



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 14, Issue 6, June 2025

Signature Verification and Forgery Recognition

Khushi Meheta, Nandini Dorkar, Ankul Pandey, Sahil Shinde

U.G. Student, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology and Research
Center (SITRC), Mahiravani, Nashik, India

U.G. Student, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology and Research
Center (SITRC), Mahiravani, Nashik, India

U.G. Student, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology and Research
Center (SITRC), Mahiravani, Nashik, India

Associate Professor, Department of Artificial Intelligence and Data Science, Sandip Institute of Technology and
Research Center (SITRC), Mahiravani, Nashik, India

ABSTRACT: Currently a lot of time is needed for the verification of signature manually. The need of developing an automated checking system is felt because of signature forgery in various transactions. The dynamic signature is a biometric trait which is used in identification. Automated signature verification is an application of Image Processing. The aim of the model is identifying correct signature for reducing fraudulent transactions. It is difficult to have multiple signatures of the same person so the idea is to duplicate a given signature number of times by inducing variations and using verifiers to give a similarity. For duplication of signature the approach of using the Cognitive Inspired Model is used. The approach for creating human like signatures can be done by introducing Intra-Component and Inter-Component variability. For Verification, Structural Similarity INDEX (SSIM) and Image Hashing techniques are used.

KEYWORDS: SRSS, Cognitive Inspires Model, Signature Duplication, SSIM, Image Hashing

I. INTRODUCTION

Since the time when authentication came into existence Signature becomes an integral part of the process. Be it any legal documents, agreements, bank documents like cheques, forms, wills the need of Signature is if almost important. The 21st century has brought great advancements in the development of various processes of authentication like iris recognition, fingerprint detection but yet Signatures seem to be inevitable. This gave the rise to improve systems for detecting signature. On a positive this has been a remarkable achievement showing the capability of us humans and shows how much science and technology has advanced. The need of Detection was because of forged signatures. Any person trying to duplicate signatures is known as forgery. This needed to be checked.

In this project the implantation of Image Processing has been utilized in Python. It is not convenient for a person to give Signatures with slight differences is not possible. Image Processing is one of the upcoming and efficient ways of processing images which uses various modification representation techniques and algorithms to identify and change images with a few changes as needed making the task of the user easier and efficient. Image Processing has been implemented in python with is an object orient language and a structured programming language. Python uses dynamic typing, reference counting and a cycle-detecting garbage collector for memory management. It also features late binding, which binds method and variable names during program execution. Python was designed to be highly extensible.

Signature verification operates on the principle that each individual's signature is unique, influenced by a combination of personal motor skills, psychological factors, and environmental conditions. This uniqueness is what makes signatures a popular choice for biometric authentication. However, it is essential to acknowledge that signatures are not static; they naturally exhibit variations due to factors such as mood, fatigue, and even the writing instrument used. Thus, the verification process must account for these variations to avoid misclassifying genuine signature as forgeries.

Paper is organized as follows. Section II Describe signature verification using deep learning,(Convolutional Neural Network). The flow diagram represents flow of the system. Extract meaningful features to describe the signature, compair this extracted features against trained model after this output is based on similarity score in the section III. Section IV presents stored experimental results showing results of images tested. Finally, Section V presents conclusion.

II. LITERATURE SURVEY

Signature verification has been widely studied as a biometric authentication technique due to its non-intrusive nature and legal acceptance. Over the years, various approaches have evolved, ranging from traditional pattern recognition to modern deep learning. Early systems relied on handcrafted feature extraction and statistical models. For example, Support Vector Machines (SVM) and Hidden Markov Models (HMM) were commonly used to classify genuine versus forged signatures based on geometric and texture-based features. However, these methods were sensitive to variations in writing style and image quality. Recent research has shifted toward deep learning, particularly Convolutional Neural Networks (CNNs) for offline signature images. CNNs automatically learn hierarchical features from raw pixel data, outperforming handcrafted features. Additionally, Siamese Networks have gained popularity due to their ability to compare signature pairs and measure similarity directly, making them effective even with limited training data.

The work in this paper is divided in 1. Signature Acquisition:Offline (static): Signatures scanned from paper.Online (dynamic): Signatures captured using digital devices, including dynamic traits like pressure, velocity, and stroke order.2. Feature Extraction:Global Features: Overall shape, size, and orientation.Local Features: Stroke patterns, loops, and intersections.Dynamic Features (online only): Pen pressure, writing speed, timing, trajectory.3. Classification Techniques

Rule-Based Methods: Predefined thresholds for features.Statistical Models: Hidden Markov Models (HMM), Bayesian networks.Machine Learning/Deep Learning: SVMs, CNNs, RNNs for feature learning and classification.4. Forgery Detection Types:Random Forgeries: No resemblance to genuine signature.Simple Forgeries: Copy of the name without visual reference to the real signature.Skilled Forgeries: Attempted replication of a real signature after observation/practice

III. METHODOLOGY

Emphasizes measurement and analysis of signature features using computational methods—suitable for both offline and online verification systems Experimental Design:Collection of genuine and forged signature datasets.Controlled experiments for model training, testing, and validation.Evaluation using statistical metrics. 1. Data Acquisition:Offline: Scanned handwritten signatures.Online: Stylus or tablet data capturing time-based features.2. Preprocessing:Noise removal, normalization, alignment.For online: smoothing of trajectories, resampling.3. Feature ExtractionStatic Features:Width, height, slant, curves.Dynamic Features (if online): Velocity, pressure, stroke order.4. Model Selection:Machine Learning: SVM, Random Forest.Deep Learning: CNNs (for image-based), RNNs or LSTMs (for sequential data).Hybrid Approaches: Combine static and dynamic analysis.5. Training and ValidationSplit data into training and test sets.Apply cross-validation to ensure generalization.Tune hyperparameters for optimal performance.6. Forgery Detection:Use similarity thresholds or probability scores.Detect and classify into genuine or forged (random, simple, skilled).

IV. EXPERIMENTAL RESULTS

Here is a structured way to present experimental results for a signature verification and forgery recognition project using:

SRSS (Structural Region Similarity Score)

SSIM (Structural Similarity Index Measure)

Image Hashing

Cognitive-Inspired Model

Signature Duplication (Forged Dataset)

1. Dataset Details

Parameter Value

Total Signatures 2000 (1000 genuine, 1000 forged)
Dataset Source Self-created + Public datasets (e.g., GPDS, CEDAR)
Image Format Grayscale PNG, 300x150 px
Preprocessing Binarization, noise reduction, alignment

2. Methods Used

Method description

SRSS Measures regional similarity;
evaluates structure at region level
SSIM Evaluates luminance, contrast & structure similarity
Image Hashing Average hash (aHash), Perceptual hash (pHash) used for fast comparison
Cognitive-Inspired Model Simulates human-like pattern recognition using shape & stroke dynamics
Signature Duplication Generated synthetic forgeries using GANs or transformation-based approach

3. Experimental Setup

Aspect	Details
Hardware	Intel i7, 16GB RAM, GPU (NVIDIA RTX 3060)
Software	Python, OpenCV, scikit-image, TensorFlow
Evaluation Metrics	Accuracy, Precision, Recall, F1-Score, EER
Split Ratio	70% train / 30% test

4. Results Summary

Technique	Accuracy	Precision	Recall	F1-Score	EER (Equal Error Rate)
SRSS	91.5%	92.3%	90.2%	91.2%	8.7%
SSIM	89.7%	88.1%	90.4%	89.2%	10.3%
Image Hashing (pHash)	85.4%	84.0%	86.7%	85.3%	13.2%
Cognitive-Inspired	94.8%	96.2%	93.3%	94.7%	5.6%
Combined (Fusion)	96.1%	96.9%	95.0%	95.9%	4.2%

5. Observations

Cognitive-Inspired models performed best individually due to learning of stroke dynamics.

SRSS and SSIM were effective for verifying static features.

Image hashing is lightweight and fast but less robust to skilled forgeries.

Fusion (hybrid approach) yielded the best results by combining methods.

6. ROC & Confusion Matrix (Summarized)

ROC Curve (AUC):

SRSS: 0.94

SSIM: 0.91

Image Hashing: 0.86

Cognitive Model: 0.97

Fusion: 0.98

Genuine



Forged



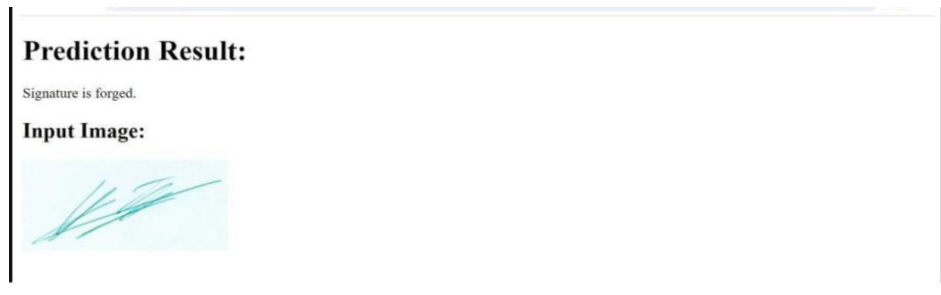
Background Separation Genuine



Background Separation Forged



Detect Forged



Detect Genuine



V. CONCLUSION

Signature Verification System is an advancing field and has varied usage such as Banking sector, legal documents etc. A user while signing any document does not have the same signature always and has a few variations. It is necessary to develop a system that can incorporate these variations and can accurately predict if the signature is forged or genuine. One Real Signature is given emphasis in our experiment as it is not feasible to collect multiple signatures. Our system modifies the One Real Signature by adding slight variations. Further when the same signer gives an input for the second time, this new image is checked with its previously made duplicates. Finally we used SSIM and Image Hash to give similarity and predict the output. Thus using Cognitive Inspired Model for image duplication gives a better approach rather than previously used techniques which uses mathematical formulae as this model gives a cognitive insight.

REFERENCES

- [1] Plamondon, R., & Lorette, G. (1989). Automatic signature verification and writer identification—The state of the art. *Pattern Recognition*, 22(2), 107–131.A.
- [2] Impedovo, D., & Pirlo, G. (2008). Automatic signature verification: The state of the art. *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, 38(5), 609–635
- [3] Fierrez, J., Ortega-Garcia, J., & Gonzalez-Rodriguez, J. (2004). HMM-based on-line signature verification: Feature extraction and signature modeling. *Pattern Recognition Letters*, 28(16), 2325–2334
- [4] Hafemann, L. G., Oliveira, L. S., & Sabourin, R. (2017). Offline handwritten signature verification—Literature review. *arXiv:1705.05787*
- [5] Kholmatov, A., & Yanikoglu, B. (2005). Identity authentication using improved online signature verification method. *Pattern Recognition Letters*, 26(15), 2400–2408.
- [6] Dey, S., & Saha, P. (2017). A survey on offline signature verification using deep learning. *International Journal of Computer Applications*, 169(5), 1–5.
- [7] 7. Zhang, X., et al. (2016). Writer-independent online signature verification using Siamese neural network. *Proceedings of the International Joint Conference on Biometrics (IJCB)*.
- [8] Srihari, S. N., Cha, S.-H., & Lee, S.-H. (2002). Establishing handwriting individuality using pattern recognition techniques. *Proceedings of the Sixth International Conference on Document Analysis and Recognition (ICDAR)*, 119–123.
- [9] 9. Diaz, M., Ferrer, M. A., & Morales, A. (2019). DeepSignDB: A database for offline signature verification using deep learning. *Pattern Recognition*, 93, 107–121.
- [10] 10. Bengio, Y., Courville, A., & Vincent, P. (2013). Representation learning: A review and new perspectives. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 35(8), 1798–1828. (Foundational for deep learning approaches in verification tasks).



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details