systems. *International Journal of Safety & Security Engineering*, *12*(6).

[5] Hameed, M. M., Ahmad, R., Kiah, M. L. M., & Murtaza, G. (2021). Machine learning-based offline signature verification systems: A systematic review. *Signal Processing: Image Communication*, *93*, 116139.

[6] Impedovo, D., & Pirlo, G. (2008). Automatic signature verification: The state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, *38*(5), 609-635.

[7] Alajrami, E., Ashqar, B. A., Abu-Nasser, B. S., Khalil, A. J., Musleh, M. M., Barhoom, A. M., & Abu-Naser, S. S. (2020). Handwritten signature verification using deep learning.

[8] Sam, S. M., Kamardin, K., Sjarif, N. N. A., & Mohamed, N. (2019). Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet inception-v1 and inception-v3. *Procedia Computer Science*, *161*, 475-483.

[9] Navid, S. M. A., Priya, S. H., Khandakar, N. H., Ferdous, Z., & Haque, A. B. (2019, November). Signature verification using convolutional neural network. In *2019 IEEE International Conference on Robotics, Automation, Artificial-intelligence and Internet-of-Things (RAAICON)* (pp. 35-39). IEEE.

[10] Parcham, E., Ilbeygi, M., & Amini, M. (2021). CBCapsNet: A novel writer-independent offline signature verification model using a CNN-based architecture and capsule neural networks. *Expert Systems with Applications*, *185*, 115649.

[11] Alsuhimat, F. M., & Mohamad, F. S. (2023). A Hybrid Method of Feature Extraction for Signatures Verification Using CNN and HOG a Multi-Classification Approach. *IEEE Access*, *11*, 21873-21882.

[12] Ghosh, R. (2021). A Recurrent Neural Network based deep learning model for offline signature verification and recognition system. *Expert Systems with Applications*, *168*, 114249.

[13] Sharma, N., Gupta, S., Mehta, P., Cheng, X., Shankar, A., Singh, P., & Nayak, S. R. (2022). Offline signature verification using deep neural network with application to computer vision. *Journal of Electronic Imaging*, *31*(4), 041210-041210.

[14] Hanmandlu, M., Sronothara, A. B., & Vasikarla, S. (2018, November). Deep learning based offline signature verification. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 732-737). IEEE.

[15] Pinzón-Arenas, J. O., Jiménez-Moreno, R., & Pachón-Suescún, C. G. (2019). Offline signature verification using DAG-CNN. *International Journal of Electrical & Computer Engineering (2088-8708)*, *9*(4).

[16] Naz, S., Bibi, K., & Ahmad, R. (2022). DeepSignature: fine-tuned transfer learning based signature verification system. *Multimedia Tools and Applications*, *81*(26), 38113-38122.

[17] Yapıcı, M. M., Tekerek, A., & Topaloğlu, N. (2021). Deep learning-based data augmentation method and signature verification system for offline handwritten signature. *Pattern Analysis and Applications*, *24*(1), 165-179.

[18] Hazra, A., Maity, S., Pal, B., & Bandyopadhyay, A. (2024). Adversarial attacks in signature verification: a deep learning approach. *Computer Science and Information Technologies*, *5*(3), 215-226.

[19] Attri, V. K., Jaiswal, T., Singh, B., Bansal, P., Sarangal, H., Kaur, S., & Kaur, H. (2024, January). Signature Verification Using Deep Learning: An Empirical Study. In *International Conference on Advances in Distributed Computing and Machine Learning* (pp. 175-187). Singapore: Springer Nature Singapore.

[20] Singh, A., & Viriri, S. (2020, March). Online signature verification using deep descriptors. In *2020 Conference on information communications technology and society (ICTAS)* (pp. 1-6). IEEE.

[21] Suganthe, R. C., Geetha, M., Sreekanth, G. R., Manjunath, R., Krishna, S. M., & Balaji, P. M. (2022, January). Performance Evaluation of Convolutional Neural Network Based Models On Signature Verification System. In *2022 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.

[22] Alvarez, G., Sheffer, B., & Bryant, M. (2016). Offline signature verification with convolutional neural networks. In *Technical report, Stanford University*.

[23] Hameed, M. M., Ahmad, R., Kiah, M. L. M., & Murtaza, G. (2021). Machine learning-based offline signature verification systems: A systematic review. *Signal Processing: Image Communication*, *93*, 116139.

[24] Pan, S. J., & Yang, Q. (2009). *A survey on transfer learning*. IEEE Transactions on Knowledge and Data Engineering, 22(10), 1345–1359. https://doi.org/10.1109/TKDE.2009.191

[25] Bengio, Y. (2009). Learning Deep Architectures for AI.

[26] Pan, S. J., & Yang, Q. (2009). A survey on transfer learning. *IEEE Transactions on knowledge and data engineering*, *22*(10), 1345-1359.

[27] Yosinski, J., Clune, J., Bengio, Y., & Lipson, H. (2014). How transferable are features in deep neural networks?. *Advances in neural information processing systems*, *27*.

[28] Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., & Chen, L. C. (2018). Mobilenetv2: Inverted residuals and linear bottlenecks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 4510-4520).

[29] He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 770-778).

[30] Huang, G., Liu, Z., Van Der Maaten, L., & Weinberger, K. Q. (2017). Densely connected convolutional networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 4700-4708).

[31] Szegedy, C., Vanhoucke, V., Ioffe, S., Shlens, J., & Wojna, Z. (2016). Rethinking the inception architecture for computer vision. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 2818-2826).

[32] Tan, M., & Le, Q. (2019, May). Efficientnet: Rethinking model scaling for convolutional neural networks. In *International conference on machine learning* (pp. 6105-6114). PMLR.

[33] Cover, T., & Hart, P. (1967). Nearest neighbor pattern classification. *IEEE transactions on information theory*, *13*(1), 21-27.

[34] Cortes, C. (1995). Support-Vector Networks. *Machine Learning*.

[35] Breiman, L. (2001). Random forests. *Machine learning*, *45*, 5-32.

[36] Yosinski, J., Clune, J., Bengio, Y., & Lipson, H. (2014). How transferable are features in deep neural networks?. *Advances in neural information processing systems*, *27*.

[37] Oquab, M., Bottou, L., Laptev, I., & Sivic, J. (2014). Learning and transferring mid-level image representations using convolutional neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1717-1724).