IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Survey Of Explainable Machine Learning Techniques For Offline Signature Forgery Detection Using Forgexplain

[1]Madiha Kaunain, [2]Nalini M, [3]Noor Ayesha, [4]Aparna N

[1]Student, [2]Student, [3]Student, [4]Assitant Professor

[1]Department of Computer Science and Engineering

[1]Rajiv Gandhi Institute of Technology, Bengaluru, India

Abstract: Offline signature verification is an effective biometric authentication method with widespread applications in areas including finance, law, and security. However, because of variations in the way that each person writes, as well as the existence of highly skilled forgeries, distinguishing real from false signatures can be very difficult. As a result, a number of researchers have proposed various methods for investigating the validity of signatures by applying principles of image processing and machine learning. Typically, researchers will preprocess the image of the signature, extract features related to it, and then classify these features to determine if a signature is either real or false. Historically, researchers have used many different methods to accomplish signature verification, including Support Vector Machines, Artificial Neural Networks, Hidden Markov Models, and Dynamic Time Warping, as well as more recently developing sophisticated detection models using deep learning architectures like Convolutional Neural Networks to improve accuracy. The purpose of this paper is to provide a survey of the current methods for offline signature verification to detail the advantages and disadvantages of each method. In addition, by comparing the strengths and weaknesses of their methodologies, researchers and practitioners can gain insight into what types of improvements can be made to signature verification systems in order to enhance their accuracy and dependability.

Keywords - Signature verification, Forgery detection, Biometrics, Image processing, Machine learning.

I. INTRODUCTION

Biometric methods that are used for identifying and verifying individuals are most commonly associated with a person's handwritten signature as this method is found in financial transactions, legal documents and contracts, banking transactions, as well as administrative functions. With the advent of new digital technologies for authenticating an individual's identity the handwritten signature continues to be important in the determination of a person's identity. Unfortunately, written signatures are subject to various forms of forgery and result in significant security risks. Forged signatures can be produced by individuals who do not have permission to use a person's signature and typically do so with the intent of obtaining access or approval in an unauthorized manner. Therefore, developing an accurate and accessible method for detecting forged signatures has become critical to the areas of pattern recognition and computer vision within the scientific research community.

There are two major types of signature verification systems; online and offline signature verification systems. Online signature verification systems collect dynamic information while the signature is being produced; dynamic information can be collected using a digital tablet or stylus. When producing the signature, dynamic properties such as pressure, velocity, sequence of strokes and trajectory of the stylus

can be captured. Conversely, in offline signature verification systems only static images of signatures are used (scanned from documents or from photographs). Therefore, since no dynamic features are available to offline systems, they must use: image processing techniques; and pattern recognition techniques to determine the image characteristics and structure of signatures. The comparison between online and offline signature verification techniques is shown in Fig. 1

Due to the ease of integrating offline signature verification with existing document processing systems, offline systems have received considerable attention because they can be used with any computer or device without requiring special hardware devices. However, recognizably identifying forged signatures after having been processed offline (i.e., from photographs of actual handwritten signatures) has been challenging due to varying writing styles that are present from one person to another, distorted signatures as a result of image noise and/or differences between scanning conditions. Researchers have developed a number of techniques, primarily using image processing, machine learning, and deep learning, to perform offline signature verification on signature images through multiple stages of processing (preprocessing, feature extraction, and classification).

The first step in the image processing stage is called 'Pre-processing': The signature image must first be enhanced through methods such as converting the image to grayscale, removing background noise, converting the image to binary, and normalizing the resulting image. Image enhancement techniques are performed to provide for improved signature quality. Once the preprocessing has been completed, feature extraction methods will be applied to extract the relevant features of the signature. Features such as texture, shape, stroke direction, and distribution of pixels can be features that are used to compare a target signature to a reference signature. Some techniques used in feature extraction are Local Binary Pattern (LBP), Gray Level Co-Occurrence Matrix (GLCM), Histogram of Oriented Gradients (HOG), and other structural features.

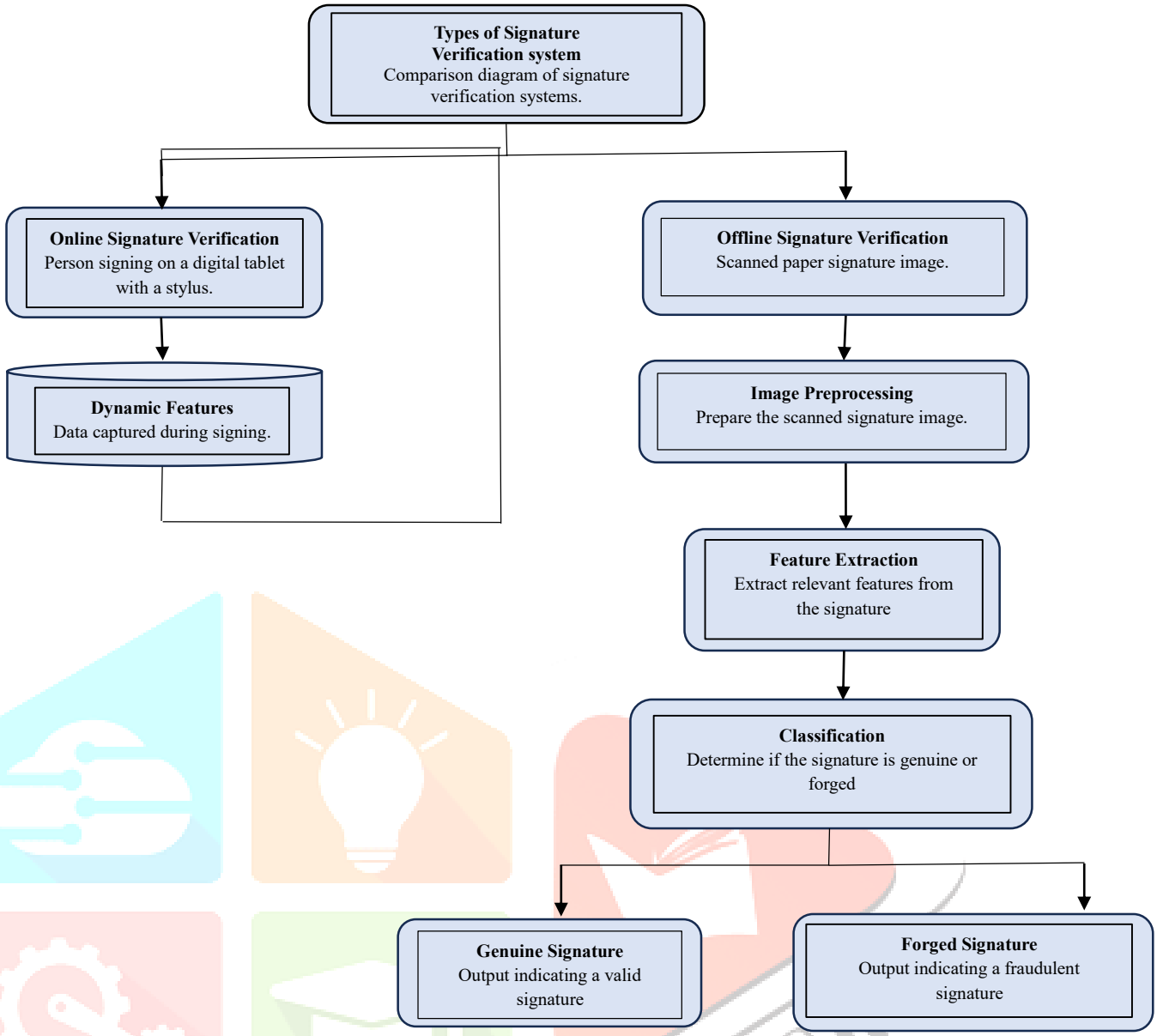

Fig. 1 Online vs. Offline Signature Verification Systems (Two Types of Signature Verification Systems)

Once the relevant features are extracted, machine learning and deep learning algorithms are employed to classify the signatures as genuine or forged. Several classification models such as Support Vector Machines (SVM), Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and hybrid models have been widely used for this purpose. These models analyse the extracted feature vectors and learn to distinguish between authentic signatures and different types of forgeries, including random, simple, and skilled forgeries.

The general workflow of an offline signature forgery detection system involves signature acquisition, preprocessing, feature extraction, and classification stages. Each stage plays an important role in improving the accuracy and reliability of the system. A typical architecture of the offline signature forgery detection framework is shown in Fig. 2, which illustrates the sequential steps involved in the process of identifying genuine and forged signatures.

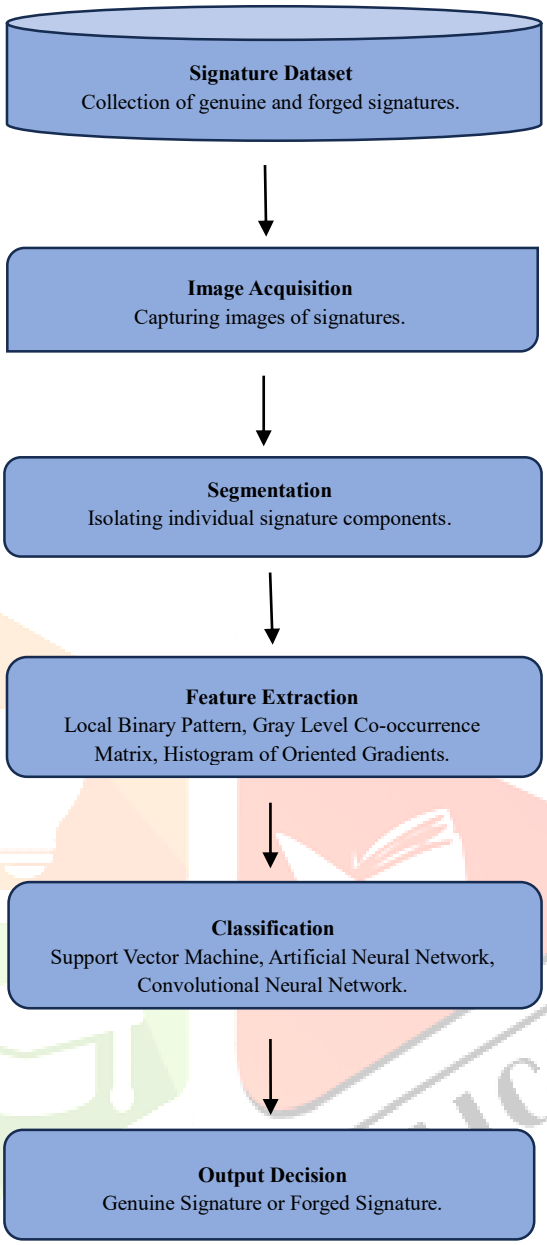

Fig. 2 Shows the Structure of a System that Detects Forged Signatures.

II. LITERATION SURVEY

Signature verification systems consist of five phases: data acquisition(preprocessing), data processing(feature extraction), data comparison, and performance evaluation. In dynamic systems, a digitiser or instrumented pen will obtain pen position, pressure, velocity, and acceleration information. Static systems, on the other hand, will extract features from scanned signature images via imaging technology.

The research focuses on developing different features to distinguish genuine signatures from forgeries. Some examples of feature extraction technologies include geometric features, dynamic parameters, statistical features, and transforms. The extracted features will be stored in a reference method and compared against the unknown signature to determine if it is authentic.

Md. Iqbal Quraishi, Syeda Khaja Mohiddin, and B. Ramesh [1] put forward a method for offline signature verification that consists of the Ripplet-II transform and an Artificial Neural Network (ANN). This approach uses the Ripplet transform to obtain both multi-directional and multi-scale features from images of handwritten signatures, enabling it to extract both types of characteristics present in the structure of the handwritten signature. The resulting features are then input to an ANN classifier, which distinguishes genuine from forged signatures. The method produces a better representation of features than traditional transforms (e.g., wavelets). Experimental evaluation indicates that this combination of the Ripplet transform and neural-network-based classification yields improved accuracy and lower error rates.

The paper "An extensive review of offline signature verification systems" by **Othman O. Khalifa, Aisha Hassan A. Hashim, and Sayed A. Samad [2]** gave a very thorough overview of the various types of offline (i.e., no dynamic signature data) signature verification systems currently in use. In addition, their work examined all possible methods used to verify signatures, such as statistical methods, structural pattern recognition, neural networks, and various machine learning techniques. One of their conclusions was that one of the major obstacles to effective offline signature verification is the lack of any dynamic information about the signing process, e.g., writing speed, pressure, pen trajectory, etc. Furthermore, the authors reviewed the literature regarding pre-processing (cleaning), feature extraction, and classification algorithms, and provided a comprehensive overview of the types of algorithms available. They concluded that, overall, current algorithms for signature verification are insufficient; therefore, advanced learning algorithms must be developed to improve the performance of signature verification.

Local Binary Patterns (LBP) texture analysis technique has been proposed by **Rameez Wajid, Hafiz Malik, and Muhammad Imran Malik [3]**. This LBP operator captures the local texture variation of the pixels of a given image by encoding and provides a representation of the micro-patterns contained in each signature's writing style. The features that are extracted from the signature will then be classified using a classification framework to indicate the legitimacy of the signature during the process of verifying its authenticity. The experimental findings from this study indicate that LBP provides significantly enhanced verification capabilities through feature extraction from the data.

An offline signature verification system has been developed by **Gautam S. Prakash, B. Shekar, and K. Ramesh [4]** that incorporates computer vision algorithms and neural network classifiers. The system starts with several pre-processing steps that include image normalisation, noise removal, and binarization to improve the quality of signature image data. After pre-processing is complete, structural features are extracted using computer vision algorithms, which are then used to train a neural network for the classification of signatures. The results of the experiments conducted on this system show that the combination of computer vision feature extraction methods, combined with a neural network classifier, increases the accuracy of detecting forged signatures and significantly increases the reliability of the overall system.

A systematic examination was conducted by **Haritha Damarla, K.S. Rao [5]**, and the rest of the researching team regarding offline signature verification strategies, both technology and methodology. Different methods of feature extraction for signature analysis were examined, including geometric features, grid-based approaches, and texture-based descriptors. The classification methods that were discussed were neural networks, support vector machines, and statistical classifiers. This study highlighted the benefits and limitations of each of the various techniques used in offline signature verification. The research findings provide an understanding of how signatures have been verified using different technologies (offline signature verification system). In addition to developing a comparative understanding among the various offline signature verification systems, Haritha Damarla and K.S. Rao's findings also demonstrate some of the most significant factors that impact system performance.

An offline signature verification system using image processing techniques was proposed by **Neelima Singh and Ritu Singh [6]**. The first step in verifying a signature is to preprocess the scanned image; the preprocessing consists of binarising the scanned image (creating a black and white version of the image), filtering out any noise, and normalising the image in preparation for feature extraction. Once the signature has been preprocessed, the next step is to extract geometric and structural features from the signature. The extracted features are then compared to stored reference signatures to determine whether the signatures

are authentic or not. The authors concluded that the use of image processing techniques can improve the accuracy and reliability of signature verification systems.

An offline handwritten signature recognition system was proposed by **K. Daqrouq, H. Sweidan, A. Balamesh and M. N. Ajour [7]**. The authors used a combination of wavelet transform decompositions and neural network classifiers to implement their method. Wavelet transform decompositions are applied to the signature to allow the signature image to be decomposed into many frequency components, which permits the analysis of both global and local features of the signature. Entropy of the wavelet transform decomposition is calculated to measure the complexity and irregularity of the signature pattern. The entropy-based features are used to train a neural network classifier for the purpose of verifying the authenticity of the signatures. The authors concluded that combining wavelet decomposition with neural network classifiers improves performance and reduces classification errors.

The authors, **Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira [8]**, proposed an offline handwritten signature verification approach using a CNN-based deep learning framework. Unlike conventional methods that utilize handcrafted features, the CNN automatically extracts discriminative features from the input signature images. The proposed deep learning framework requires an extensive collection of genuine and forged signature examples to establish its ability to learn complex visual patterns and variations. The results of the experimental work indicated that deep learning approaches outperformed traditional machine learning techniques for verifying signatures.

The authors**, S. Dey, A. Dutta, J. I. Toledo, S. K. Ghosh, J. Llados, and U. Pal, [9]** presented a writer-independent offline signature verification framework utilizing a Convolutional Siamese Network architecture called SigNet. In the case of the Siamese Network, two identical networks are utilized to process two signatures at once. When the two networks have been trained for similarity, the Siamese architecture will determine whether the two signatures were created by the same author. Because the SigNet structure is writer-independent, it can generalize across all signatures or individuals without requiring another training set for each signature. SigNet demonstrated strong results for the detection of forged signatures.

An offline signature verification system using a One-Class Support Vector Machine (SVM) classifier has been proposed by **A. Guerbai, Y. Chibani and B. Hadjadji [10]**. The new method focuses on features that are independent of the writer that are able to characterize the signatures effectively. The One-Class SVM uses only genuine signature samples to be trained, and during the verification of the signatures will identify forged signatures as being anomalies. This method works particularly well when there are very few forged samples available for training. Experimental results show that this method is effective at distinguishing between genuine and forged signatures.

In **S. Y. Ooi, A. B. J. Teoh and Y. H. Pang [11]**, the authors proposed a technique for offline signature verification based on the Radon Transform. The Radon transform is used to extract directional and projection-based features from the signature images by analyzing how the distribution of the intensity of the pixels occurs at different angles. The resultant features effectively capture both the structural features of the signature as well as its orientation patterns. The features obtained are then used in a classification process for verifying the authenticity of the signatures. In this study, Radon transform-based feature extraction provides better feature representation and subsequently improves the performance of signature verification systems.

TECHNIQUES USED FOR DETECTION

Ref No.	Year	Methods Used	Findings
[1]	2002	Watershed Segmentation Used to Extract Features Using GLCM With Thresholding and Classify with an SVM.	Multi-stage classification reduces noise and increases accuracy for verifying original signatures
[2]	2011	Using a clustering-based ML Classifier Along With Using Deep Learning Model, the performance classification can be enhanced. The Decision-Making Process for classification is further enhanced by applying the Weighted Average or Mean Probability Techniques for Decision-Making.	The combination of clustering & Deep-Learning Models increases the accuracy of forgery detection and reduces the number of errors in classifying forged signatures.
[3]	2014	The use of Local Binary Pattern (LBP) Features from the Signature Images and Classifying Them in an Offline Signature Verification System can be used to Distinguish Between Genuine Signatures and Fake/Forged Signatures More Effectively.	The use of Texture-based Features improves the ability of the Verification System to Distinguish Between Genuine Signatures and Forged Signatures.
[4]	2014	Using Artificial Neural Networks, Computer Vision Techniques along With Detecting & Verifying Signature Recognition.	Using Artificial Neural Networks with Computer Vision Techniques will enhance the Detection of Fake/Forged Signature Recognition by Learning Complex Visual Patterns Through Signature Recognition.
[5]	2015	The study analysed various offline signature verification techniques, such as Feature Extraction, Pre-processing, and Different Classification Methods.	The study gives a complete analysis of all proven techniques and illustrates Feature Selection as an Essential Method to Improve the Accuracy of Signature Verification.
[6]	2015	This article presents image-processing techniques (including filtering, normalizing, and extracting features) that can be applied to enhance signature images for classification purposes.	These techniques improve the clarity and quality of signature images, thus increasing the performance of respective classifications.
[7]	2017	Wavelet entropy-based feature extraction is employed in combination with a neural network classifier for signature recognition.	This method captures both the spatial and frequency domain information of signatures, which will improve the recognition accuracy..

[8]	2017	CNN (Convolutional Neural Networks) are the model of choice for automatically learning and extracting discriminative features from offline handwritten signatures..	The use of deep learning techniques significantly advances the representation of features and enhances the accuracy of signature verification algorithms.
[9]	2019	SigNet (Siamese Convolutional Neural Network) can, therefore, create models used for offline signature verification that are independent of who wrote the signature being compared.	The increased use of CNNs will help improve signature verification systems by increasing the accuracy associated with model comparisons across different users.
[10]	2024	Using support vector machines (SVM) and principal component analysis (PCA), data will be reduced in dimensionality.	Increases computational efficiency and enhances classification performance.
[11]	2025	An analysis for signature image processing has been developed by employing a deep-learning framework based on Transformers.	Deep learning that is advanced enhances pattern identification and detects forgeries more accurately. Multi-stage classification reduces noise and increases accuracy for verifying original signatures.

III. PROBLEM FORMULATION

The raise in the requirement for secure authentication in banking, especially with the increase in reliance upon electronic transactions and remote verification of legal documents, has meant that signature verification is of particular significance today. Unfortunately, signature verification is still typically performed manually and thus is subject to human error and can be slow to perform.

There are a number of factors that must be considered when designing an automated signature verification system:

- Natural variation in the way someone signs their name means that regardless of how closely the signature is reproduced at different times by the same person, there will always be some level of variability between those signatures.
- The use of expert or high-quality forgeries makes signatures hard to verify. An experienced forger may be able to sign exactly as the person they are impersonating signed; therefore, some signatures are extremely difficult to detect as forgeries.
- The writing conditions experienced by the user may have affected the signature, either positively or negatively.
- Rapid extraction of features and efficient classification techniques are critical for the accurate differentiation of original signatures compared to forged signatures.

It is important, therefore, to have an effective signature verification system that is capable of identifying signature patterns with enough accuracy to differentiate genuine signatures from fraudulent signatures with a sufficiently low rate of error.

IV. SOLUTION DOMAIN

Automated signature verification systems tackle these challenges using many different techniques from various fields, such as pattern recognition, machine learning, and image processing.

A general solution framework may include the following elements:

- Data Acquisition: Signatures can be collected through scanners (offline) or digital pens/tablets (online).
- Preprocessing: Noise reduction, normalization and segmentation of signatures are performed to enhance signature quality.
- Feature Extraction: Extracted features will consist of geometric characteristics, pressure profiles, velocity profiles, acceleration profiles and structure.
- Signature Comparison: Feature comparison will take place between the features of the signature being evaluated and the stored signatures using similarity measures or profile distance measures.
- Decision-Making: A threshold value will be determined to identify a signature as either authentic or forged.

In addition, current signature verification research incorporates machine learning models and deep learning models to enhance accuracy while minimizing false positives and false negatives.

V. CONCLUSION

The importance of offline signature verification in biometric authentication systems cannot be overstated, especially within financial transactions, legal documentation, banking applications, and identity verification systems. Despite this use, one of the major challenges that both researchers and industry practitioners have with offline signature verification is the detection of forged signatures due to differences in writing styles, environmental conditions when signatures are captured, and the fact that some skilled forgers are able to produce forged signatures that look very similar to authentic signatures.

As a result, developing accurate and reliable automated offline signature verification systems has become a significant research area in the realm of image processing and machine learning.

Many different groups of researchers over the past several years have proposed different methods of implementing offline signatures verification and detection of forgeries through the use of image processing, machine learning, and deep learning techniques. The majority of these techniques follow a standard process flow that consists of 3 overall phases: image pre-processing, feature extraction, and classification.

The image pre-processing phase consists of applying various techniques to remove noise, binarize, normalise, and perform edge detection on the image in order to improve the quality of the captured signature image. In the feature extraction phase, as well as structural and geometrical features of the signature, there are specific characteristics/features that can be collected. The analysis of the extracted features can be used as input to machine learning classifiers, specifically SVM, ANN, Random Forest and KNN classifiers/classifications, to determine if the signature is a genuine or forged signature.

The traditional machine learning methods used in signature recognition typically use hand-crafted feature extraction methods such as: Local Binary Patterns (LBP), Gray Level Co-Occurrence Matrix (GLCM), Histogram of Oriented Gradients (HOG), and morphological features. These types of feature extraction techniques do a great job of capturing some of the characteristics of signature images, but they have difficulty capturing the complex patterns found in signatures written by an expert forger. In contrast, recent advances in using deep learning approaches (i.e. Convolutional Neural Networks or CNNs, Siamese Networks, and transformer-based models) have produced a great deal of interest because they can automatically learn discriminative features directly from signature images. The performance of the deep learning models has been greatly improved when compared to the classification accuracy and forgery detection performance of traditional machine learning methods.

As a result of these advances, there are still many challenges associated with offline signature verification systems. For instance, most deep learning approaches require large amounts of training data and can require significant computational resources to train and deploy the models. Furthermore, many of the existing deep learning methods do not provide any type of interpretability, so you cannot easily understand

why the system made a specific classification decision. In addition, there is variation in handwriting style and changes in conditions when signing signatures; as well as a large number of highly skilled forgers, which all make signature verification difficult.

From the analysis of previous research, it is clear that different techniques will offer different levels of efficiency; that is, they may yield more or less effective outcomes based on the dataset being analyzed as well as the method of feature extraction, and the classification algorithm. Although machine-learning techniques typically yield moderate accuracy with lower computational costs, deep-learning techniques generally yield much higher accuracy but require substantial advanced hardware resources and comparatively long training times. Therefore, there is a need for the development of frameworks that are efficient, reliable and explainable, and that use the strengths of both machine learning and deep learning.

Going forward, efforts should focus on developing hybrid systems that combine some form of image processing technology with XAI technologies in order to increase both accuracy and interpretability. Advanced feature extraction techniques combined with the use of transfer learning methods and transformer networks will help to augment signature verification systems. Development of large benchmark datasets, as well as real-time signature verification systems, will also assist in the enhancement of the robustness and practical application of these types of systems.

To conclude, computer-based signature verification systems have the potential to streamline efficiency and improve the reliability of authentication processes. As further progression occurs within the areas of image processing combined with machine learning and deep learning technologies, automated offline signature verification systems may help to deter fraud, increase security, and reduce the level of human interaction required for authentication tasks.

REFERENCES

[1] Md. Iqbal Quraishi, Syeda Khaja Mohiddin and B. Ramesh, “Offline Signature Verification Using Ripplet-|| Transform and Artificial Neural Network,” International Journal of Computer Applications, vol. 79, no. 12, pp. 20-25,2013.
DOI: https://doi.org/10.5120/13771-1673

[2] Othman O. Khalifa, Aisha Hassan A. Hashim and Sayed A. Samad, “Offline Signature Verification and Forgery Detection: A Review,” International Journal of Computer Science and Network Security,” vol. 11, no. 3, pp. 170-176,2011.
DOI: https://doi.org/10.1109/ICICS.2011.6173635

[3] Rameez Wajid, Hafiz Malik and Muhammad Imran Malik, “Offline Signature Verification Using Local Binary Pattern Features,” International Journal of Pattern Recognition and Artificial Intelligence, vol. 28, no. 7, pp. 1-15, 2014.
DOI: https://doi.org/10.1142/S0218001414560036

[4] Gautam S. Prakash, B. Shekar and K. Ramesh, “Offline Signature Verification and Forgery Detection Using Computer Vision and Neural Networks, " International Journal of Computer Applications, vol. 96, no. 18, pp. 15-20,2014.
DOI: https://doi.org/10.5120/16895-6921

[5] Haritha Damarla and K. S. Rao, “Offline Signature Verification Techniques,” International Journal of Computer Science and Information Technologies, vol. 6, no. 3, pp. 2456-2460,2015.
DOI: https://doi.org/10.1109/ICIP.2015.7351085

[6] Neelima Singh and Ritu Singh, “Offline Signature Verification Using Image Processing Techniques,” International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 6, pp. 450-455,2015.
DOI: https://doi.org/10.23956/ijarcsse.v5i6.110

[7] K. Daqrouq, H. Sweidan, A. Balamesh and M. N. Ajour, "Off-Line Handwritten Signature Recognition by Wavelet Entropy and Neural Network Entropy," vol. 19, no. 6, pp. 1-8,2017.
DOI: https://doi.org/10.3390/e19060252

[8] Luiz G. Hafemann, Robert Sabourin and Luiz S. Oliveria, "Learning Features for Offline Handwritten Signature Using Deep Convolutional Neural Networks," Pattern Recognition, vol. 70, pp. 163-176,2017.
DOI: https://doi.org/10.1016/j.patcog.2017.05.012

[9] S. Dey, A. Dutta, J. I. Toledo, S. K. Ghosh, J. Llados and U. Pal, "SigNet: Convolutional Siamese Network for Writer Independent Offline Signature Verification," Pattern Recognition Letters, vol. 128, pp. 182-189,2019.
DOI: https://doi.org/10.1016/j.patrec.2017.07.024

[10] A. Guerbai, Y. Chibani and B. Hadjadji, "The Effective Use of One -Class SVM Classifier for Handwritten Signature Verification Based on Writer-Independent Parameters," Pattern Recognition, vol. 48, no. 1, pp. 103-113,2015.
DOI: https://doi.org/10.1016/j.patcog.2014.07.015

[11] S. Y. Ooi, A.B.J. Teoh and Y. H. Pang, "Radon Transform Based Approach for Offline Signature Verification," Expert Systems with Applications, vol. 40, no. 17, pp. 6838-6846,2013.
DOI: https://doi.org/10.1016/j.eswa.2013.06.042

[12] S. Bhatia, P. Bhatia, D. Nagpal, S. Nayak, "Online Signature Forgery Prevention," International Journal of Computer Applications, Vol. 75, no. 13, pp. 0975 -8887,2013.

[13] Chang, W., Shin, J., "DPW Approach for Random Forgery Problem in Verification," Fourth Online Handwritten International Signature Conference Networked Computing and Advanced Information Management, vol.1, pp. 347-352, 2008.

[14] J. Fierrez, J. Ortega-Garica, D. Ramos, J. Gonzalez Rodriguez, "HMM-based On-Line Signature Verification: Feature Extraction and Signature Modelling", Pattern Recognition Letters, vol.28, No.16, pp.2325-2334, December 2007.

[15] M. Hanmandlu, M. Hafiz, V. K. Madasu, "Offline Signature Verification and forgery detection using fuzzy modelling," Pattern Recognition 38, pp. 341-356,2005.