

---

# Offline-Signature Verification System using Transfer Learning VGG-19

---

Kazi Tanvir<sup>1\*</sup>, Saidul Mursalin Khan<sup>2</sup>, Al-Jobair Ibna Ataur<sup>3</sup>, Shaikh Allahma Galib<sup>4</sup>

<sup>1\*,2,3,4</sup>Department of Computer Science, American International University  
Bangladesh(AIUB), Kuratoli, Dhaka, Bangladesh.

Email: <sup>2</sup>saidulmursalinkhan@gmail.com, <sup>3</sup>ajibnaaraaurbd@gmail.com,  
<sup>4</sup>shaikhallahmagalib.bd@gmail.com  
Corresponding Email: <sup>1\*</sup>kazitanvir.ai@gmail.com

Received: 03 June 2022

Accepted: 20 August 2022

Published: 29 September 2022

**Abstract:** Nowadays, Signature verification is one of the most common and effective biometric systems that used to recognize people in many institutions. In modern era of technology, advanced neural networks have provided us an option to solve this issue. In this study, The Robinreni Signature Dataset was utilized to classify the signatures of 64 people, each of whom had 64 original signatures and 64 fake signatures. One of the most popular CNN architecture, namely, VGG19, were used. Firstly, the dataset was distributed accordingly 1649 and 500 for training and validation. Secondly, preprocess the data to train the model. After that the model training process is started using transfer learning approach. Obtained experimental results that VGG19 is best suited for datasets with a validation accuracy of 98.79%.. Everyone has their own unique signature that used to identify and verify important documents and legal transactions. Our study shows the effectiveness of VGG19 for Signature Verification task. The findings will aid in the development of more effective Deep Learning-based signature verification methods.

**Keywords:** Transfer Learning, Signature Verification, VGG-19, Forgery Detection.

## 1. INTRODUCTION

A signature is defined as a distinctively crafted script that an individual inscribes onto various documents to establish their identity. This personalized mark is commonly employed whenever a person needs to endorse a check, a legal document, a contract, and so forth [1]. The issue arises when someone attempts to forge it. The signature of an individual portrays an image that represents a specific arrangement of pixels which holds significance for that particular individual [2]. Signature verification is essential due to the requirement of guaranteeing the genuineness and completeness of documents or transactions [3]. This



process entails validating that the given signature corresponds to the authentic one linked to an individual, thereby thwarting fraud, unauthorized entry, and deceit [4]. The verification of signatures plays a pivotal role in upholding the safety and legitimacy of legal, monetary, and individual affairs [5]. Signatures embody a distinct style of script in which distinct characters flourish and are viable [6]. The procedure of verifying signatures entails intricate pattern recognition, a process that has a constraint since it's impossible for two genuine signatures of an individual to be completely indistinguishable [7].

## **Related Works**

### **Offline Signature Verification Systems**

Numerous techniques have been introduced and effectively employed to determine whether a signature is authentic or counterfeit [8]. The application of Dynamic Time Warping (DTW), an algorithm designed to assess similarity between two sequential data sets, is employed to differentiate between legitimate and falsified handwritten signatures. Additionally, Neural Networks (NNs) have been harnessed for the validation of offline signatures, leveraging their capacity for autonomous learning of distinctive characteristics [9]. Shahane et al. [2] employed a technique for implementation that involves the utilization of varied thresholds for comparison, aimed at enhancing the overall effectiveness of the system. This approach also encompasses the validation of both the account number and the amount on the check through Optical Character Recognition (OCR), determining whether the check has been successfully processed or rejected. However, the specific threshold values employed in this context were not universally applicable to all types of signatures, as these values varied across signatures from different individuals. Zhu et al. [10] employed an implementation strategy involving a sophisticated structural framework to collectively identify and extract signatures from document images through a structural analysis detection process across varying image scales. Jahandad et al. [8] utilized two well-known CNN architectures, Inception-v1 and Inception-v3, achieving validation accuracy rates of 83% and 75% respectively after training on samples from 20 users; Inception-v1 demonstrated a particularly low Equal Error Rate (EER) of 17, surpassing Inception-v3's EER of 24, despite Inception-v3's superior performance in ImageNet classification, with Inception-v1 also boasting faster training due to its lower computational load. Umar et al. [11] introduce a high-performance embedded system designed for verifying offline Urdu handwritten signatures, addressing the absence of Urdu datasets; their approach involves creating a unique dataset, employing an embedded system to differentiate authentic and forged signatures based on diverse attributes, and utilizing a majority voting algorithm to enhance the system's accuracy, with the proposed method achieving an overall accuracy of 95.13%, further tested on an English signature dataset to yield a 97.46% accuracy. Ryan et al. [12] present an approach to streamline signature verification through signature preprocessing, coupled with an innovative deep learning technique for identifying counterfeit signatures, achieving a detection accuracy range of 85-95%.

This paper aims to propose a deep learning model using VGG-19 by transfer learning method. The subsequent sections of the document are outlined as follows: Section 2 elucidates the research methodology, Section 3 deliberates on the research outcomes and

discoveries, and Section 4 concludes by summarizing the entire study and suggesting potential avenues for future endeavours.

## 2. METHODOLOGY

### Proposed Model

The model used in this research is VGG-19 by transfer learning method. VGG-19 stands out as a convolutional neural network design distinguished by its profound structure, comprising 19 layers that encompass both convolutional and fully connected layers. It garnered recognition in the realm of computer vision assignments and image classification contests due to its uncomplicated yet impressive performance [13]. The distinctive trait of the VGG-19 architecture lies in its employment of compact 3x3 convolutional filters, arranged sequentially, which enhances its capability to grasp intricate attributes within images [14].

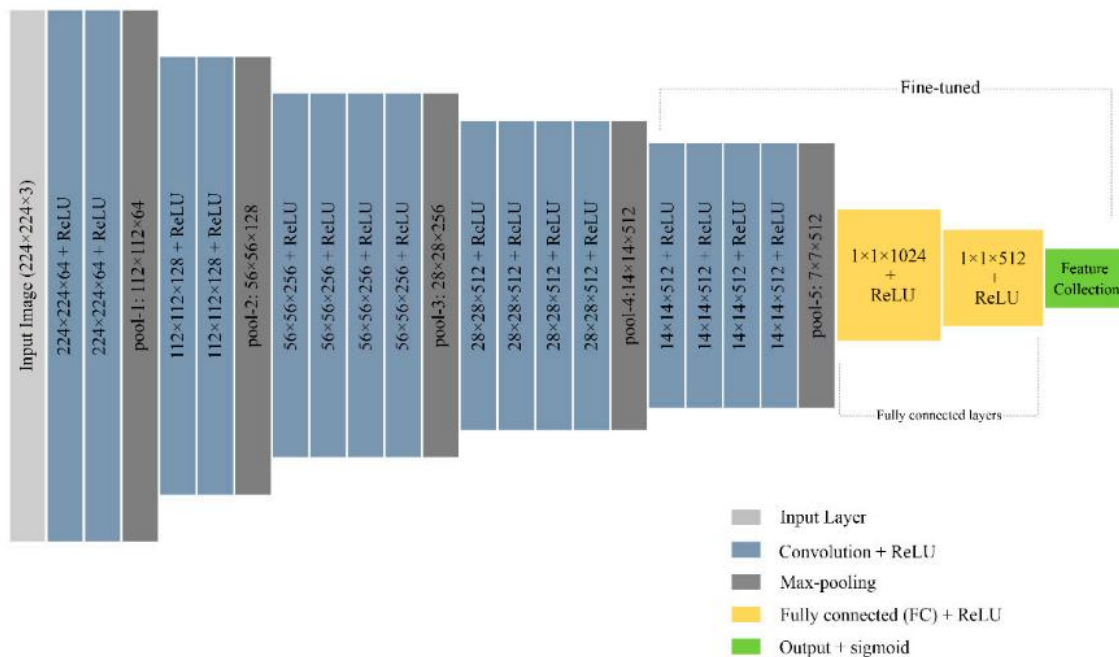


Fig. 1 Fine-tuned VGG19 pre-trained CNN model[15]

Transfer learning constitutes a machine learning strategy that entails utilizing insights obtained from training a model on one assignment and employing it for a correlated task [16]. This technique is notably advantageous in fields such as computer vision and natural language processing, where deep learning models can be refined to match particular problem domains without commencing training anew [17].

The input shape for the model was 224x224x3 which means that the image size is 224x224 and the input is 3 channelled or the colour is RGB. A dense layer with input shape (None, 2) and 6,423,298 parameters whose activation function was softmax [18] was added to get the output.

Table 1: Hyperparameters for Compiling the Model

Hyperparameters	Values
Loss	Categorical Crossentropy [19]
Optimizer	Adam (Learning Rate = 0.0001) [20]
Metrics	Accuracy
Batch Size	32

**Dataset**

The dataset used in this paper is a public dataset from Kaggle called the Robinreni Signature Verification Dataset [21]. It contains signatures from 64 persons. From one person 12 signatures were taken and the same number of signatures were forged. In total there are 2149 images divided in training and testing where there are 1649 images for training and 500 images for testing. The training images were split for validation purposes which gave 1320 images for training and 329 images for validation.

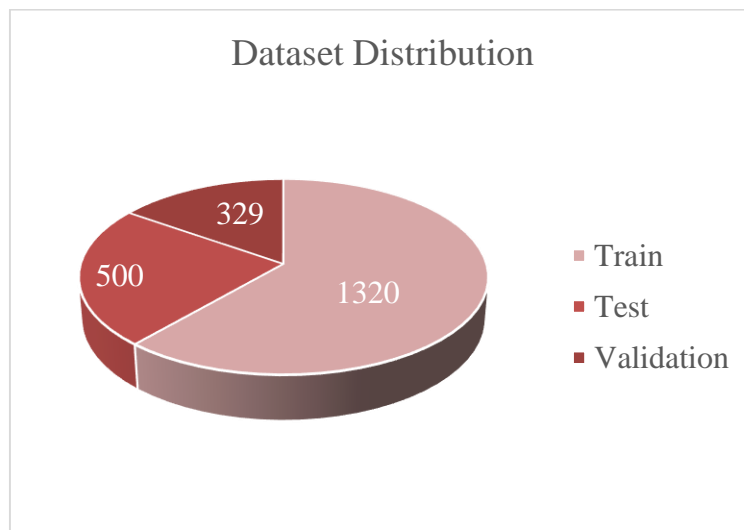


Fig. 2 Dataset Distribution

**Training the Model**

The model was trained on the google colaboratory platform which has 12.7 GB of System RAM and 15 GB GPU RAM [22]. The callback that was used during fitting the model is early stopping [23] which monitored the validation loss for 3 epochs and if there was no improvement then it would stop the training phase. The number of epochs that were set for the training phase was 10 epochs.

**3. RESULTS AND FINDINGS**

After 4 epochs with learning rate 0.0001, the model stopped training with training accuracy of 99.20% and loss of 4.72%. The validation accuracy after the said number of epochs was 98.79% and loss was 9.42%. The perceived test accuracy for the model was 98.8%. The training and validation curve is as follows:

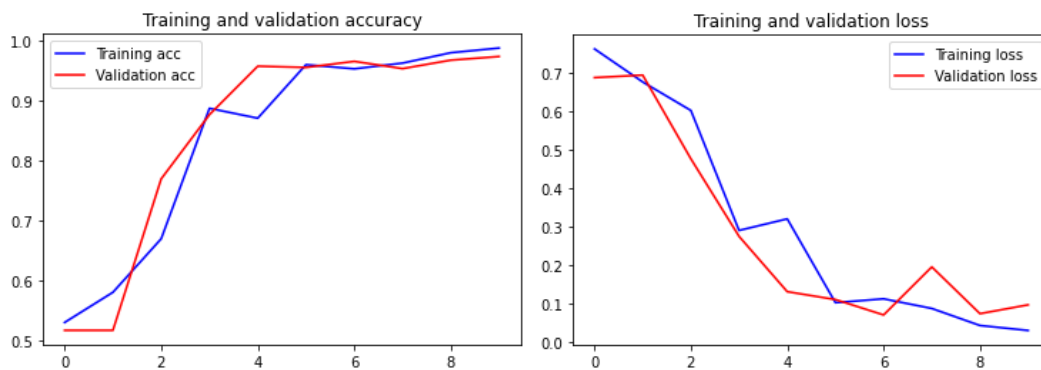


Fig. 3 Training and Validation Curve

A confusion matrix serves as a structured display that concisely captures the outcomes of a classification model, presenting the tallies of true positives, true negatives, false positives, and false negatives, thereby revealing the model's precision and error allocation across distinct categories [24]. This tool holds significant utility in appraising model performance and pinpointing prospects for enhancement within classification tasks in machine learning.

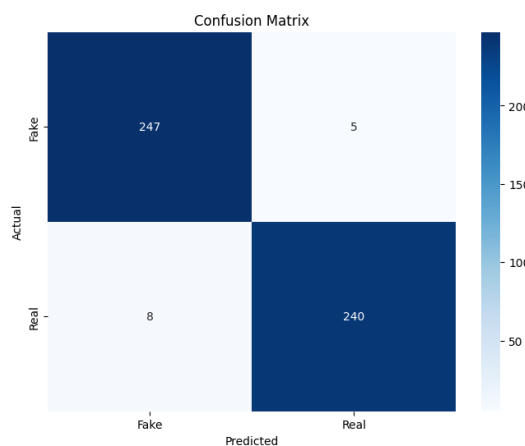


Fig. 4 Confusion Matrix for the proposed model

Precision, within the context of machine learning assessment, serves as a metric to gauge the correctness of affirmative predictions rendered by a model, revealing the ratio of accurately recognized positive cases relative to the entirety of instances classified as positive [25]. Conversely, recall, alternatively referred to as sensitivity or the true positive rate, assesses the model's capacity to encompass all factual positive instances by evaluating the proportion of accurate positive predictions in relation to the complete count of genuine positive instances [25]. The precision and recall value for the proposed model is 0.98 and 0.97 respectively. The F1-score functions as a comprehensive measure within machine learning, harmonizing precision and recall, and providing a cohesive evaluation of a model's binary classification performance [26]. The f1-score of the mentioned model is 0.97. The precision, recall and f1-score shows that the proposed model performs significantly on the stated dataset.



#### 4. CONCLUSIONS

In conclusion, this study introduced a Transfer Learning-based Offline-Signature Verification System utilizing the VGG-19 architecture. The experimental outcomes emphasized the model's impressive aptitude for discerning authentic and forged signatures. With only 4 epochs and a controlled learning rate of 0.0001, the model demonstrated remarkable competency, achieving a notable training accuracy of 99.20% and a convergent training loss of 4.72%. Moreover, the validation phase reinforced the model's capacity for generalization, evidenced by a commendable validation accuracy of 98.79%. This outcome attested to the model's ability to accurately classify previously unseen signature samples, while the validation loss of 9.42% indicated successful avoidance of overfitting. The assessment metrics further affirm the model's efficacy. Boasting a precision rate of 0.98, the model demonstrates its skill in mitigating false positives, while a recall figure of 0.97 underscores its proficiency in identifying true positives. The exceptional f1-score of 0.97 amalgamates precision and recall, underscoring the overall effectiveness of the suggested model in authenticating signatures. In conclusion, this investigation effectively illustrates the capabilities of the Offline-Signature Verification System through Transfer Learning utilizing the VGG-19 architecture. The attained notable accuracy, precision, recall, and f1-score collectively substantiate the model's capacity to accurately differentiate genuine and counterfeit signatures, thereby not only showcasing its potential in signature validation but also highlighting the broader applicability of transfer learning in intricate recognition assignments. Future endeavors might delve into additional optimization techniques and expanded datasets to further elevate the model's performance and resilience.

#### 5. REFERENCES

1. "signature," Aug. 16, 2023.
2. <https://dictionary.cambridge.org/dictionary/english/signature> (accessed Aug. 23, 2023).
3. J. Poddar, V. Parikh, and S. K. Bharti, "Offline Signature Recognition and Forgery Detection using Deep Learning," *Procedia Comput. Sci.*, vol. 170, pp. 610–617, Jan. 2020, doi: 10.1016/j.procs.2020.03.133.
4. H. al Suwaidi, "Signature Verification: Safeguarding Legal Documents in UAE," *Notary Public Dubai*, Jun. 26, 2023. <https://notarypublicdubai.com/signature-verification-uae/> (accessed Aug. 23, 2023).
5. "Fraud and Identity Theft Issues: Security & Forensics Book Chapter | IGI Global." <https://www.igi-global.com/chapter/content/63093> (accessed Aug. 23, 2023).
6. "Contested compliance regimes in global production networks: Insights from the Bangladesh garment industry - Fahreen Alamgir, Subhabrata Bobby Banerjee, 2019." <https://journals.sagepub.com/doi/abs/10.1177/0018726718760150> (accessed Aug. 23, 2023).
7. D. N. Shalin, "Signing in the Flesh: Notes on Pragmatist Hermeneutics," *Sociol. Theory*, vol. 25, no. 3, pp. 193–224, Sep. 2007, doi: 10.1111/j.1467-9558.2007.00305.x.
8. C. Belley, S. Gaboury, B. Bouchard, and A. Bouzouane, "An efficient and inexpensive method for activity recognition within a smart home based on load signatures of



- appliances,” *Pervasive Mob. Comput.*, vol. 12, pp. 58–78, Jun. 2014, doi: 10.1016/j.pmcj.2013.02.002.
9. Jahandad, S. M. Sam, K. Kamardin, N. N. Amir Sjarif, and N. Mohamed, “Offline Signature Verification using Deep Learning Convolutional Neural Network (CNN) Architectures GoogLeNet Inception-v1 and Inception-v3,” *Procedia Comput. Sci.*, vol. 161, pp. 475–483, Jan. 2019, doi: 10.1016/j.procs.2019.11.147.
  10. S. Inglis and I. H. Witten, “Compression-based template matching,” in *Proceedings of IEEE Data Compression Conference (DCC’94)*, IEEE, 1994, pp. 106–115.
  11. Guangyu Zhu, Yefeng Zheng, D. Doermann, and S. Jaeger, “Signature Detection and Matching for Document Image Retrieval,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 31, no. 11, pp. 2015–2031, Nov. 2009, doi: 10.1109/TPAMI.2008.237.
  12. U. Tariq, Z. Hu, R. Tariq, M. S. Iqbal, and M. Sadiq, “High-Performance Embedded System for Offline Signature Verification Problem Using Machine Learning,” *Electronics*, vol. 12, no. 5, Art. no. 5, Jan. 2023, doi: 10.3390/electronics12051243.
  13. R. C. Reyes, M. J. Polinar, R. M. Dasalla, G. S. Zapanta, M. P. Melegrito, and R. R. Maaliw, “Computer Vision-Based Signature Forgery Detection System Using Deep Learning: A Supervised Learning Approach,” in *2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, Jul. 2022, pp. 1–6. doi: 10.1109/CONECCT55679.2022.9865776.
  14. K. Simonyan and A. Zisserman, “Very Deep Convolutional Networks for Large-Scale Image Recognition.” *arXiv*, Apr. 10, 2015. doi: 10.48550/arXiv.1409.1556.
  15. L. Alzubaidi et al., “Review of deep learning: concepts, CNN architectures, challenges, applications, future directions,” *J. Big Data*, vol. 8, no. 1, p. 53, 2021, doi: 10.1186/s40537-021-00444-8.
  16. R. Mostafiz, M. M. Rahman, A. K. M. K. Islam, and S. Belkasim, “Focal Liver Lesion Detection in Ultrasound Image Using Deep Feature Fusions and Super Resolution,” *Mach. Learn. Knowl. Extr.*, vol. 2, no. 3, Art. no. 3, Sep. 2020, doi: 10.3390/make2030010.
  17. A Gentle Introduction to Transfer Learning for Deep Learning - *MachineLearningMastery.com*.” <https://machinelearningmastery.com/transfer-learning-for-deep-learning/> (accessed Aug. 23, 2023).
  18. M. Tsiakmaki, G. Kostopoulos, S. Kotsiantis, and O. Ragos, “Transfer Learning from Deep Neural Networks for Predicting Student Performance,” *Appl. Sci.*, vol. 10, p. 2145, Mar. 2020, doi: 10.3390/app10062145.
  19. J. Brownlee, “Softmax Activation Function with Python,” *MachineLearningMastery.com*, Oct. 18, 2020. <https://machinelearningmastery.com/softmax-activation-function-with-python/> (accessed Aug. 23, 2023).
  20. “tf.keras.losses.CategoricalCrossentropy | TensorFlow v2.13.0.” [https://www.tensorflow.org/api\\_docs/python/tf/keras/losses/CategoricalCrossentropy](https://www.tensorflow.org/api_docs/python/tf/keras/losses/CategoricalCrossentropy) (accessed Aug. 23, 2023).
  21. J. Brownlee, “Gentle Introduction to the Adam Optimization Algorithm for Deep Learning,” *MachineLearningMastery.com*, Jul. 02, 2017.



- <https://machinelearningmastery.com/adam-optimization-algorithm-for-deep-learning/> (accessed Aug. 23, 2023).
22. “Signature\_Verification\_Dataset.”  
<https://www.kaggle.com/datasets/robinreni/signature-verification-dataset> (accessed Aug. 23, 2023).
  23. “colab.google,” colab.google. <http://0.0.0.0:8080/> (accessed Aug. 23, 2023).
  24. “tf.keras.callbacks.EarlyStopping | TensorFlowv2.13.0.”  
[https://www.tensorflow.org/api\\_docs/python/tf/keras/callbacks/EarlyStopping](https://www.tensorflow.org/api_docs/python/tf/keras/callbacks/EarlyStopping) (accessed Aug. 23, 2023).
  25. “Confusion Matrix - an overview | Science Direct Topics.”  
<https://www.sciencedirect.com/topics/engineering/confusion-matrix> (accessed Aug. 23, 2023).
  26. “Classification: Precision and Recall | Machine Learning | Google for Developers.”  
<https://developers.google.com/machine-learning/crash-course/classification/precision-and-recall> (accessed Aug. 14, 2023).
  27. “sklearn.metrics.f1\_score,” scikit-learn. [https://scikit-learn/stable/modules/generated/sklearn.metrics.f1\\_score.html](https://scikit-learn/stable/modules/generated/sklearn.metrics.f1_score.html) (accessed Aug. 23, 2023).