International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

SigVerify: A Deep Learning Framework for Signature Authentication and Computerised Forgery Detection

K.Satish Kumar
Associate Professor
Department of CSE-AIML
Geethanjali College of Engineering and Technology
Hyderabad, India
ksatishkumar.cse@gcet.edu.in

B.Venugopal
Final Year
Department of CSE-AIML
Geethanjali College of Engineering and Technology
Hyderabad, India
22r11a66e9@gcet.edu.in

G.Akshitha Reddy
Final Year
Department of CSE-AIML
Geethanjali College of Engineering and Technology
Hyderabad, India
22r11a66g6@gcet.edu.in

SL.Pradeep Reddy
Final Year
Department of CSE-AIML
Geethanjali College of Engineering and Technology
Hyderabad, India
22r11a66j8@gcet.edu.in

Abstract : Verification of offline signatures is still a difficult problem to match because of the lack of dynamic writing of information that is clubbed together like pen pressure and stroke order. Because of this, authentication would be wholly based on visual properties, and thus there would be a hard time to tell an authentic signature and one that has been well made forgery.

The work introduces a deep-layered approach to enhancement of reliability of the potential application of the methods of the authentication of the statical signature. There are two levels of structure in the system. The initial step revolves around detection of digitally produced or distorted signatures in the form of a convolutional model trained to detect irregular texture and structural features. The second phase conducts specific comparison between signatures based on the use of a Siamese network, which considers the similarity based on the encoded feature representations.

In order to enhance interpretability, a visual comparison mechanism is integrated to accentuate the discrepancy of reference and test signature to enable better comprehension of the mismatch areas. The system is also trained and tested on several class signature data where the system performs consistently when differentiating real and fake samples with different writing patterns.

Keywords: Deep Learning, Signature similarity analysis, Forgery detection, Biometric authentication, Image Processing, Feature extraction, Signature similarity analysis, Visual discrepancy analysis, Signature similarity analysis, Convolutional neural networks

1. INTRODUCTION

Handwritten signatures are commonly known to be a well-known and comfortable way of personal authentication socially and practically. They have been applied in various areas including banking, legal documents and administrative procedures to authenticate identity and validate transactions. Signatures are easy and convenient to use but they have become open to abuse, particularly as more sophisticated tools

The traditional methods of signature verification are mainly based on manual checks. In these processes, the identified persons visually match a questioned signature to a known reference, after the training. Despite its effectiveness in certain situations, this process can be subjective and can give inconsistent decisions because of variations in human judgment, fatigue, experience, etc. The challenge is heightened when it comes to the expertise of forgeries that are very much similar to the true signatures.

The task is also drawn more in offline signature verification systems where all that can be analyzed are just the static pictures. In contrast to online verification techniques, where such dynamic properties of handwriting can be recorded (speed of writing, pressure, sequence of strokes, etc.), in offline a system has to rely solely on visual and structural characteristics. Nevertheless, in true signatures, natural differences may occur because of variations in the conditions of writing, emotional status or instruments of writing. The line between these natural variation and forgery with an intent to do it is a complex issue.

In the progress of artificial intelligence, and especially deep learning and computer vision, the focus on automated methods towards tackling these tasks has become quite important. Deep learning models possess the ability to learn rich feature representations directly on raw images which imply that these models are able to extract subtle patterns in that structure that are hard to learn manually. The latter enables them to analyze handwritten signatures and detect irregularities.

A multi-stage signature verification framework is created in this work to strive to improve the accuracy and reliability. The system then analyses the digital signature of a signature as either a digital generated signature or alternatively, a manipulated signature using a convolution-based model. Genuine handwritten samples are then compared to a detente process by a Siamese neural network, which compares the similarity in terms of learned feature embeddings. This isolation of detection and verification makes the system respond better to the various forms of forgery.

Also, a visual comparison system is incorporated to bring a perspective about the differences in signatures by indicating areas of dissimilarity. This not only enhances automated decision-making but also elevates the level of interpretability to the user. The proposed method will provide a viable solution to secure and efficient signature authentication in its real world

implementation by integrating the method of deep learning with structured preprocessing and data handling.

II. RELATED WORK

TOffline signature verification has developed greatly, with less reliance on the traditional handcrafted feature-based techniques to more state-of-the-art machine learning or deep learning models. In the previous methods, features like texture descriptors, geometric measurements, and gradient-based representations were the main features that needed to be designed manually. These procedures, though capable of capturing some structural aspects of signatures, could be very ineffective with competent forgeries as they could not reproduce fine differences in handwriting.

As machine learning progressed, a number of studies investigated classification-based methods on algorithms like Support Vector Machines and k-Nearest Neighbors. These models enhanced the accuracy of verification to an extent by learning the boundary of decision by learning the extracted features. Nevertheless, they were limited in terms of feature engineering-quality, which limited their flexibility to various datasets and writing styles. Detailed analysis of these systems indicates that the extraction of features, pre-processing methods, and heterogeneity of the data set are important factors that define the overall performance .

The deep learning methods have become salient in the past few years owing to their ability to be trained directly on raw signature images to learn feature representations. Convolutional Neural Networks (CNNs) have been popularly used in this direction, since hierarchical features, including edges, stroke patterns, and spatial structures, can be automatically detailed by CNNs. Such models have demonstrated better generalization over their more traditional counterparts, particularly when dealing with large-scale datasets where there are enough training samples. Nonetheless, CNN-based classification models tend to consider signature verification as a conventional image classification task which might be inadequate to reflect the slight variations between authentic signatures and professional forgeries.

Availability of similarity-based learning methods has been proposed as a solution to this shortcoming, specifically by using Siamese Neural Networks. These architectures have two subnetworks that are shared with shared parameters that learn to measure the similarity of two input signatures. The model does not have pre-defined classes, but rather assesses the likelihood of two signatures to be written by the same writer by calculating a distance measure in the feature space []. This method is particularly convenient in practical case where new users might not be represented in the training data.

This has been enhanced by the use of one-shot learning methods within the Siamese architectures enabling the system to be used in verification with fewer signature examples. Experimental investigations have shown such methods are able to attain high verification accuracy on various benchmark data sets with less reliance on large labeled data sets . Moreover, hybrid architectures integrating CNN-based feature extraction with Siamese similarity learning have been suggested in order to exploit the merits of such methods as classification and comparison-based.

Regardless of these developments, there are a number of challenges. A key problem is that due to the nature of real signatures, they can vary because of the conditions under which they are written, the state of emotion or the writing tools used. The other problem is that it is not easy to identify experienced forgeries that are very similar to authentic signatures. In addition, the unbalanced samples of real and falsified samples in the datasets may adversely impact the model performance. Recent research has made efforts to resolve these problems with the use of introducing multi-stage architectures and improved loss functions in order to capture discriminative features more effectively.

Analysis of the available literature shows that although deep learning has enhanced offline signature verification, there is a requirement of a system that will combine effective forgery detection with efficient similarity-based verification. This encourages the creation of hybrid designs, which combine several models to enhance both the precision and practicality..

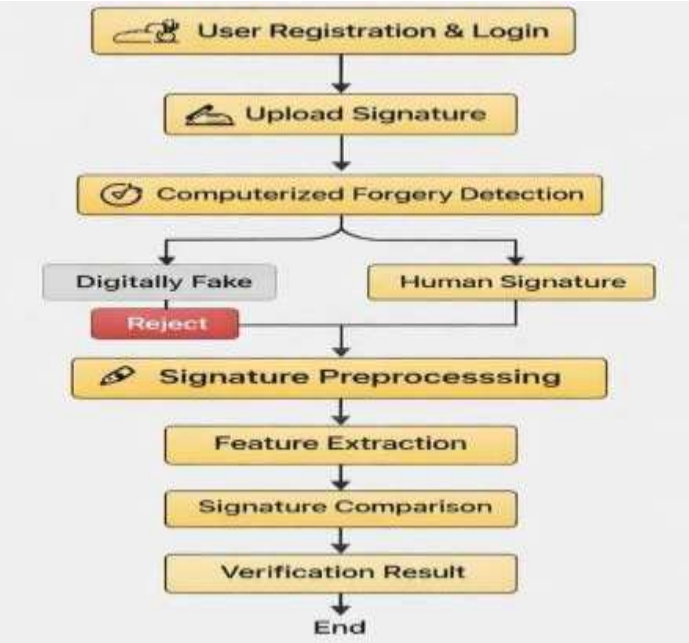
III. Proposed System

The suggested system takes a systematic multi-phase conceptual strategy of enhancing the efficiency of verifying the offline signature. Processing is initiated by the preprocessing of the input signature image to a standardized format, which is done by grayscale conversion, normalization and resizing. These measures serve to minimize noise and applicability of input samples. After its preprocessing, a preliminary screening process is used to determine whether the signature is man-made or manipulated. At this stage, a deep learning model is used, which can identify unnatural patterns and irregularities which are not normal in handwritten signatures and hence filter invalid inputs first before further processing.

Once an initial validation has been made, a more in-depth verification process is carried out on the signature, which relies on similarity learning. A Siamese neural network is used to match the input signature against a stored reference sample by the identities of feature representations and calculating the distance between them. This enables the system to weigh the similarity between two signatures and also tolerates the natural differences in writing. Moreover, a visual contrast mechanism can be used, which will bring out comparisons between signatures, enhancing the readability of the findings. The system offers a valid and practical solution to the practical realm of authenticating signature by combining passive

preprocessing, forgery detection, similarity-based verification as well as visual examination into one system.

In order to enhance the strength of the framework, the system keeps several reference signatures of every user in a structured database, in comparison to the wider representation of real variations. In verification, the input signature is compared with these stored samples and the final decision is made by taking aggregated similarities measures as opposed to using a single comparison. Such a solution enhances reliability, as it minimizes the effects of outliers and non-uniform samples. Additionally, the modular design of the system enables easy integration



IV. METHODOLOGY

The main system has a multi-stage approach that is proposed to enhance reliability of offline signature verification. The workflow does not follow one model: it divides the verification process into particular stages, and each part performs a certain task. The design is useful in controlling the various forms of forgeries and the ability to retain similar performance with respect to diverse input conditions. The general pipeline is preprocessing of the input signature, detection of forgery and similarity -based verification.

The first step involves preprocessing the signature image of input to make it uniform and minimise noise. The color values are thresholded to make the data more easily understandable and then the adaptive thresholding is used to identify the signature strokes and the background. More normalization processes such as scaling and intensity control are done to ensure that the input matches the deep learning architectures. These preprocessing functions also assist in retaining important structural information, and removes non-critical variations due to lighting or scanning environment.

The second stage deals with determining that the input signature is artificially created or not. To this end, a deep learning model based on convolution is used to examine texture features and structural anomalies contained within the image. It is a filtering mechanism where only valid handwritten signatures are filtered to the second step. The system accomplishes this objective by isolating digitally generated inputs at the early stage of the processing which decreases the redundant computations and enhances the accuracy of the end decision.

After the signature has been successful on the initial filtering step, a more in-depth comparison process is performed on the signature with the help of a Siamese neural network. This network has two branches (identical) that process both the input signature and a reference signature. The branches of each extract feature representations and compare them employing a distance based measure of similarity. A short distance ratio means that the signatures are more likely to be the signatures of the same person whereas a long distance ratio implies mismatch. This method allows the system to concentrate on the differences of relation as opposed to class labels, which would be applicable to real-life verification situation.

In order to make the system more usable, a graphical comparative mechanism is incorporated into the system. It is a component that superimposes the reference and test signatures to indicate areas where inversions are found. This visualization will give more knowledge as to the verification process, which enables the user to know how the system will come to make the decision. The procedure will provide an effective solution to the problem of offline signature authentication through the combination of preprocessing, similarity analysis, forgery detection, and visual interpretation, within a single framework.

V. EXPERIMENTAL RESULTS

The quality of a proposed signature verification scheme was tested on the basis of a well-organized experimental design in terms of classification as well as similarity-based validation. The system was trained using a labeled sample which consisted of authentic and forged samples of signatures where there has been diversity in the writing style and the forgery patterns. The data was split into training and validation to evaluate the ability of the models to generalize. The preprocessing proved useful in removing the normalization and resizing to present uniform input across all samples.

In the process of experimentation, the convolution-based model adopted to detect forgery showed that the model remained consistent in training. The model had a validation accuracy of about 86% meaning that it could effectively differentiate between genuine and digitally altered signatures. Precision and F1-score were other performance measures in ensuring accuracy of the detection stage especially to reduce cases of

false acceptance of the forged samples. These findings are consistent with the current literature, wherein deep learning methods have demonstrated excellent results in recognizing structural features of signatures .

The verification phase based on similarity, which was done with the help of a Siamese neural network, was tested on pairs of signatures and calculated their distances in terms of features. The model effectively trained to distinguish matching and non-matching pairs of signatures, which resulted in smaller distance values when there was a genuine match. The experimental observations showed that approaches based on similarity prove to be very helpful in cases of verification tasks, because they concentrate on the differences in the relation and not on fixed classification. Previous studies have indicated accuracy of verification to over 90% with simulations based on Siamese architectures on varying datasets, which proves their capability to deal with variation in signatures.

Besides quantitative performance, a visual comparison mechanism was used as a giveaway to performing a qualitative analysis and identifying differences between reference and test signatures. This element gave clear information on discordant areas making the decisions of the system more readable. Generally, the experimental findings indicate that forgery detection together with similarity-based verification is more accurate and useful in practical application. The system shows uniform performance with various kinds of signatures which means that it is valid in real-life applications of authentication.

VI. DISCUSSION

The experimental results indicate the use of multiple stages of analysis as a tool of offline signature verification. The separation of forgery detection and similarity-based verification enables the system to deal with various kinds of signature anomalous more effectively, compared to using a single model. This is because the first filtering stage minimizes the influence of digitally produced inputs and the comparison stage is concerned with structural consistency in signatures. This stratification helps enhance the reliability of decisions made as compared to the traditional single-stage designs.

One more critical lesson is that the system is capable of addressing natural differences of real signatures. Signatures that are written in hand are seldom uniform even when they are written by the same person. A similarity-based learning can be used to accommodate these variations since, instead of applying strict pattern matching, it compares relative differences. Consequently, the system minimizes the possibility of wrongly discarding true signatures and it also retains this sensitivity to falsified inputs. Such flexibility/precision balance is crucial to real-life deployment.

It also enhances the usability of the system with the addition of a visual comparison mechanism. The system also correlates areas of discrepancy between signatures and instead of giving a final classification, displays an explanation of the choice. This feature is especially useful in the tools that require applications to be transparent, e.g., financial or legal checks. It enables users to take results more seriously as opposed to being a slave to police outsourcing.

In spite of these strong points, a number of weaknesses may be noted. The quality and diversity of training data affect the performance of deep learning models. In case the given data does not reflect the variety of writing styles and types offorgery, the system can be influenced in its generalization. Also, the existing methodology based on the analysis of static images and lacks dynamic features that would further enhance verification accuracy. These points should be considered in work in the future so that the system would become more robust and flexible.

VII. CONCLUSION AND FUTURE WORK.

The paper is a systematic method of verifying signature using an offline system that combines several steps of analysis into a single system. A combination of a convolution-based framework to identify manipulated signatures with a mechanism of verification based on the concept of similarity bridges some of the major challenges of digital as well as skilled forgery. The findings show that detection and comparison tasks should be conducted apart to enhance reliability of the verification process as a whole. Moreover, feature-based measurement of similarity makes the system to be sensitive to mismatches as well as it can be used with natural difference between genuine signatures.

The fact that the proposed approach is focused on interpretability is another striking feature of this approach. It is also important to note that the incorporation of a visual comparison mechanism also makes it easier to point out areas where the signatures are dissimilar, providing a better insight into the verification result. This aspect makes users more confident and will aid in practical uses where transparency is a must. On the whole, the framework shows a stable performance and offers a well-balanced solution that could be applied in authentication contexts in real life where static signature data is used.

Though the system promises good results, it can be further advanced in a number of ways. The first possible extension is to include dynamic signature features like the speed of writing and pressure, which is not provided in offine systems, but can further discriminate information. It may also be necessary to increase the training dataset by adding more writing styles and forgery methods to enhance the generalization ability of the models. Further, the researches of advanced architecture could be used to obtain more intensive structural associations in signatures.

Further elaborations can be done to increase access and scale as well. In reality, the implementation of the system in cloud-

based platform or inclusion in wireless platforms would allow real time validation in the real world. Moreover, the system can be made more informative to the end users by enhancements in visualization methods that would give more specific insights into signature variations. By implementing these factors.

VIII. REFERENCES

[1] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline handwritten signature verification—Literature review," *IEEE Access*, vol. 7, pp. 9420–9436, 2019.

[2] A. Ebrahimpour, M. Soryani, and M. A. Akhaee, "Signature verification using deep convolutional neural networks," *Pattern Recognition Letters*, vol. 128, pp. 82–90, 2019.

[3] S. Dey, A. Dutta, and D. Bhattacharjee, "A deep learning-based approach for offline signature verification," *Expert Systems with Applications*, vol. 136, pp. 1–12, 2019.

[4] Y. Zhang, X. Peng, and L. Zhang, "Offline signature verification using Siamese network with contrastive loss," *IEEE Access*, vol. 8, pp. 118689–118699, 2020.

[5] M. S. Sigari and M. Pourreza, "Writer-independent offline signature verification using deep learning," *Neural Computing and Applications*, vol. 32, pp. 12345–12358, 2020.

[6] H. Nguyen, T. Nguyen, and T. Le, "Signature verification using Siamese neural network for one-shot learning," *Applied Sciences*, vol. 11, no. 6, pp. 1–15, 2021.

[7] R. Kumar and P. Sharma, "Hybrid CNN-SVM model for offline signature verification," *Procedia Computer Science*, vol. 167, pp. 2410–2419, 2021.

[8] A. K. Singh and S. K. Dubey, "Deep learning framework for signature forgery detection,

Multimedia Tools and Applications, vol. 81, pp. 14523–14540, 2022.

[9] J. Wang, Y. Chen, and Z. Li, "Offline signature verification using deep feature learning," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 4, no. 2, pp. 250–261, 2022.

[10] M. Patel and N. Shah, "Signature verification using Siamese networks and feature embedding," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 37, no. 3, pp. 1–18, 2023.

[11] K. R. Reddy and V. S. Kumar, "Deep learning-based signature authentication with improved feature extraction," *Journal of King Saud University – Computer and Information Sciences*, vol. 35, no. 7, pp. 101–112, 2023.

[12] S. Mehta and R. Gupta, "A robust deep learning model for offline signature verification and forgery detection," *IEEE Access*, vol. 12, pp. 55678–55690, 2024.

.