Alexandria Journal of Science and Technology

Article

Signature Verification Based on Deep Learning

Samar A. Kandeil [1], El-Sayed M.E. Mostafa [1], Wessam M. Salama [2,*]

[1] Department Mathematics and Computer Science, Faculty of Science, Alexandria University, Alexandria, Egypt.
[2] Department of Computer, Faculty of Engineering, Pharos University, Alexandria, Egypt.
[*] Correspondence Address:
Wessam M. Salama: Department of Computer, Faculty of Engineering, Pharos University, Alexandria, Egypt. Email: wessam.salama@pua.edu.eg.

KEYWORDS: Signature Recognition; Machine Learning; Handwriting Signature; Convolutional neural network; Transfer Learning.

Received: September 13, 2023
Accepted: November 24, 2023
Published: December 07, 2023

ABSTRACT: Signature verification is considered one of the main features in determining the person identity. Our proposed framework emphasizes the potential of Deep Learning Models (DLMs) in revolutionizing signature verification techniques and underscores the need for continuous exploration and advancement in the realm of automated signature authentication. Therefore, five pre-trained DLMs, ResNet50, DenseNet121, MobileNetV3, InceptionV3, and VGG16, based on four different datasets, CEDAR, BH-Sig260 Bengali, BHSig260 Hindi, and ICDAR 2011(Dutch),are introduced in this paper to verify the person identity. Furthermore, data augmentation techniques are applied to overcome dataset limitations and increase the framework's performance. Additionally, transfer learning and fine-tuning techniques are performed to reduce computational time and memory usage. It is observed that the InceptionV3 DLM based on the ICDAR 2011 (Dutch) achieved the best performance of 100% accuracy, 100% AUC and 100% sensitivity. While, CEDAR Dataset achieves performance with an accuracy of 99.76%, an AUC of 99.94%, sensitivity of 99.76%, precision of 99.76%, an F1-score of 99.71%, score, and a computational time of 13.627s.

1. INTRODCTION

Signature verification [1] is a fundamental modality for legally and socially confirming an individual's identity on a global scale. A reliable and robust signature verification system plays a vital role in sectors such as banking, finance, security, and legal documentation, serving as a means to detect and prevent fraud and forgery.

Handwritten signatures, whether collected offline or online [2] have served as a biometric modality for many decades due to their ease of acquisition and adaptability. With the rapid advancement of information technology and the increasing integration of machine learning [3] techniques across various domains, sophisticated computer-based identification systems are continuously emerging. These systems encompass a wide range of applications, including visual salience prediction in natural videos, character recognition, machine translation, signature verification, and writer identification.

The primary objective of a signature verification system is to validate an individual's identity by authenticating a provided scanned signature sample. Such verification processes can be categorized into two primary systems: offline (static) and online (dynamic) [4]. Offline systems involve capturing signatures using pen and paper, with the data subsequently obtainable through the scanning of physical signature documents.

As artificial intelligence continues to advance, deep learning techniques have gained increasing prominence in image analysis. Deep convolutional neural networks [5] have emerged as a practical means of extracting rich and intricate information. Within these deep learning models, the feature extraction stage, where the model learns the essential features present in signature images, holds critical importance [6]. Numerous studies have explored various Deep Learning Models (DLMs) for the verification of diverse signature types [7-12]. However, it is important to note that many DLMs demand substantial computational effort for accurate verification, and their effectiveness hinges on the features employed to characterize the signature images.

Consequently, researchers have explored various techniques for the verification process, including Neural Networks [13], Support Vector Machines [14], Hidden Markov Models [15], Genetic algorithms [16], Euclidean distance, k-nearest neighbors, among others. Geometric features, local and global characteristics [17], have also been extensively examined in the literature. More recently, researchers have leveraged deep convolutional neural networks for feature extraction in different domains of image processing [18-21].

DOI: 10.21608/AJST.2023.236375.1016

This research primarily aims to evaluate the performance of five distinct pre-trained deep learning models in the domain of signature verification, using four diverse signature datasets. This evaluation seeks to enhance the efficiency of the signature verification process while concurrently reducing associated costs.

In recent times, a specific subset of deep learning known as transfer learning has demonstrated significant potential in signature image verification. Transfer learning facilitates the utilization of pre-trained models initially designed for similar tasks. Several studies have been conducted leveraging pre-trained networks to extract valuable features from signature images. A number of these studies have employed different pre-trained Deep Learning Models (DLMs) and reported promising results for signature image verification [22].

Data augmentation represents a strategy for expanding the size of input data by generating new data instances from existing ones [23]. To address the limitation of signature databases, researchers have explored image augmentation techniques. These techniques encompass various options, including rotation, scaling, random cropping, and color adjustments, with pre-trained Convolutional Neural Network (CNN) architectures frequently employed for data augmentation.

The contribution of this paper lies in the utilization of five distinct pre-trained DLMs (ResNet50, DenseNet121, MobileNetV3, InceptionV3, and VGG16) for signature verification across four distinct datasets (CEDAR, BH-Sig260 Bengali, BHSig260 Hindi, and ICDAR 2011(Dutch)). In our proposed framework, data augmentation, fine-tuning, and transfer learning techniques are employed to address the challenge of limited data availability, thereby reducing memory requirements, computational time, and overall costs. In summary, the objectives of this paper are as follows:

- Utilizing five different pre-trained DLMs to verify signatures from four different datasets, CEDAR, BH-Sig260 Bengali, BHSig260 Hindi ,and ICDAR 2011(Dutch).
- Data augmentation techniques are applied to expand our training datasets and enhance our framework performance.
- Fine-tuning and transfer learning are introduced to reduce Computational time and improve our framework efficiency.

The subsequent sections of this paper are organized as follows: Related research and studies are reviewed in Section 2. Furthermore, our research approach and methodologies including training settings and models for all datasets are adopted in Section 3. The results of our experiments with a specific focus on the performance evaluation of signature verification model are presented in Section 4. Section 5 is dedicated to summarize the major findings and outlining directions for future research.

2. Related Work

Several studies have explored the field of signature verification using various approaches and datasets. Foroozandeh et al. [24] conducted experiments with different deep learning-based models on datasets such as the GPDS Synthetic signature dataset, MCYT-75, FUM-PHSD, and UTSig. Notably, when utilizing the UTSig dataset, they achieved significant accuracy rates, including 89.53% for SigNet, 88.24% for SigNet-F, 98.71% for VGG-16, 98.55% for VGG-19, 92.59% for ResNet50, and 97.58% for InceptionV3.

In another study [25], Abdel Raouf and Salama focused on Haar features, employing the Haar Cascade Classifier for signature classification and verification. They reported an accuracy rate of up to 92.42% on the UTSig dataset.

Mersa et al. [26] adopted a different approach by employing residual CNN to extract salient features, which were subsequently fed into an SVM classifier. Their system was tested on datasets including MCYT, GPDS-Synthetic, and UTSig, achieving impressive accuracy rates of up to 96.02%, 93.19%, and 90.2%, respectively.

Furthermore, Siamese Neural Networks were implemented for signature analysis by utilizing the GAVAB dataset and various combinations of synthetic data. Their trained model was evaluated with GPSSynthetic, MCYT, CEDAR, and SigComp11 datasets for forgery detection. Additionally, datasets from Kaggle consisting of 300 images were used, achieving a maximum accuracy of 99.7%.

In other studies [25-27], the UTSig dataset was evaluated using SVM and thresholding techniques for classification, employing various features including statistical, geometric, HOG, DRT, and DMML features.

These previous works highlight the diversity of methods and datasets utilized in the field of signature verification, laying the groundwork for our research.

3. Methodology

Our proposed framework is divided into different strategies, data augmentation and transfer learning based on five pre-trained DLMs. Data augmentation and transfer learning are introduced in this paper to overcome the lack of our datasets and reduce the computational time. Moreover, five different pre-trained DLMs, ResNet50, DenseNet121, MobileNetV3, InceptionV3, and VGG16, are utilized to verify the signature based on four different datasets. Our proposed framework harnesses the capabilities of pre-trained ResNet50, DenseNet121, MobileNetV3, InceptionV3, and VGG16 DLMs to avoid the model training from scratch. Pre-trained DLMs are performed in our framework to reduce the computational time, memory requirement and avoid the over fitting.

3.1. Datasets

- CEDAR: It contains English language signatures of 55 signers having a place with a different social and expert background as shown in **Fig.1**. Here for every user, 24 forged signatures and 24 genuine signatures are considered.
- BHSig260: This dataset contains Hindi as explained in **Fig.2**. and Bengali language signatures as shown in **Fig.3**. 100 signers from Bengali and around 160 from Hindi Each user comprises 24 genuine and 30 forged signatures.
- Dutch : This dataset comprises signatures of Dutch users, including both genuine and fraudulent samples. The dataset categorizes users into two groups: genuine users identified by their own user numbers and fraudulent users identified by appending “forg” to their user numbers as shown in **Fig.4**. All data is extracted from the ICDAR 2011 Signature Dataset and meticulously organized for user convenience.

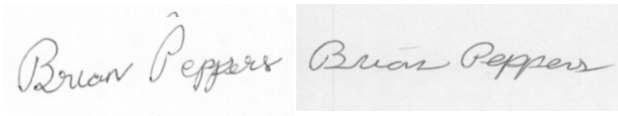

Fig.1 CEDAR dataset forged and genuine signatures

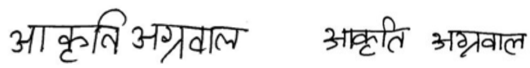

Fig.2 Hindi dataset forged and genuine signatures

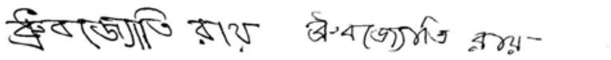

Fig.3 Bengali dataset forged and genuine

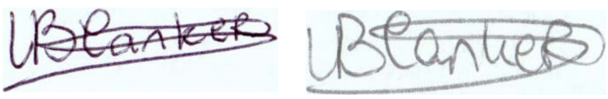

Fig.4 Dutch dataset forged and genuine signatures

An overview of general workflow is illustrated in Fig. 5 while the detailed explanations are presented in the following sections.

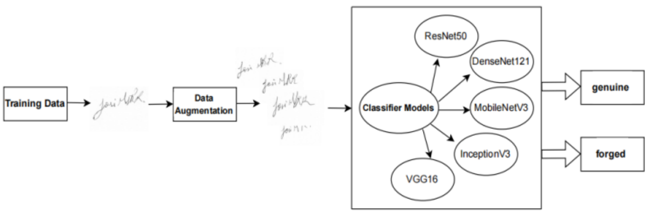

Fig.5 The Workflow Diagram of Training and Testing Phase for Proposed System

3.2. Transfer Learning

Transfer learning [28] plays a crucial role in leveraging small datasets, such as signature photos, which are often more challenging to gather in large quantities compared to other types of datasets. The process of training DLMs from scratch demands a significant amount of labeled data, considerable computational resources, and extensive time. To address these challenges, the concept of transfer learning is employed.

In our work, the capabilities of pre-trained models are employed to get the learned features and representations that are already encoded within these models. By utilizing transfer learning, these pre-trained models are adapted to the task of signature verification using our specific datasets.

To apply transfer learning, a two-step process is adopted. Initially, the pre-trained InceptionV3, DenseNet121, ResNet50, VGG16, and MobileNetV3 DLMs, are loaded. These models serve as a starting point, with their weights and parameters already fine-tuned on extensive datasets.

Subsequently, fine-tuning is performed to adjust the weights of the pre-trained models on our signature datasets. This allows the models to learn and adapt to the unique patterns and characteristics present in our data. Fine-tuning involves freezing certain layers of the pre-trained models, preventing them from being updated during training, while enabling the deeper layers to learn task-specific features from our signature data.

By applying transfer learning and fine-tuning, a balance between leveraging the rich knowledge acquired from pre-trained models and tailoring their capabilities to the specific task of signature verification are stroked. This approach not only mitigates the challenge of limited data availability but also expedites the training process and minimizes the computational resources required.

This approach empowers us to harness the strengths of state-of-the-art architectures while effectively addressing the challenges posed by limited signature data.

3.3. Data Augmentation Phase

Data augmentation techniques [29] are applied to increase the quantity of training images. In this paper, the following techniques are utilized to assess their impact on the efficiency of our models:

- Horizontal Flip: Images are horizontally flipped, creating mirror images. This augmentation technique contributes to diversifying the dataset and enhancing the model's ability to recognize signatures in various orientations.
- Rotation Range: Images are rotated by an angle of up to 20 degrees. This can improve the model's capacity to handle signatures with varying angles.
- Width Shift Range: Images are shifted horizontally by up to 20% of their width. This alteration changes the signature's position in the image, aiding the model's discrimination capabilities.
- Height Shift Range: Images are shifted vertically by up to 20% of their height. This enhances the model's ability to accommodate signatures at different positions.
- Zoom Range: Images are zoomed in or out by up to 20% from their original size. This augmentation technique enhances the visibility of details within the signatures.

These augmentation techniques are implemented to test their effectiveness in improving the performance of signature verification models in this research. They serve as a critical means to increase dataset diversity and boost model performance, particularly when working with limited available signature data.

3.4. Deep learning models

In this paper, we delve into the heart of our research by introducing the DLMs that serve as the building blocks of our signature verification system. Moreover Table.1 explains the parameters and hyper- parameters which are implemented in our proposed framework.

3.4.1. ResNet50 model

Residual Network50 (ResNet50) [30] is a deep learning model that has been widely utilized in various computer vision applications, including image classification, object detection, and signature verification. In our research, ResNet50 model is customized for our specific task by adding additional layers, including Batch Normalization, Dropout, and a final Dense layer with a softmax activation function for multi-class classification.

3.4.2. DenseNet121 model

DenseNet121 [31] is another deep learning model. DenseNet121 has been pre-trained on large-scale datasets, making it a strong candidate for transfer learning in our research. The model is customized by adding layers appropriate for signature verification, such as Batch Normalization, Dropout, and a final Dense layer for classification.

3.4.3. MobileNetV3 model

In this paper, we have included MobileNetV3 [32] as a deep learning model for signature verification. The model's efficiency and speed make it an attractive option, especially when computational resources are limited. MobileNetV3 is fined tuned on our signature datasets, adapting it to the specific requirements of signature verification.

By utilizing MobileNetV3, the trade-off between model efficiency and accuracy in the context of signature verification are explored in this paper. This investigation will provide insights into the feasibility of deploying lightweight models for real-world signature authentication applications.

3.4.4. InceptionV3 model

InceptionV3 [33] is a deep learning model known for its sophisticated architecture, which incorporates multiple parallel convolutional pathways of different filter sizes.

In our framework, the InceptionV3 model is applied for signature verification. Its ability to extract features at multiple scales can be advantageous when dealing with signature images of varying sizes and complexities.

3.4.5. VGG16 model

VGG16 [34] is a classic deep learning model that gained prominence for its simplicity and effectiveness. It consists of 16 layers, including 13 convolutional layers and 3 fully connected layers. Despite its relatively straightforward architecture, VGG16 has demonstrated strong performance in image classification tasks.

3.5. Training Settings and Models for All Datasets

In this paper, the training settings used during the DLMs training for all four datasets: CEDAR, BH-Sig260 Bengali, and BHSig260 Hindi are explained and outlined in Table.1.

As shown in Table.1, our implemented learning rate is 0.001 which is selected for all models, which is an appropriate rate to facilitate effective learning. Furthermore, from our experimental result, it is observed that the Adam optimizer and the momentum value used in the models is 0.99 which is used to aid in escaping local minima and speeding up convergence towards better solutions and achieves the best performance. Furthermore, the SoftMax activation function was utilized throughout the models to transform model outputs into probability distributions across signature classes. In the case of InceptionV3, an interesting experiment is conducted where the ReLU activation function is introduced alongside SoftMax. This addition is made with the intention of diversifying the activation functions and exploring their impact on the model's performance in the context of signature classification. Batch sizes were chosen differently for each model and play a crucial role in training speed and memory consumption. The categorical_crossentropy loss function is used in to measure the loss between the actual and predicted outputs of the model. Model selection should consider specific application requirements and the desired balance between precision and recall. These settings were consistently applied across all datasets to ensure uniformity and facilitate meaningful comparisons.

To extend the analysis, an additional dataset, ICDAR 2011 (Dutch), is incorporated. This dataset introduces a new dimension to the study. Notably, during experimentation with this dataset on the five models, certain adjustments were are made. Specifically, the learning rate and batch size are reduced to accommodate the smaller dataset size, ensuring a valid and reliable experiment. These modifications are implemented to optimize the models for the characteristics of the ICDAR 2011 (Dutch) dataset while maintaining consistency in the overall experimental framework.

4. Results and Discussion

In this paper, the results of our experiments and engage in a comprehensive discussion of the findings are represented. The performance of five distinct pre-trained deep learning models across four diverse signature datasets, CEDAR, BH-Sig260 Bengali, BHSig260 Hindi,and ICDAR 2011 (Dutch), are evaluated in this paper. Different approaches, including data augmentation, fine-tuning, and transfer learning, to address the challenges posed by limited data availability are applied. The evaluation of the signature verification performance relies on a set of critical metrics, including the number of true positives (TP), true negatives (TN), false negatives (FN), and false positives (FP). These metrics are fundamental in assessing the capabilities of the models in distinguishing genuine from forged signatures. Specifically, we calculate accuracy, Area Under the Curve (AUC), positive predictive value (Pr), F1-score, and computational time as key evaluation criteria.

Our framework is conducted using the Keras deep learning library in Python, and the experiments are executed on a Notebook GPU cloud environment equipped with 2 CPU cores and 13 GB RAM.

The findings of our investigation will shed light on the effectiveness of different DLMs and strategies in the context of signature verification. This comprehensive evaluation will facilitate the selection of the most suitable models for real-world signature authentication applications

4.1. Performance Evaluation of Signature Verification Models

Our objective is to provide a comprehensive understanding of the outcomes, shedding light on the strengths and weaknesses of each model. Additionally, we will explore the impact of data augmentation on the performance of these models to assess whether it leads to improvements as shown in Table 2.

Table.1: Explains the parameters of our proposed DLMs based on three different datasets.

Setup	Learning rate	Optimizer	Activation function	Momentum	Batch size	Loss	Epoch
VGG16	0.001	Adam	SoftMax	0.99	30	categorical_crossentropy	50
InceptionV3	0.001	Adam	SoftMax, Relu	___	32	categorical_crossentropy	100
MobileNetV2	0.001	Adam	SoftMax	0.99	30	categorical_crossentropy	100
ResNet50	0.001	Adam	SoftMax	0.99	30	categorical_crossentropy	50
DenseNet121	0.001	Adam	SoftMax	0.99	30	categorical_crossentropy	100

Table 2: Comprehensive results for all models across different Datasets

Model	Accuracy %		AUC %		Recall %		Precision %		F1-score %		Sensitivity %	
	With	With out	With	With out	With	With out	With	With out	With	With out	With	With out
	Augmentation		Augmentation		Augmentation		Augmentation		Augmentation		Augmentation	
Hindi dataset												
InceptionV3	98.24	99.19	99.76	99.93	98.05	99.04	98.41	99.37	98.23	99.21	98.05	99.04
VGG16	83.09	94.78	98.88	99.33	79.67	93.86	88.96	95.73	83.93	94.77	79.67	93.86
MobileNet V3	83.64	92.94	99.32	98.76	80.15	92.57	89.23	93.33	84.34	92.95	80.15	92.57
DenseNet121	26.18	92.02	77.59	98.84	22.13	91.62	34.05	92.74	26.68	92.16	22.13	91.62
ResNet50	65.07	90.62	96.51	98.64	59.52	89.93	75.16	91.68	66.25	90.77	59.52	89.93
Bengali dataset												
InceptionV3	98.35	99.59	99.76	99.97	98.29	99.59	98.47	99.59	98.41	99.59	98.32	99.59
DenseNet121	28.94	96.06	75.82	99.58	27.24	96	35	96.23	30.38	96.11	27.24	96
VGG16	88.24	95.59	99.08	99.43	85.53	95.29	91.5	96.43	88.37	95.84	85.53	95.29
MobileNet V3	89.35	94.65	99.36	99.14	87.82	94.47	91.6	94.92	89.63	94.68	87.82	94.47
ResNet50	68.88	93.12	95.53	99.16	64.12	92.82	75.59	93.93	69.21	93.36	64.12	92.82
CEDAR dataset												
InceptionV3	98.55	99.76	99.75	99.94	98.55	99.76	98.67	99.76	93.58	99.76	98.52	99.76
ResNet50	97.21	97.82	99.81	99.51	97.21	97.7	97.45	97.82	97.38	97.8	97.26	97.74
VGG16	96.85	97.21	99.8	99.56	96.85	96.73	97.32	97.79	97.12	97.09	96.9	96.43
DenseNet121	63.88	94.06	91.54	99.07	61.58	93.94	68.83	94.4	65.22	93.92	61.9	93.69
MobileNet V3	73.82	93.45	93.95	98.94	71.76	93.21	75.99	93.89	73.47	93.65	71.55	93.33
Dutch dataset												
Inception V3	100	100	100	100	100	100	100	100	100	100	100	100
ResNet50	100	99.83	100	100	100	99.83	100	99.83	100	99.83	100	99.83
DenseNet121	99.67	99.67	99.78	99.99	99.67	99.67	99.67	99.67	99.67	99.67	99.67	99.67
VGG16	99.5	99.4	100	100	99.5	99.4	99.5	99.4	99.5	99.4	99.5	99.4
MobileNet V3	99.2	98.8	99.59	99.19	99.2	98.8	99.2	98.8	99.21	98.81	99.21	98.81

It is observed that the InceptionV3 demonstrates remarkable performance with high accuracy, initially achieving an impressive 99.19% accuracy. After data augmentation, the accuracy remains quite high at 98.24%. AUC percentages also demonstrate strong performance, with data augmentation yielding a 99.76% AUC, while without augmentation, it achieves 99.93%. Additionally, Recall percentages show 98.05% with augmentation and 99.04% without augmentation, with 98.41% precision with augmentation and 99.37% without augmentation. Furthermore, the F1-score percentages are noteworthy, 98.23% with augmentation and 99.21% without augmentation, indicating its proficiency in correctly identifying genuine signatures based on Hindi Dataset. Moreover, VGG16 initially performs well based on Hindi Dataset, with an accuracy of 94.78%, but it experiences a significant drop to 83.09% after data augmentation. Moreover, Data augmentation has varying effects on model performance, with some models maintaining stability, while others experience drops in accuracy.

This drop is reflected in precision and recall, suggesting a trade-off between minimizing false positives and false negatives. Furthermore, MobileNetV3 shows reasonable performance with an accuracy of 92.94% initially and 83.64% after data augmentation. Precision and recall remain balanced, making it a viable choice. In addition, the DenseNet121 follows MobileNetV3 in both scenarios, maintaining reasonable but lower performance compared to InceptionV3. Its performance remains consistent after data augmentation. It is observed that the ResNet50 consistently performs well but falls slightly behind InceptionV3 and VGG16 in accuracy. After data augmentation, its performance remains relatively stable.

Integrating the ICDAR 2011 (Dutch) dataset into our evaluation provides valuable insights into the performance of signature verification models across diverse datasets. InceptionV3 consistently achieved perfect accuracy of 100% in both scenarios, with and without data augmentation. This underscores its robust performance and underscores its exceptional ability to generalize effectively to the ICDAR 2011 (Dutch) dataset.

ResNet50 exhibited 100% accuracy with data augmentation, showcasing adaptability to increased data, and maintained a high accuracy of 99.83% without augmentation. ResNet50's performance on the ICDAR 2011 (Dutch) dataset is strong, comparable to InceptionV3, and remains stable with or without data augmentation. DenseNet121 demonstrated consistent performance with an accuracy of 99.67% both with and without data augmentation, showcasing its robustness to increased data. DenseNet121 consistently performed well on the ICDAR 2011 (Dutch) dataset, with no significant change in accuracy with data augmentation. VGG16 achieved an accuracy of 99.5% with data augmentation, indicating adaptability to increased data, and maintained a high accuracy of 99.4% without augmentation. VGG16 demonstrated stable performance on the ICDAR 2011 (Dutch) dataset, with minimal impact from data augmentation. MobileNetV3 achieved an accuracy of 99.2% with data augmentation, showcasing adaptability to increased data, and maintained a high accuracy of 98.8% without augmentation. MobileNetV3 displayed resilience to the ICDAR 2011 (Dutch) dataset, with a slight decrease in accuracy with data augmentation. In summary, the models consistently performed well on the ICDAR 2011 (Dutch) dataset, with data augmentation generally enhancing adaptability. The impact varied across models, emphasizing the need for careful consideration of data augmentation strategies based on the specific characteristics of the dataset and the chosen model architecture.

The training and testing times for signature verification models across different datasets, both with and without data augmentation is explained in Table.3. The training time represents the time taken to train each model, while the testing time indicates the time required for model testing. It's evident that the presence or absence of data augmentation has varying effects on training and testing times, which can be a critical factor when considering the practical deployment of these models. This information contributes to a comprehensive evaluation of model performance and aids in the selection of suitable models for real-world signature authentication applications.

The results show that the better performance is achieved by the proposed frameworks, as shown in Table 4.

5. Conclusion

In this paper, a new framework based on DLMs, including InceptionV3, DenseNet121, ResNet50, VGG16, and MobileNetV3, is proposed for the accurate identification of individuals' signatures with minimal computational time. The performance evaluation encompassed crucial metrics such as accuracy, Area Under the Curve (AUC), positive predictive value (Pr), F1-score, and computational time. The thorough analysis of the results underscored the effectiveness of the developed framework. Notably, InceptionV3 consistently outperformed other models across various dataset showcasing its robustness in accurately discerning genuine signatures while minimizing false positives and false negatives. Moreover, data augmentation was shown to have both positive and negative impacts on different models, signifying the necessity of considering specific application requirements when selecting the appropriate model. The proposed framework achieved an exceptional performance level, with InceptionV3 demonstrating the best results on Dutch dataset with 100% accuracy, 100 % AUC and 100 % sensitivity.

Moreover, the InceptionV3 achieves a suitable result with Accuracy of 99.19%, AUC of 99.93%, Sensitivity of 99.04%, Precision of 99.37%, F1-score of 99.21% based on Hindi dataset. Our proposed framework serves as a valuable contribution to the field of signature verification, offering an automated approach that eliminates the need for human intervention. The significance of this research extends to real-world applications where accurate and efficient signature verification is essential. Future research endeavors can explore further enhancements to these models, potentially addressing the challenges posed by data augmentation to ensure consistently improved performance.

Table 3: Time for all models to be trained and tested on four different Datasets

Model	Training time (s)		Testing time (s)	
	With	With out	With	With out
	Augmentation		Augmentation	
Hindi dataset				
InceptionV3	4131.0251	1903.768	23.289	30.629
VGG16	1854.646	952.5115	6.195	4.9267
MobileNetV3	3440.428	1736.945	8.3644	8.9858
DenseNet121	3701.4259	1753.507	17.5346	17.852
ResNet50	1805.6547	903.2445	7.659	9.1683
Bengali dataset				
InceptionV3	3313.134	1734.057	19.749	20.109
DenseNet121	3287.8786	1188.4177	13.2351	13.9707
VGG16	1653.8006	660.4835	4.293	4.814
MobileNetV3	3251.304	967.824	7.3	12.4939
ResNet50	1702.447	582.1727	9.2257	7.1653
CEDAR dataset				
InceptionV3	3496.93	1583.0649	13.503	13.627
ResNet50	1660.27	526.718	7.841	8.357
VGG16	1741.2596	657.9411	6.094	6.1245
DenseNet121	3285.352	1382.94	12.2525	12.843
MobileNetV3	3881.243	1005.1466	7.2825	5.661
Dutch dataset				
InceptionV3	233.822	173.642	7.518	7.438
ResNet50	484.457	203.57	5.187	5.1189
DenseNet121	972.7433	456.588	9.499	9.091
VGG16	471.863	188.1754	3.4513	2.145
MobileNetV3	914.274	382.2273	4.0493	4.0189

Table 4: Comparison between our work and other work in the literature

References	Techniques	Dataset Used	Accuracy %
Our Proposed framework	InceptionV3	CEDAR	99.76%
		BHSig260 Beng	99.59%,
		Hindi	99.19%
[35]	Siamese Neural Network	BHSig260	80%
		Bengali, Hindi	78%
[36]	CNN	CEDAR	95.31%
		BHSig260 Bengali	95.19%
		Hindi	95.12%
[37]	Surroundedness features	CEDAR	91.67%
[38]	Graph matching(Chen and Srihari)	CEDAR	92.10%
[39]	InceptionSVGNet	BHSig260 Bengali	97.77%
		Hindi	95.40%

References

[1] Bhattacharya, U.; Bhattacharya, S. An Efficient Handwritten Signature Verification System using Deep Learning Techniques. In Proceedings of the International Conference on Artificial Intelligence and Machine Learning. 2022, 47-54.

[2] He, Z.; Huang, D.D.; Yau, W.Y. A Deep Learning Framework for Offline Handwritten Signature Verification. IEEE Access. 2022, 10, 44271-44282.

[3] Ammar, R.; Mabroukeh, N.R. Machine Learning for Network Security. In 2021 International Conference on Communications, Signal Processing, and Systems CSPS, Chang Bai Shan, China, IEEE. 2021, 89-93.

[4] Sharma, N.; Sheifali G.; Puneet M.; Xiaochun C.; Achyut S.; Prabhishek S.; Soumya R.N. Offline signature verification using deep neural network with application to computer vision. Journal of Electronic Imaging, 31(4), 2022, 041210.

[5] Zhang, Y.; Li, Z.; He, K; Liu, J. Deep Convolutional Neural Networks for Image Processing: A Comprehensive Review. IEEE Transactions on Neural Networks and Learning Systems, 32(8), 2021, 3073-3092.

[6] Kao, H.H.; Wen, C.Y. An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach. Applied Sciences, 10 (11), 2020, 3716-3719.

[7] Abbas, S.; Zhou, Y. A. Survey of Deep Learning Models for Signature Verification. In 2022 International Conference on Computing, Data Science and Engineering (ICCDSE), Dubrovnik, Croatia, IEEE. 2022, 24-29.

[8] Aslan, Ö.A.; Samet, R. A. comprehensive review on malware detection approaches. IEEE access, 8, 2020, 6249-6271.

[9] Kothadiya, D.; Bhatt, C.; Sapariya, K.; Patel, K.; Gil-González, A.B.; Corchado, J.M. Deepsign: Sign language detection and recognition using deep learning. Electronics, 11(11), 2022, 1780.

[10] Rasheed, A.F.; Alkababji, A.M. A Novel Method for Signature Verification Using Deep Learning. Webology, 19(1), 2022, 1561-1572.

[11] Li, Y.; Xu, D.; Huang, L.; Yang, X.; Gong, Y. Offline Signature Verification Using a Two-Stream Network. IEEE Access, 10, 2022, 42136-42147.

[12] Zhang, S.; Zhang, S.; Wang, B.; Habetler, T.G. Deep learning algorithms for bearing fault diagnostics–A comprehensive review. IEEE Access, 8, 2020, 29857-29881.

[13] Hafemann, L.G.; Sabourin, R.; Oliveira, L.S.; Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition, 70, 2017, 163-176.

[14] Abdulhussien, A.A.; Nasrudin, M.F. Darwish, S.M.; Alyasseri, Z.A.A. A Genetic Algorithm Based One Class Support Vector Machine Model for Arabic Skilled Forgery Signature Verification. Journal of Imaging, 9(4), 2023, 79.

[15] Joon, D.; Kikon, S. An Offline Handwritten Signature Verification System-A Comprehensive Review. International Journal of Enhanced Research in Science Technology & Engineering, 4(6), 2015, 433-439.

[16] Abdulhussien, A.A.; Nasrudin, M.F. Darwish, S.M.; Alyasseri, Z.A.A. Feature selection method based on quantum inspired genetic algorithm for Arabic signature verification. Journal of King Saud University-Computer and Information Sciences, 35(3), 2023, 141-156.

[17] Shashi Kumar, D.R.; Raja, K.B.; Chhotaray, R. K.; Sabyasachi P. Off-line signature verification based on fusion of grid and global features using neural networks. International Journal of Engineering Science and Technology, 2(12), 2010, 7035-7044.

[18] Wang, X.; Zhang, Y.; Wang, Z. Deep Convolutional Neural Networks for Image Feature Extraction: A Comprehensive Review. IEEE Transactions on Image Processing, 31, 2022, 157-171.

[19] Hafemann, L.G., Sabourin, R.; Oliveira, L.S. Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition,70, 2017, 163-176.

[20] Zhang, J.; Li., C.; Yin, Y.; Zhang, J.; Grzegorzek, M. Applications of artificial neural networks in microorganism image analysis: a comprehensive review from conventional multilayer perceptron to popular convolutional neural network and potential visual transformer. Artificial Intelligence Review, 56(2), 2023, 1013-1070.

[21] Liu, J.; Liu, C.; Wang, Z. Deep Convolutional Neural Networks for Feature Extraction in Image Processing. IEEE Transactions on Neural Networks and Learning Systems, 33(1), 2022, 283-297.

[22] Kensert, A.; Harrison, P.J.; Spjuth, O. Transfer learning with deep convolutional neural networks for classifying cellular morphological changes. SLAS Discovery: Advancing Life Sciences R&D, 24(4), 2019, 466-475.

[23] Kebaili, A.; Lapuyade-Lahorgue, J.; Ruan, S. Deep Learning Approaches for Data Augmentation in Medical Imaging: A Review. Journal of Imaging, 9(4), 2023, 81.

[24] Foroozandeh, A.; Hemmat, AA.; Rabbani, H.; Offline handwritten signature verification and recognition based on deep transfer learning. International conference on machine vision and image processing (MVIP), IEEE. 2020, 1-7.

[25] AbdelRaouf, A.; Salama, D. Handwritten signature verification using haar cascade classifier approach. In: 2018 13Th international conference on computer engineering and systems (ICCES), 2018, 319–326.

[26] Mersa, O.; Etaati, F.; Masoudnia, S.; Araabi, B.N. Learning representations from persian handwriting for offline signature verification, a deep transfer learning approach. In 2019 4th International Conference on Pattern Recognition and Image Analysis (IPRIA), Tehran, Iran, 2019, 268-273.

[27] Salama, M.W.; Aly, M.H. Deep learning in mammography images segmentation and classification: Automated CNN approach. Alexandria Engineering Journal, 60(5), 2021, 4701-4709.

[28] Naz, S.; Bibi, K.; Ahmad, R. Deep Signature: fine-tuned transfer learning-based signature verification system. Multimedia Tools and Applications, 81(26), 2022, 38113-38122.

[29] Hameed, M.M.; Ahmad, R.; Kiah, L.M.; Murtaza, G.; Mazhar, N. Off Sig-Sin GAN: A Deep Learning-Based Image Augmentation Model for Offline Signature Verification. Computers, Materials & Continua, 76(1), 2023, 1267-1289.

[30] Kumar, D.; Sharma, S.; Mishra, M.P.; Unimodal biometric identification system on Resnet-50 residual block in deep learning environment fused with serial fusion. Global Journal of Enterprise Information System, 15(1), 2023, 40-49.

[31] Sharma, S.; Guleria, K. A. systematic literature review on deep learning approaches for pneumonia detection using chest X-ray images. Multimedia Tools and Applications, 2023, 1-51.

[32] Jia, L.; Wang, T.; Chen, Y.; Zang, Y.; Li, X.; Shi, H.; Gao, L. Mobile Net-CA-YOLO: An Improved YOLOv7 Based on the MobileNetV3 and Attention Mechanism for Rice Pests and Diseases Detection. Agriculture, 13(7), 2023, 1285-1289.

[33] Amiri, Z.; Heidari, A.; Navimipour, N. J.; Unal, M.; Mousavi, A. Adventures in data analysis: A systematic review of Deep Learning techniques for pattern recognition in cyber-physical-social systems. Multimedia Tools and Applications, 2023, 1-65.

[34] A.Jeyarani, R.; Senthilkumar, R. Eye Tracking Biomarkers for Autism Spectrum Disorder Detection using Machine Learning and Deep Learning Techniques. Research in Autism Spectrum Disorders, 2023, 108- 102228.

[35] Sharma, N.; Gupta, S.; Mohamed, HG.; Anand, D.; Mazón, JLV.; Gupta D.; Goyal, N. Siamese convolutional neural network-based twin structure model for independent offline signature verification. Sustainability, 14(18), 2022, 11484.

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

[37] Kumar, R.; Sharma, J.D.; Chanda, B. Writer-independent off-line signature verification using surroundedness feature," Pattern Recognit. Lett. 33(3), 2012, 301–308.

[38] Chen, S.; Srihari, S. A new off-line signature verification method based on graph," in 18th International Conference on Pattern Recognition (ICPR'06), 2(8), 2006, 869–872.

[39] Mohapatra R.K.; Shaswat, K.; Kedia, S. Offline handwritten signature verification using CNN inspired by inception V1 architecture. Fifth International Conference on Image Information Processing (ICIIP), 9, 2019, 263-267.