Augmented Human Research (2024) 9:4
https://doi.org/10.1007/s41133-024-00069-5

ORIGINAL PAPER

Enhancing Offline Signature Verification via Transfer Learning and Deep Neural Networks

S. Singh[1] · S. Chandra[1] · Agya Ram Verma[1,2]

Received: 5 April 2024 / Revised: 5 August 2024 / Accepted: 8 August 2024

Abstract
This paper presents a brief overview of signature identification and verification systems based on transfer learning. Different databases, namely CEDAR, ICDAR-2011, and BHSig260, are utilized for this study. In the field of biometrics and forensics, automated signature verification plays a crucial role in validating a person's authenticity. The signature can be offline (handwritten) or online (digital). This study mainly focuses on offline signatures forged by the skilled forgers because offline systems lack dynamic information such as pressure and velocity available in online systems. The offline signatures are analyzed on pretrained models, and their efficiency is analyzed on two critical metrics in the field of biometrics and security systems, namely false acceptance rate (FAR) and false rejection rate (FRR). InceptionV3 model gives highest accuracy of 99.10% and lowest FRR and FAR of 1.03% and 0.74%.

Keywords Handwritten signature · Transfer learning · Biometrics · Signature verification · Security

Introduction

The process of identifying a person using their physiological and behavioral characteristics is known as biometric identification. One of the most popularly used personal attributes is a handwritten signature, which is regarded as a legitimate means of person authentication in administrative and financial institutions. Generally, signatures are acquired in two methods—online and offline. Online signatures which are also called dynamic mode signatures are acquired by electronic gadgets which records the dynamic features like writing velocity, pressure, angle, number of pen-ups, time taken to put a signature, etc. Offline signatures are processed on paper, scanned using high-resolution scanners, and stored as images for automated processing. Offline signatures are categorized as genuine and forged signatures. Genuine signature reveals the identity of claimed individuals, whereas forged signature represents the imitation of the real one. However, offline signatures lack dynamic information available in online signatures; it poses a significant challenge in the field of image processing. Based on duplication of data in offline signatures, forgeries are classified as simple, random, skilled, unskilled, opposite handed, and free handed [1]. Identifying a proficient forgery poses the greatest difficulty. A novel method was proposed by Jivesh et al. [2], a two-staged algorithm used CNN, crest-trough-based model for signature recognition and Harris algorithm in combination with speeded up robust features (SURF) for forgery detection. Vohra et al. [3] used SVM for feature extraction and histogram of gradient, shape, aspect ratio, bounding area, contour area, and convex hull area which are extracted, and further CNN is used for classifying signature as forged or genuine. The algorithm proposed by Agarwal et al. [4] took the tampered image as an input to the system and detected tampered region. The system comprised of segmentation, feature extraction, dense depth reconstruction module and final identification of tampered area was done. Haffemann et al. [5] proposed a model based on meta-learning (learning to learn) for random forgeries which has two levels of learning, namely task level and meta-level.

✉ Agya Ram Verma
arverma06ei03@gmail.com

S. Singh
shivani.singh582@gmail.com

S. Chandra
shantichandra@iiita.ac.in

[1] Department of Electronics and Communication Engineering, IIIT Allahabad, Prayagraj, India

[2] Department of Electronics and Communication Engineering, Govind Ballabh Pant Institute of Engineering and Technology, Pauri, India

Published online: 19 August 2024

Ghosh [6] introduced a deep learning model based on recurrent neural network (RNN) for Object-free Signature Verification (OfSV). The model incorporates various structural and directional features, which are then utilized as inputs for separate RNN models, namely long-short term memory (LSTM) and bidirectional long-short term memory (BLSTM), to perform classification. Another innovation by Ghosh et al. [7] involves the proposal of a spatio-temporal version of a Siamese neural network (ST-SNN). This model is designed to efficiently handle one-shot learning tasks using data that integrates both spatial and temporal information. The achieved performance metrics include a true positive rate (TPR) of 94.63% and a false acceptance rate (FAR) of 4.1%. Hameed et al. [8] reviewed nearly 56 articles and concluded that support vector machine (SVM) in combination with convolutional neural network (CNN) is a popular method used for offline signature verification (OfSV). Further, Foroozandeh et al. [9] used transfer learning which is a reuse of pretrained model on two publicly available datasets of Persian and Latin signatures. The overview of the existing methods discussed above leads to the research findings to fill the research gaps that motivates us to propose an efficient model for OfSV. The following are the contributions of the proposed work: (i) Pre-processing of the signatures is done using different morphological operations which aims to improve the quality and consistency of the signatures. (ii) Different transfer learning models, namely ResNet, VGG-Family and Inception, are deployed over varied datasets for OfSV. (iii) Key metrics in the field of biometrics and security systems are evaluated, namely FAR and FRR which is closely associated with the concept of Type I and Type II errors, respectively.

Data Availability Statement

CEDAR Dataset Data Statement

The CEDAR (Cursive Electronic Dataset and Recognizer), Source: Department of Computer Science and Engineering, Indian Institute of Technology (IIT), Patna, India. Purpose: CEDAR is a benchmark dataset for cursive handwriting recognition research, containing handwritten English characters and digits. Size: The dataset comprises a total of 7800 handwritten samples, including 62 classes (52 English characters and 10 digits). Format: Each sample is provided as a gray-scale image with dimensions 32 × 32 pixels. Collection Method: The dataset was collected by soliciting handwritten samples from multiple participants. Data Attributes: (i) Features: Each sample consists of pixel intensity values representing the handwritten character or digit. (ii) Target Variable: The target variable is the class label corresponding to the handwritten character or digit. Data Availability: Accessibility: The dataset can be downloaded from the official website of the Department of Computer Science and Engineering, IIT Patna.

BHSig260 Dataset Data Statement

The BHSig260 (BioHashing Signature Database), Source: Department of Computer Engineering and Industrial Automation, School of Electrical and Computer Engineering, University of Campinas (UNICAMP), Brazil. Purpose: BHSig260 is a signature database for benchmarking biometric signature verification systems, containing genuine and skilled forgery signatures. Size: The dataset comprises a total of 260 genuine signatures and 260 skilled forgeries, collected from 160 individuals. Format: Each signature is represented as a binary image with variable dimensions. Data Collection: Collection Method: The dataset was collected using a digital tablet, capturing both genuine and forged signatures. Data Attributes: (i) Features: Each sample consists of binary pixel values representing the signature image. (ii) Target Variable: The target variable indicates whether the signature is genuine or a skilled forgery. Data Availability: Accessibility: The dataset can be downloaded from the official website of the Department of Computer Engineering and Industrial Automation, UNICAMP.

Proposed Method

The offline signatures are special types of behavioral biometrics. In the field of biometrics and security systems, OfSV is a challenging task because there is no information of signing process. So, there is a need of a system that distinguishes between genuine and forged signature. A state of the art of different techniques is shown in Table 1. This paper is based on deep transfer learning which is a kind of machine learning technique that uses pretrained model in order to reduce the training time and foremost a reduced dataset is required for the study. Figure 1 shows the flow of the model used for signature verification.

Acquisition of Data

This study uses two datasets, namely CEDAR [16] and BHSig260 [17]. The details are mentioned in Table 2.

Table 1 Literature survey of OfSV

Ref.	Features used	Methods	Datasets	Results	Advantages	Drawbacks
[10]	Histogram of oriented gradients (HOG)	CNN, LSTM, SVM, KNN	UTSig and CEDAR	FAR(%) = 12.5 FRR(%) = 13.8 EER(%) = 12.5	Improved results	Results can be improved by other methods
[11]	Auto-encoders	CNN	Self-Made	FAR(%) = 7.78 FRR(%) = 17.3 Acc(%) = 83.73	More versatile and less overfit	Satisfactory results
[12]	Secure-KNN	KNN	SG-NOTE and MYCT-100	EER-RF = 0.64 EER-SF = 2.67	Faster and secure method of verification	Online verification provides more feature vectors than offline verification
[13]	CSN with triplet loss	Siamese Networks	Self-made	Acc(%) = 84 TL(%) = 49.98	Robustness	Resource intensive
[14]	Time-series warping and dependent warping (EB-DBA)	DTW	(MCYT-100 dataset with five genuine signatures as reference set)	UD Threshold-Yes EER(%) 1.34	(Minor error rate and estimate difficulty)	Complex model
[15]	RNN with gated autoregressive units (GARU) and DTW	RNN	MCYT-100, Mobisig, and e-BioSign	MCYT-100 -1.62% EER - Mobisig -10.87% e-BioSign—6.94%	Explicitly minimize the intra-individual variability and enhance the inter-individual variability	Model inefficient for large dataset and when there is skilled forgeries

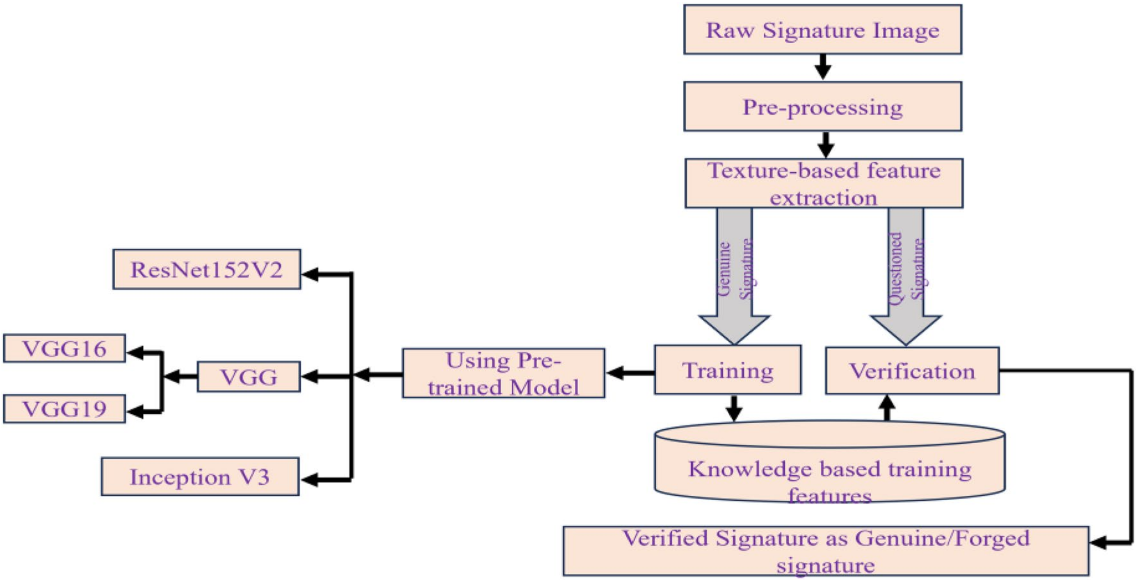

Fig. 1 Flowchart of methodology

Table 2 Description of dataset

Ref	Dataset name	No. of writers	Genuine signatures	Forgeries	Total
[16]	CEDAR	55	24	24	2640
[17]	BHSig 260	260	24	24	12,480

Pre-processing of Signatures

Different filters and functions are used to effectively extract the signature portion for comparison and verification operations. One common operation is noise removal which can be done using denoising algorithms. Signatures are resized to a standardized and uniform size which facilitates batch processing and improves the accuracy of comparison between different signatures.

Training of the Model

The model is trained using transfer learning approach. It is machine learning (ML) procedure in which a model skilled on one mission is adapted to perform a different, but related task. This is accomplished by three main processes, pre-training, feature extraction and fine-tuning. Pre-training is the process of training a model on a large dataset for the source task, which is chosen such that it shares some characteristics with the target task. In the next step, the model captures the universal features and patterns from the source mission. Then, this pretrained model is adapted or fine-tuned to the target task by using a smaller dataset specific to the target task. The model parameters are adjusted to better suit the nuances of the target domain. In this presented work, three pretrained models are used for signature verification named as ResNet152V2, VGG (VGG16 and VGG19) and InceptionV3. ResNet152V2 is an advanced variant of the residual network architecture (ResNet) and is characterized by its deep structure having 152 layers. Figure 2 represents the model architecture of ResNet152V2. It makes use of residual connections, or skip connections, which facilitate the flow of information by circumventing the vanishing gradient problem encountered in training very deep networks. It allows learning intricate patterns and representations across multiple levels of abstraction, making it highly effective for image classification tasks. VGG- The Visual Geometry Group (VGG) architecture was designed for creating a deep neural network capable of learning intricate features from images. Figure 3 represents the VGG model. In VGG, the layers contain 3×3 convolutional filters and it employs a gradual

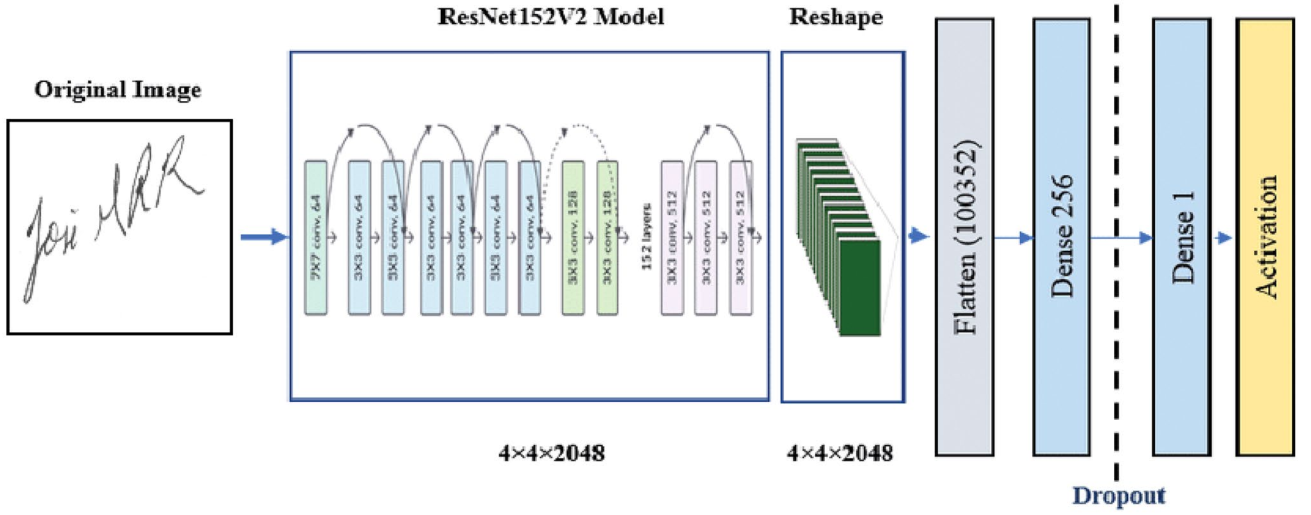

Fig. 2 Model architecture of ResNet152V2

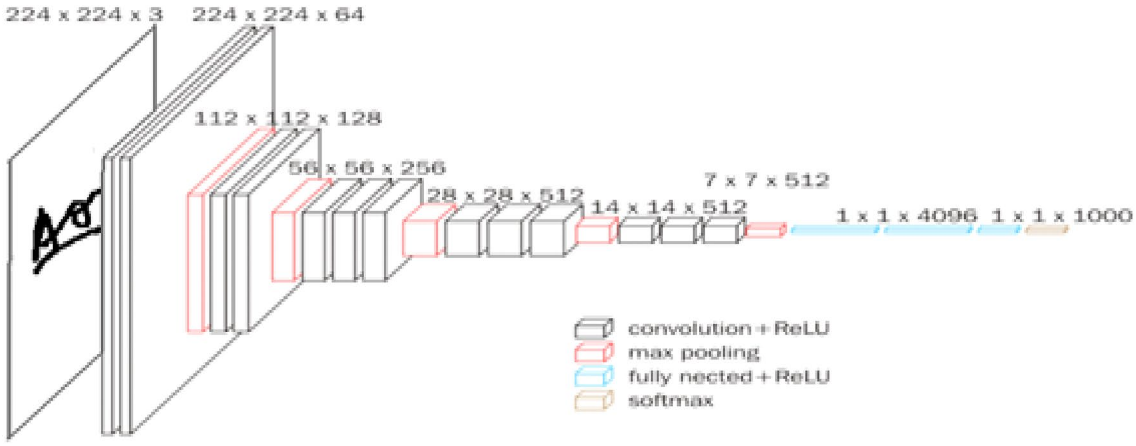

Fig. 3 Model architecture of VGG

Table 3 Tabular difference between VGG16 and VGG19

Layers	VGG16	VGG19
Dimension of layer	41	47
Image input size	224 × 224 pixel	224 × 224 pixel
Convolutional layer	13	16
Filter size	64 and 128	64, 128, 256 and 512
ReLu	5	18
Max-pooling	5	5
FCL	3	3
Dropout	0.5	0.5
Softmax	1	1

increase in filter depth as progressed deeper into the network. The initial layers start with 64 filters and gradually increase to 128, 256, and finally 512 filters. VGG comes in two variants named as VGG16 and VGG19. The differences are listed in Table 3. Inception V3—The modules in this model incorporate a combination of parallel convolutional filters with different dimensions (1 × 1, 3 × 3, and 5 × 5) and max-pooling layers within a single layer which enables it to effectively capture features across various scales and complexities concurrently.

Results of the Transfer Learning Models for OFSV

The pretrained models are analyzed over two different datasets, namely BHSig260 and CEDAR, mentioned above. In the field of biometrics and security systems, the aforementioned metrices are of great importance.

Accuracy—It is a metric that measures how often a trained model predicts the outcome correctly [18].

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{1}$$

False rejection rate (FRR)—It is also called Type I error is denoted by 'α', which gives the possibility of rejection even with a genuine signature.

$$\text{FRR}(\alpha) = \frac{\text{FN}}{\text{TP} + \text{FN}} \tag{2}$$

False acceptance rate (FAR)—It is also called Type II error denoted by 'β' which gives the possibility of acceptance even with the forged signature.

$$\text{FAR}(\beta) = \frac{\text{FP}}{\text{FP} + \text{TN}} \tag{3}$$

where TP, TN, FP and FN are true positives, true negatives, false positives and false negatives, respectively. For a model to be efficient in the field of biometrics, the accuracy should be high and the Type I and Type II error should be minimum. The models are fed with the varied dataset, and the confusion matrix is obtained which shows the no. of correct and incorrect predictions per class. In the next step, the evaluation metrices are calculated and listed in respective tabular format.

a. Results for ResNet152V2 model
b. Results for VGG model

- VGG16
- VGG19

c. Results for inception V3 model

Discussion of the Result

The pretrained models are fed with the varied set of datasets and the confusion matrix is obtained for each of the model for the different datasets, namely BHSig and CEDAR, which

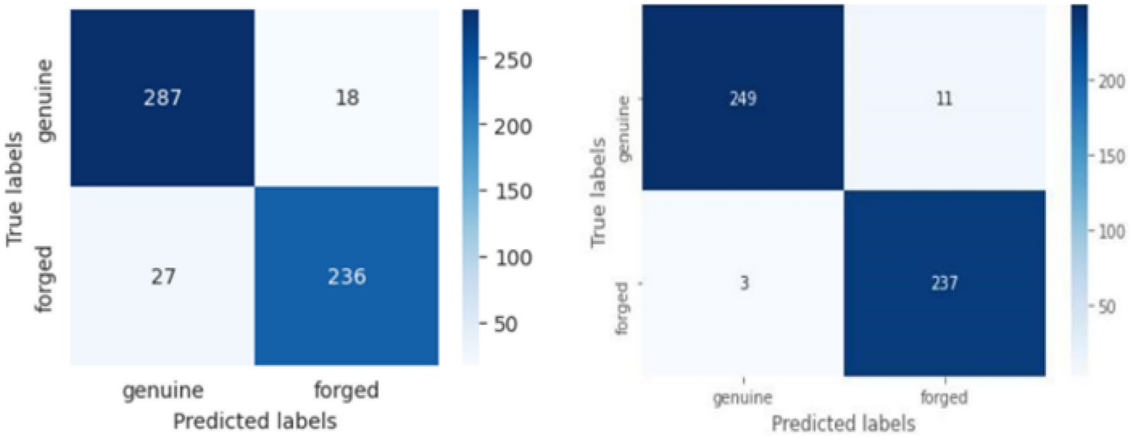

Fig. 4 Confusion matrix for ResNet152V2 over BHSig260 and CEDAR

Table 4 Evaluation metrices for ResNet152V2

Dataset	Accuracy (%)	*α* (%)	*β* (%)
BHSig 260	92.07	8.59	7.08
CEDAR	97.20	1.19	4.43

Table 5 Evaluation metrices for VGG16

Dataset	Accuracy (%)	*α* (%)	*β* (%)
BHSig 260	95.32	4.42	4.97
CEDAR	99.8	4.31	0

Table 6 Evaluation metrices for VGG19

Dataset	Accuracy (%)	*α* (%)	*β* (%)
BHSig 260	95.7	3.4	5.3
CEDAR	100	0	0

Table 7 Evaluation metrices for inceptionV3

Dataset	Accuracy (%)	*α* (%)	*β* (%)
BHSig 260	81.12	15.7	25.31
CEDAR	99.10	1.03	0.74%

is shown in Figs. 4, 7, 10 and 13. Further, the evaluation metrices Accuracy, *α* and *β* are calculated and listed in tabular form for each model in Tables 4, 5, 6 and 7, respectively.

The ResNet152V2 model has an accuracy of 92.07% for BHSig and 97.20% for CEDAR dataset. The values of the Type I error (α) and Type II error (β) which are 1.19% and 4.43% which is very low as compared with BHSig260 dataset, verifying that the ResNet152V2 performs better on CEDAR dataset. The accuracy plot and the loss plot are listed in Figs. 5 and 6. Figure 6 shows high accuracy and low loss which concludes that the model makes a few small errors. Further the study is carried over VGG models, i.e., on VGG16 and VGG19. The VGG16 performs better over CEDAR with 0% of acceptance rate that shows the model does not accepts the forged signatures at all. On the other part, the VGG19 shows 100% accuracy over CEDAR dataset which shows the model predicts the correct label and it has a direct relationship with all the values of confusion matrix or there might be a possibility that the model is overfitted. Inception V3 model shows a drastic change over the two of the datasets. It gives 81.12% over BHSig260 dataset and 99.10% over CEDAR dataset. Also the values of α and β justify that the model gives the low false acceptance and false rejection rate of 0.74% and 1.03%, respectively. For a model to perform good, it should have high accuracy and low false acceptance and low false rejection rate which is clearly justified

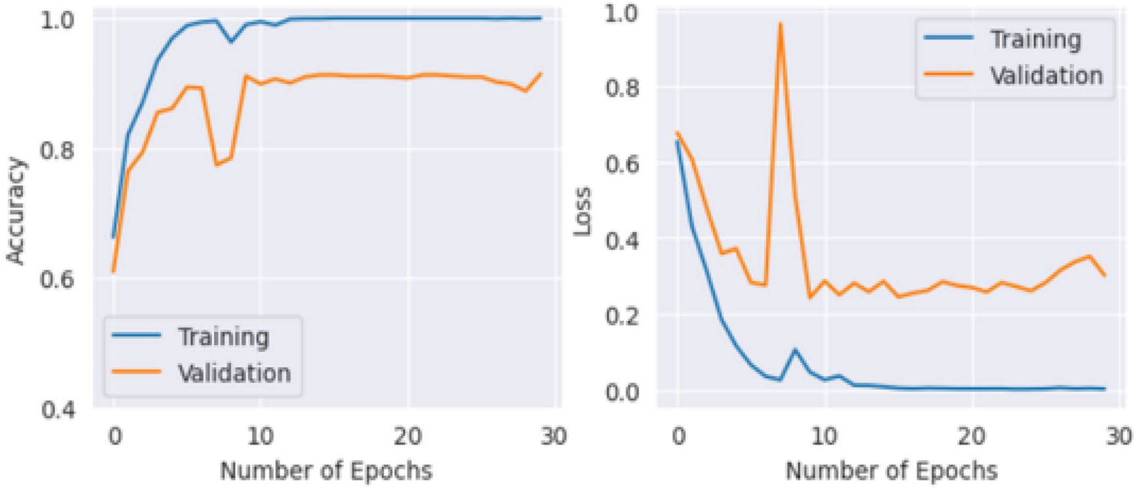

Fig. 5 Accuracy and loss plot of ResNet152V2 over BHSig260

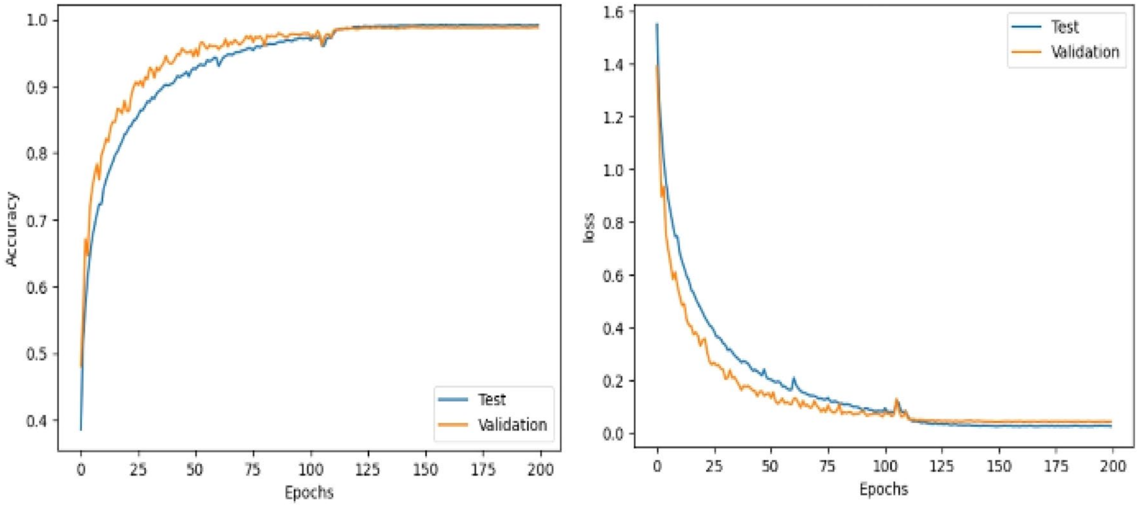

Fig. 6 Accuracy and loss plot of ResNet152V2 over CEDAR

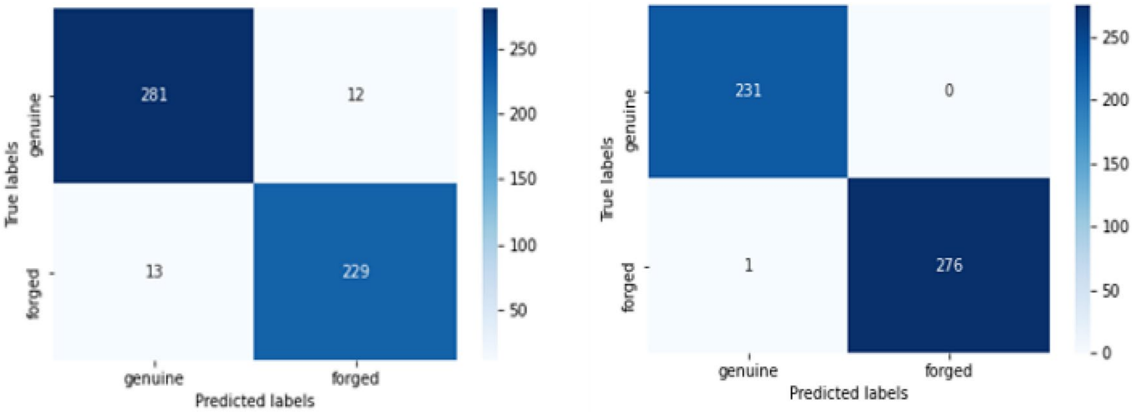

Fig. 7 Confusion matrix for VGG16 over BHSig260 and CEDAR

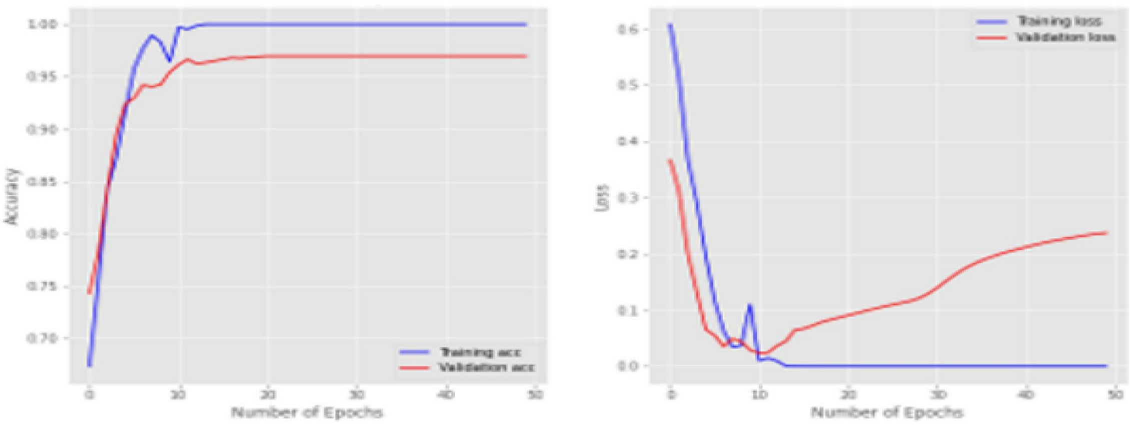

Fig. 8 Accuracy and loss plot of VGG16 over BHSig260

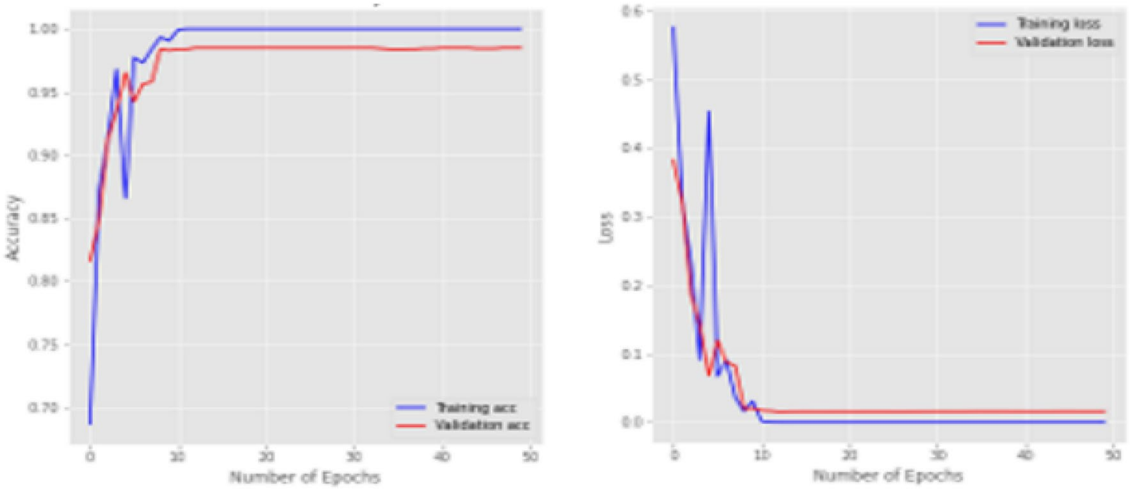

Fig. 9 Accuracy and loss plot of VGG16 over CEDAR

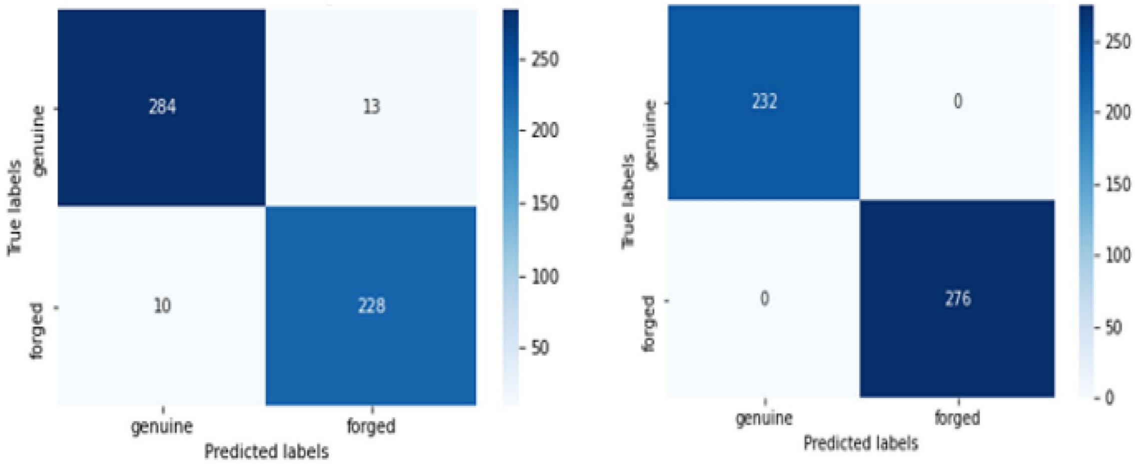

Fig. 10 Confusion matrix for VGG19 over BHSig260 and CEDAR

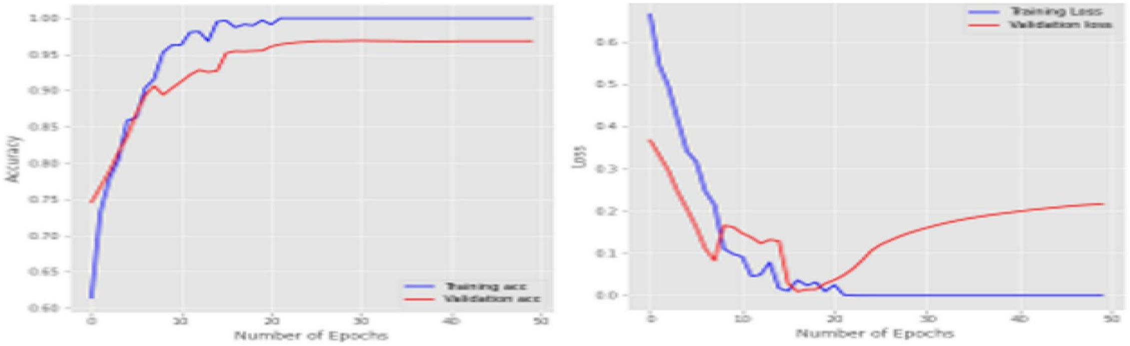

Fig. 11 Accuracy and loss plot of VGG19 over BHSig260

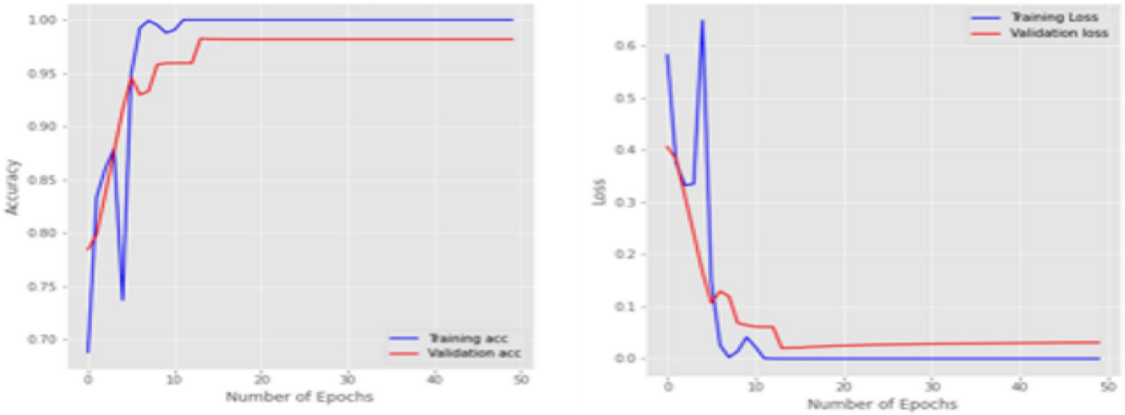

Fig. 12 Accuracy and loss plot of VGG19 over CEDAR

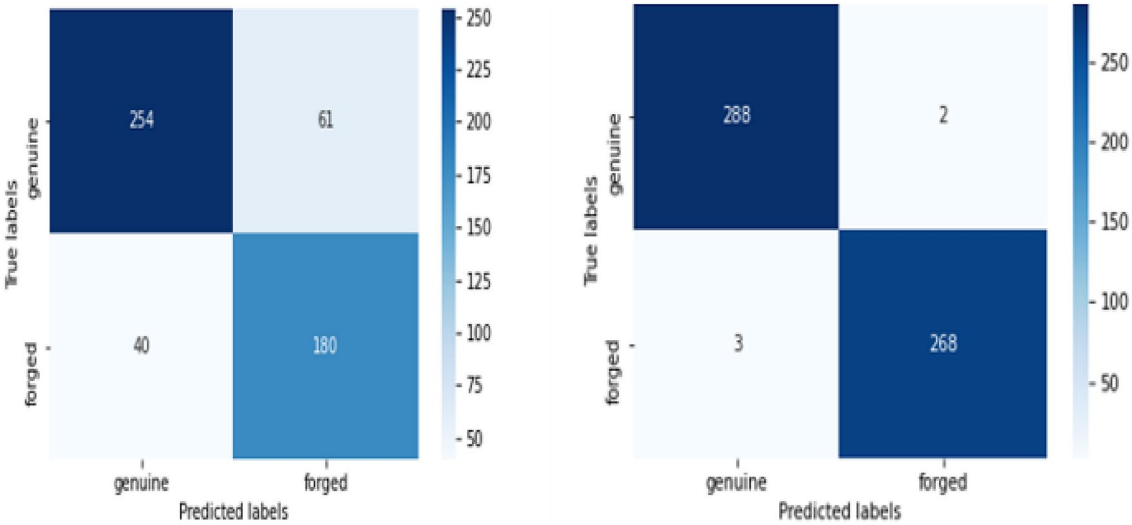

Fig. 13 Confusion matrix for Inception V3 over BHSig260 and CEDAR

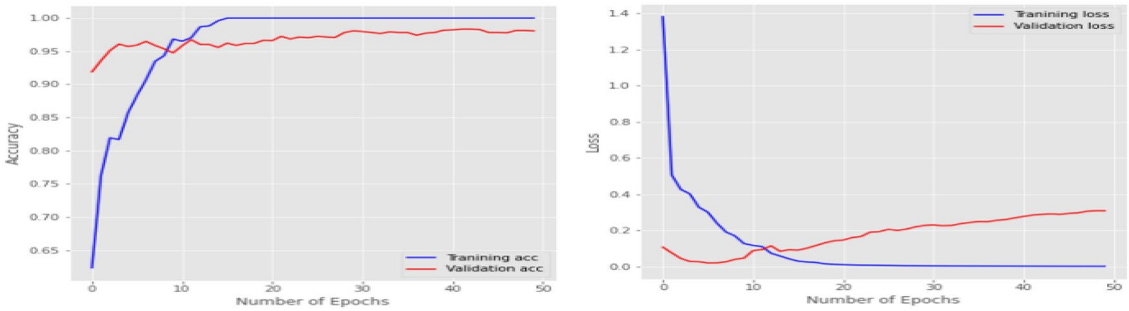

Fig. 14 Accuracy and loss plot of InceptionV3 over BHSig260

by InceptionV3 model over CEDAR dataset (Fig. 7). The performance of methods is plotted in Figs. 8, 9. In this plot, it can be observed that VGG 16 model performs good in terms of accuracy and loss both. Here we have used BHsig260 dataset. In Fig. 9, the CEDAR dataset has been employed; here it can be seen that achieved accuracy

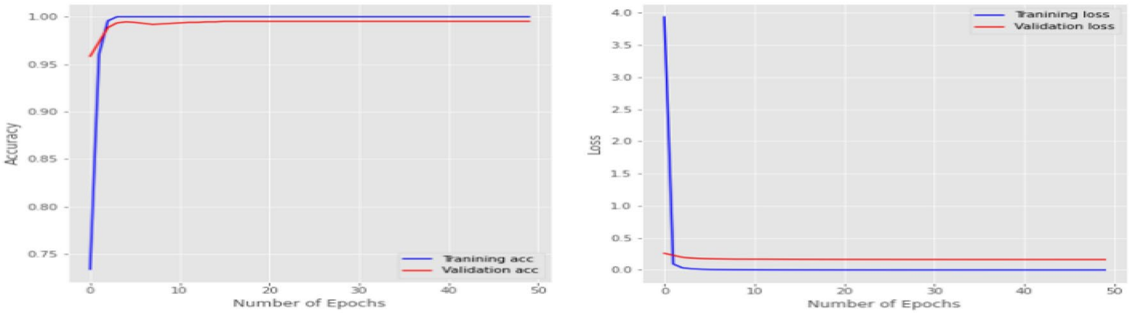

Fig. 15 Accuracy and loss plot of inception V3 over CEDAR

above 99 percent is much before than the BHsig260 dataset. The confusion matrix for both datasets is given in Fig. 10, which shows that CEDAR dataset achieved better classification in comparison to the BHsig dataset. Here, VGG19 model is also used for signature identification; the accuracy and loss graph is given in Figs. 11, 12. In Fig. 11, BHsig dataset is utilized and results abstained by utilized CEDAR dataset are given in Fig. 12. From these figures, it can be seen that VGG19 performs better in case of CEDAR dataset (Fig. 13). Inception V3 network is also utilized in this work, and obtained results are given in Figs. 14 and 15. From Figs. 11, 12, 13, 14 15, it can be seen that Inception V3 provides better results in terms of accuracy and loss both.

Conclusion

The evaluation of pretrained models, specifically ResNet152V2, VGG16, VGG19, and Inception V3, on the BHSig and CEDAR datasets reveals interesting insights into their performance. ResNet152V2 demonstrates commendable accuracy, with 92.07% for BHSig and 97.20% for CEDAR, supported by low Type I and II errors. The accuracy and loss plots further indicate the model's robust performance. VGG16 exhibits remarkable results by achieving a 0% acceptance rate on CEDAR, emphasizing its ability to discern forged signatures effectively. However, VGG19's 100% accuracy on CEDAR raises concerns about potential over-fitting. Inception V3 showcases a significant improvement over both datasets, particularly excelling with 99.10% accuracy on CEDAR. The low values of false acceptance and false rejection rates reinforce the model's proficiency. Overall, these findings underscore the nuanced performance variations among different pretrained models, emphasizing the importance of selecting the most suitable model based on specific dataset characteristics and desired outcomes in signature recognition tasks.

Data Availability The study relied on the data provided in [16, 17].

Declarations

Conflict of interest No conflict of interest.

References

1. Naz S, Bibi K, Ahmad R (2022) DeepSignature: fine-tuned transfer learning based signature verification system. Multimed Tools Appl 81(26):38113–38122
2. Poddar J, Parikh V, Bharti SK (2020) Offline signature recognition and forgery detection using deep learning. Proced Comput Sci 170:610–617
3. Vohra K (2021) Signature verification using support vector machine and convolution neural network. Turk J Comput Math Educ (TURCOMAT) 12(1S):80–89
4. Agarwal R, Verma OP (2020) An efficient copy move forgery detection using deep learning feature extraction and matching algorithm. Multimed Tools Appl 79:7355–7376. https://doi.org/10.1007/s11042-019-08495-z
5. Hafemann LG, Sabourin R, Oliveira LS (2020) Meta-learning for fast classifier adaptation to new users of signature verification systems. IEEE Trans Inf Forensics Secur 15:1735–1745. https://doi.org/10.1109/TIFS.2019.2949425
6. Ghosh R (2021) A recurrent neural network based deep learning model for offline signature verification and recognition system. Expert Syst Appl 168:114249
7. Ghosh S, Ghosh S, Kumar P, Scheme E, Roy PP (2021) A novel spatio-temporal Siamese network for 3D signature recognition. Pattern Recogn Lett 144:13–20
8. Hameed MM, Ahmad R, Kiah MLM, Murtaza G (2021) Machine learning-based offline signature verification systems: a systematic review. Signal Process: Image Commun 93:116139
9. Foroozandeh A, Hemmat AA, Rabbani H (2020). Offline handwritten signature verification and recognition based on deep transfer learning. In 2020 International conference on machine vision and image processing (MVIP) (pp. 1–7). IEEE

10. Alsuhimat FM, Mohamad FS (2023) A hybrid method of feature extraction for signatures verification using CNN and HOG a multi-classification approach. IEEE Access 11:21873–21882
11. Prajapati PR, Poudel S, Baduwal M, Burlakoti S, Panday SP (2021) Signature verification using convolutional neural network and autoencoder. J Inst Eng 16(1):33
12. Xia Z, Shi T, Xiong NN, Sun X, Jeon B (2018) A privacy-preserving handwritten signature verification method using combinational features and secure kNN. IEEE Access 6:46695–46705
13. Mshir S, Kaya M (2020). Signature recognition using machine learning. In 2020 8th International symposium on digital forensics and security (ISDFS) (pp. 1–4). IEEE
14. Okawa M (2019) Template matching using time-series averaging and DTW with dependent warping for online signature verification. IEEE Access 7:81010–81019
15. Lai S, Jin L, Yang W (2017). Online signature verification using recurrent neural network and length-normalized path signature descriptor. In 2017 14th IAPR international conference on document analysis and recognition (ICDAR) (Vol. 1, pp. 400–405). IEEE
16. CEDAR Signature Dataset | Papers With Code
17. Handwritten Signature Datasets (kaggle.com)
18. Verma AR, Chandra S, Singh GK et al (2023) ECG data compression using of empirical wavelet transform for telemedicine and e-healthcare systems. Augment Hum Res 8:2. https://doi.org/10.1007/s41133-023-00063-3

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.