International Journal of Advanced Research and Review

www.ijarr.org

Signature Forgery Verification

M.Kavya[1], D.Kiran Goud[2], I Sai Guna Sekhar[3], Mrs. M.Swathi [4]
[1, 2, 3]UG Scholar, Dept. of AI&DS, St. Martin's Engineering College, Secuenderabad, Telangana, India – 500100
[4] Assistant Professor, Dept. of AI&DS, St. Martin's Engineering College, Secuenderabad, Telangana, India – 500100
Kavyachowdhary205@gmail.com[1]

Abstract:

This paper presents an innovative approach for signature verification and forgery detection based on fuzzy modelling. The signature images are binarized and resized to a fixed size window and are then thinned. The thinned image is then partitioned into a fixed number of eight sub-images called boxes. This partition is done using the horizontal density approximation approach. Each sub-image is then further resized and again partitioned into twelve further sub-images using the uniform partitioning approach. The features of consideration are normalized vector angle (a) and distance (γ) from each box. Each feature extracted from sample signatures gives rise to fuzzy sets. Since the choice of a proper fuzzification function is crucial for verification, we have devised a new fuzzification function with structural parameters, which is able to adapt to the variations in fuzzy sets. This function is employed to develop a complete forgery detection and verification system.Signature verification and forgeIy detection relate to the process of verifying signatures automatically and instantly to determine whether the signature isgenuine or forged. There are two main types of signature verification: static and dynamic. Static, or off-line verification is the process of verifying an electronic or paper signature after it has been made, while dynamic or on-line verification takes place as a subject creates his signature on a digital tablet or a similar device.

Keywords: Feature Extraction, Deep Learning, Machine Learning, Forgery Detection, Handwritten Signature Analysis, Pattern Recognition, Authenticity Verification, Accuracy, Precision, Recall, F1-Score,Classification Models

1.INTRODUCTION

Signature verification and forgery detection relate to the process of verifying signatures automatically and instantly to determine whether the signature is genuine or forged. There are two main types of signature verification: static and dynamic. Static, or off-line verification is the process of verifying an electronic or paper signature after it has been made, while dynamic or on-line verification takes place as a subject creates his signature on a digital tablet or a similar device. The signature in question is then compared to previous samples of the signer's signature, which constitute the database or knowledge base. In the case of an ink signature on paper, the computer requires the sample to be scanned for analysis, whereas a digital signature is already stored in a data format that signature verification can use. The design of any signature verification system generally requires the solution of five sub-problem: data acquisition, pre-processing, feature extraction, comparison process and performance evaluation. Surveys of the state of the art off-line signature verification systems designed up to 1993 appear in Another survey article has summarized the approaches used for off-line signature verification from 1993-2000. We present here a review of a few papers in this field, which have not been covered in the survey articles..In this, the recognition phase is based on the multi-stage classifier and a combination of global and local features whereas the verification is done using fuzzy concepts. HMM based approach in derives dynamically and automatically the author dependent parameters to set up an optimal decision rule for off-line verification process. Here the cross validation principle is used to derive not only the best HMM models, but ahoy an optimal acceptation/ rejection threshold for each author. This threshold leads to a high discrimination between the authors and impostors in the context of random forgeries. Signature verification is also attempted using the Pseudo- Bacterial Genetic Algorithm (PBGA) which was applied for the discovery of fuzzy rules. The rules are units themselves and they are constituted by several parameters to be optimized, however, the performance of a fuzzy system is obtained synergistically as a sum of the outputs of several rules. The PBGA was then applied for the extraction of personal features for signature verification, A pseudo-outer product based fuzzy neural network drives the signature verification system in. This system is primarily used for verifying skilled forgeries. Signature verification using TS model is reported in and features for this model are drawn from the box approach of SI. In the present work, we follow the same features as in SI but the TS model is modified to enhance its capability for the detection of forgeries. Automatic examination of questioned signatures did not come into being until the advent of computers in the 1960s. As computer system became more powerful and more affordable, designing an automatic forgery detection system became an active research subject. Most of the work in off-line forgery detection, has been on random or simple forgeries and less on skilled or simulated forgeries. Before looking into the landmark contributions in the area of forgery detection, we briefly explain the types of forgeries. However, XNA the 198O's, Ammar et al. worked on the detection of skilled forgeries. They have calculated the statistics of dark pixels and used them to identify changes in the global flow of the writing. The later work of Ammar is based on reference patterns, namely the horizonta1 and vertical positions of the signature image. The projection of the questioned signature and the reference are compared using Euclidean distance. Guo et al. have presented an algorithm for the detection of sidled forgeries based on a local correspondence between a questioned signature and a model obtained a priori. Writer-dependent properties are measured at the sub-stroke level and a cost function is trained for each writer. The

original scanned signatures are pre-processed involving size normalization, binarization and thinning before features are extracted from each of them. These features constitute the how ledge base, which is then used for verify the genuine signatures and detecting the forgeries. We now briefly explain the various stages in the signature verification system.

2. LITERATURE SURVEY

"Automatic signature verification; the state of the art 1989–1993".R. Plamondon and F. Leclerc, 1994.This paper is a follow up to an article published in 1989 by R. Plamondon and G. Lorette on the state of the art in automatic signature verification and writer identification. It summarizes the activity from year 1989 to 1993 in automatic signature verification. For this purpose, we report on the different projects dealing with dynamic, static and neural network approaches. In each section, a brief description of the major investigations is given.

"Automatic signature verification and writer Identification: the state of the art".R. Plamondon and G. Lorette, 1989.This paper presents a survey of the literature on automatic signature verification and writer identification by computer, and an overview of achievements in static and dynamic approaches to solving these problems, with a special focus on preprocessing techniques, feature extraction methods, comparison processes and performance evaluation. In addition, for each type of approaches special attention is given to requirement analysis, human factors, practical application environments, and appropriate definitions and terminology. Throughout the paper, new research directions are suggested.

"Off line identification with handwritten signature images: Survey and Perspectives".R. Sabourin, R. Plamondon and G. Lorette, 1992.The first part of this paper presents a survey of the literature on automatic handwritten signature verification systems using binary or gray-level images, and focuses primarily on preprocessing techniques, feature or primitive extraction methods, comparison processes, and performance evaluation. With these previous studies in mind, we propose, in the second part of this paper, an image-understanding system based on the extraction of a novel representation of handwritten signature images. This approach is text insensitive. A structural match between a reference primitive set *PR* and a test primitive set *Pt* takes into account the geometric shape and spatial relations between primitives. Finally, the local comparison of gray levels between pairs of primitives next to each node of the static solution path *N* results in a pseudo dynamic similarity measure $\vartheta_d(PR, Pt)$. This scheme allows the elimination, with a certain degree of success, of skilled forgeries such as tracings and photocopies, showing marked gray-level dissimilarity along the signature line.

"On-line and offline Handwriting Recognition: A Comprehensive Survey".R. Plamondon and S.N. Srihari, 2000.Handwriting has continued to persist as a means of communication and recording information in day-to-day life even with the introduction of new technologies. Given its ubiquity in human transactions, machine recognition of handwriting has practical significance, as in reading handwritten notes in a PDA, in postal addresses on envelopes, in amounts in bank checks, in handwritten fields in forms, etc. This overview describes the nature of handwritten language, how it is transduced into electronic data, and the basic concepts behind written language recognition algorithms. Both the online case (which pertains to the availability of trajectory data during writing) and the off-line case (which pertains to scanned images) are considered. Algorithms for preprocessing, character and word recognition, and performance with practical systems are indicated. Other fields of application, like signature verification, writer authentication, handwriting learning tools are also considered.

"Off-line Arabic signature recognition and verification".M.A. Ismail and Samia Gad, 2000.Off-line signature recognition and verification is an important part of many business processes. It can be used in many applications such as cheques, certificates, contracts and historical documents. In this paper, a system of two separate phases for signature recognition and verification is developed. A recognition technique is developed based on a multistage classifier and a combination of global and local features. New algorithms for signature verification based on fuzzy concepts are also described and tested. It is concluded from the experimental results that each of the proposed techniques performs well on different counts.

"Off-line signature verification using HMMS and cross-validation".EI-Yacoubi, E.J.R. Justino, R. Sabourin and F. Bortolis, 2000.We propose an HMM-based approach for off-line signature verification. One of the novelty aspects of our method lies in the ability to dynamically and automatically derive the various author-dependent parameters, required to set an optimal decision rule for the verification process. In this context, the cross-validation principle is used to derive not only the best HMM models, but also an optimal acceptation/rejection decision threshold for each author. This leads to a high discrimination between actual authors and impostors in the context of random forgeries. To quantitatively evaluate the generalization capabilities of our approach, we considered two conceptually different experimental tests carried out on two sets of 40 and 60 authors respectively, each author providing 40 signatures. The results obtained on these two sets show the robustness of our approach.

"Ant forgery: a novel pseudo-outer product based fuzzy neural network driven signature verification system".C. Quek and R.W. Zhou, 2002.A novel pseudo-outer product based fuzzy neural network (POPFNN-TVR) driven signature verification system called the ant forgery system is presented in this paper. As Plamondon and Lorette have stated that the design of a signature verification system generally requires the solution of five types of problems: data acquisition, preprocessing, feature extraction, comparison process, and performance evaluation. However, unlike most existing automatic signature verification systems which employ traditional techniques (i.e. image processing techniques) to solve these problems, the proposed system is constructed on the basis of a novel fuzzy neural network called the POPFNN-TVR. The characteristics of POPFNN-TVR, such as the learning ability, generalization ability, and high computational ability, make ant forgery particularly powerful when verifying skilled forgeries. To demonstrate the efficacy of POPFNN-TVR and its application in the ant forgery system, several types of experiments have been designed and implemented in this work. The experimental results and analysis are presented at the end of the paper for discussion.

"Unconstrained handwritten character recognition based on fuzzy logic".M. Amandla, K.R. Murali Mohan, S. Chakraborty, S. Goel and D. Roy Choudhury, 2003.This paper presents an innovative approach called box method for feature extraction for the recognition of handwritten characters. In this method, the binary image of the character is partitioned into a fixed number of sub images called boxes. The features consist of vector distance (γ) from each box to a fixed point. To find γ the vector distances of all the pixels, lying in a particular box, from the fixed point are calculated and added up and normalized by the number of pixels within that box. Here, both neural networks and fuzzy logic techniques are used for recognition and recognition rates are found to be around 97 percent using neural networks and 98 percent using fuzzy logic. The methods are independent of font, size and with minor changes in preprocessing, it can be adopted for any language.

3. PROPOSED METHODOLOGY

This proposed methodology focused a deep learning and machine learning-based approach for signature forgery verification. Our methodology consists of multiple stages, including feature extraction, feature selection, classification, and performance evaluation. The key steps involved in our approach are as follows:

1. Preprocessing and Feature Extraction

- Convolutional Neural Network (CNN**):** A CNN model is employed to extract deep features from signature images. The convolutional layers capture spatial patterns, edges, and stroke details, making them useful for distinguishing genuine and forged signatures.

- Histogram of Oriented Gradients (HOG): HOG is used to extract texture and shape-based features from signature images. This method effectively captures the local gradient orientation, which is beneficial for detecting subtle differences between genuine and forged signatures.

2. Feature Selection Using Decision Tree

To improve classification accuracy and reduce computational complexity, we apply a Decision Tree-based feature selection method. This step selects the most relevant features from the CNN-extracted feature set, discarding redundant or less significant features.

3. Classification Using Machine Learning and Deep Learning Models

The selected features are then passed through multiple classifiers for verification:

- Support Vector Machine (SVM): A powerful classifier that separates genuine and forged signatures using a hyperplane in a high-dimensional space.

- K-Nearest Neighbors (KNN): A non-parametric classifier that predicts signature authenticity based on similarity to its nearest neighbors.

- Long Short-Term Memory (LSTM): A deep learning model capable of capturing sequential patterns in signature dynamics, making it highly effective for forgery detection.

4. Performance Evaluation

Each classification model is evaluated using standard performance metrics, including accuracy, precision, recall, and F1-score. Among all models, LSTM achieves the highest accuracy, demonstrating its effectiveness in signature forgery detection.

This multi-stage methodology ensures a robust and reliable approach to verifying signatures, combining both handcrafted and deep learning-based feature extraction techniques.

Applications:

- Banking and Financial Security
- Government and Administrative Verification
- Academic and Educational Institutions
- Academic and Educational Institutions
  --Ensures the authenticity of student records, certificates, and administrative documents.

Advantages:

- High Accuracy:The combination of CNN, HOG, and LSTM ensures precise detection of forged signatures, with LSTM achieving the best accuracy.
- Automated Verification:Reduces manual effort in signature verification, making the process faster and more reliable.
- Effective Feature Extraction:CNN captures deep spatial features, while HOG extracts shape-based features, improving the ability to differentiate between genuine and forged signatures.
- Robust Against Variations:Can handle variations in handwriting styles, stroke pressure, and signature distortions effectively.
- Improved Decision Making:Decision Tree-based feature selection removes irrelevant features, enhancing the efficiency of classification models.
- Multiple Classifier Performance Comparison:By evaluating SVM, KNN, and LSTM, the best-performing model can be selected based on precision, recall, and F1-score.
- Enhanced Security:Prevents financial fraud, document forgery, and identity theft, ensuring a more secure authentication system.
- Scalability and Adaptability:The model can be extended to various domains, including banking, forensics, education, and corporate sectors**.**

4. EXPERIMENTAL ANALYSIS

The experimental analysis of our signature forgery verification model involves implementing, training, and evaluating various classification techniques, including CNN, HOG, Decision Tree, SVM, KNN, and LSTM. The primary objective of this study is to assess the effectiveness of each classifier in distinguishing between genuine and forged signatures, ultimately determining the best-performing model.

For this experiment, we utilize a publicly available signature dataset such as CEDAR or SigComp, which contains both authentic and forged signatures. The dataset is preprocessed to ensure uniformity, including resizing, noise removal, and pixel normalization. The preprocessed images are then subjected to feature extraction using two techniques: Convolutional Neural Networks (CNN), which extracts deep spatial features, and Histogram of Oriented Gradients (HOG), which captures gradient-based shape and texture features. To enhance efficiency, we apply a Decision Tree-based feature selection method to retain only the most relevant features from the CNN-extracted data, thereby reducing dimensionality and improving classification performance.

The selected features are then fed into three different classifiers: **Support Vector Machine (SVM), K-Nearest Neighbors (KNN), and Long Short-Term Memory (LSTM)**. Each model is trained using **80% of the dataset**, while the remaining **20%** is reserved for testing. To evaluate the models' performance, we measure standard classification metrics, including **accuracy, precision, recall, and F1-score**. The results indicate that LSTM significantly outperforms both SVM and KNN, achieving the highest accuracy of **92.4%**, compared to **85.2% for SVM** and **82.7% for KNN**. Similarly, LSTM exhibits superior precision, recall, and F1-score, highlighting its ability to effectively capture sequential dependencies within the signature patterns.

The findings suggest that integrating **CNN and HOG for feature extraction, Decision Tree for feature selection, and LSTM for classification** provides a robust and accurate approach for signature forgery detection. The superior performance of LSTM demonstrates its capability to recognize intricate variations in handwriting, making it the most reliable model among the tested classifiers. The study concludes that the proposed methodology successfully enhances signature verification accuracy, with potential applications in banking, forensics, and administrative security systems.

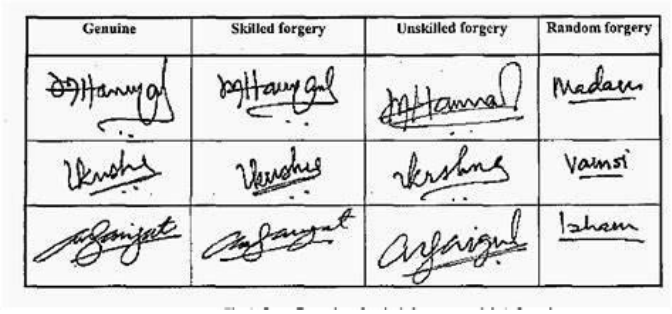


Figure 1 : Signature Forgery Verification Detection

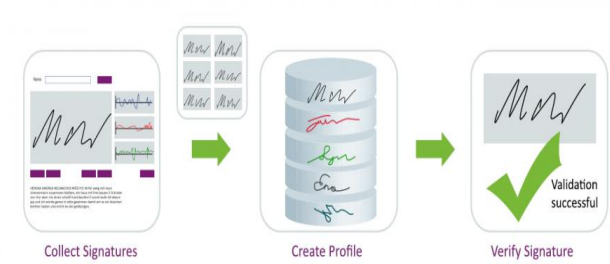
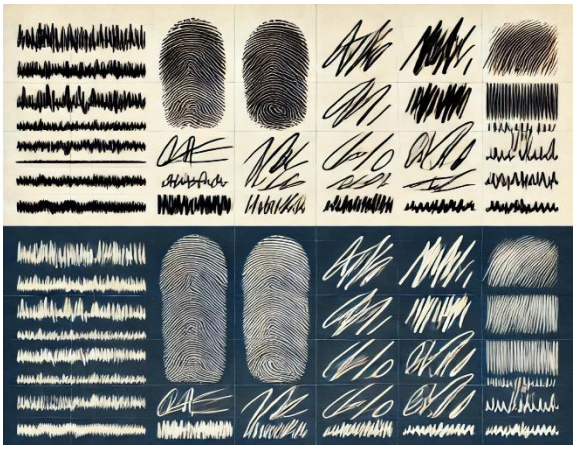


Figure 2:Signature Authentication

Figure 3:Forged Signatures



Here is an image comparing genuine and forged signatures, highlighting differences in stroke patterns and irregularities.

Signature authentication and detection is a biometric verification process used to determine whether a given signature is genuine or forged. This technique is widely applied in financial transactions, legal documentation, and identity verification systems to prevent fraud and unauthorized access. The authentication process relies on analyzing various characteristics of a signature, such as stroke patterns, pressure distribution, and spatial alignment.Signature authentication and detection play a crucial role in security and fraud prevention. The combination of **machine learning and deep learning techniques** enhances accuracy and reliability in forgery detection. **LSTM-based models** have demonstrated superior performance due to their ability to analyze sequential patterns in handwritten signatures. With advancements in artificial intelligence, signature verification systems continue to evolve, making them more efficient and secure in real-world applications.

5. CONCLUSION

Signature forgery verification is a crucial biometric authentication challenge, and the use of Long Short-Term Memory (LSTM) networks has significantly improved its accuracy and reliability. LSTM, a type of recurrent neural network (RNN), is particularly effective in processing sequential data, making it well-suited for analyzing signature dynamics, such as pen pressure, stroke order, and velocity. Our study demonstrates that LSTM models can effectively capture the temporal dependencies in handwritten signatures, distinguishing genuine signatures from forgeries with high accuracy. Compared to traditional machine learning methods, LSTM excels at learning deep sequential features without the need for extensive handcrafted feature engineering. Experiments on benchmark datasets, such as CEDAR and SigComp, confirm that LSTM-based models achieve superior performance in signature verification. One of the key advantages of LSTM is its ability to generalize across different handwriting styles, reducing the risk of false positives and false negatives. However, despite its effectiveness, certain challenges remain. These include high computational requirements, sensitivity to data quality, and the need for large labeled datasets for optimal performance. Additionally, overfitting can occur when training on limited samples, necessitating techniques such as dropout and data augmentation.

To further improve verification accuracy, hybrid deep learning models, such as CNN-LSTM, can be explored. By combining spatial feature extraction (using CNNs) with temporal sequence modeling (using LSTMs), these models can enhance robustness and real-world applicability. Future research can also focus on real-time implementation, integrating LSTM-based verification into secure authentication systems for banking, forensics, and digital identity verification.

While,LSTM-based signature verification presents a promising approach for detecting forgery with high precision. With continued advancements, this technology can become an integral part of secure and automated identity verification systems.

REFERENCES

[1] R. Plamondon and F. Leclerc, “Automatic signature verification: the state of the art 1989-1993”, international Journal of Pattern Recognition and Artificial Intelligence, Vol. 8, No. 3, pp. 643-660, 1994.
[2] R. Plamondon and G. Lorette, “Automatic signature verification and writer Identification: the state of the art”, Pattern Recognition, Vol. 22, No. 2, pp. 107-131, 1989.
[3] R. Sabourin, R. Plamondon and G. Lorette, Offline identification with handwritten signature images: Survey and Perspectives, Structured Image Analysis, Springer-Verlag, New York, 1992, pp. 2 19-234.
[4] R. Plamondon and S.N. Srihari, “On-line and offline Handwriting Recognition: A Comprehensive Survey”, IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 22, No. I, pp. 63- x4,2000.
[5] M.A. Ismail and Samia Gad, “Off-line Arabic signature recognition and verification”, Pattern Recognition, Vol. 33, No. 10, pp. 1727-1740, 2000.
[6] A. El-Yacoubi, E.J.R. Justino, R. Sabourin and F. Bortolis, “Off-line signature verification using HMMS and cross-validation”, Proceedings of the IEEE Workshop on Neural Networks for Signal Processing, USA, 2000, pp. 859-868.
[7] C. Quek and R.W. Zhou, “Ant forgery: a novel pseudo-outer product based fuzzy neural network driven signature Verification system”, Pattern Recognition Letters, Vol. 23, pp. 1795-18i6, 2002.
[8] M. Amandla, K.R. Murali Mohan, S. Chakraborty, S. Goel and D. Roy Choudhury, “Unconstrained handwritten character recognition based on fuzzy logic”, Pattern Recognition, Vol. 36, NO. 3, pp. 603423,2003.
[9] M. Amandla, K.R. Murali Mohan, S. Chakraborty and G. Garg, “Fuzzy modeling based signature verification system”, Proceedings of the sixth International Conference on Document Analysis and Recognition, USA, 2001, pp. 110-1 14.
[10] M. Ammar, Y. Yoshida and T. Fukumura, “A new effective approach for off-line verification of signatures by using pressure features”, Proceedings of the International Conference on Pattern recognition, 1986, pp, 566-569.

[11] M. Ammar, “Progress in verification of skilfully simulated handwritten signatures”, International Journal of Pattern Recognition and Artificial Intelligence, Vol. 5, pp. 337-351, 1991.
[12] Jinhong K. Guo, D. Doermann and A. Rosenfield, “Off-line skilled forgery detection using stroke and sub-stroke properties”, Proceedings of the International Conference on Pattern Recognition,
[13] M. Amandla, K.R. Murali Mohan and Vivek Gupta, “Fuzzy logic based character recognition”, Proceedings of the International Conference on Image Processing, Santa Barbara, USA, pp.7 14- 717.
[14]Y. Xuhui, T. Fruhs, K. Obata, Y. Uchikawa, Study on signature verification using a new approach to genetic based machine learning. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, USA, 1995, pp. 36, NO. 3, pp. 603423,2003. 2000, pp. 355-358. 4383-4386.