DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

A Survey: Handwritten Signature Verification Using Different Methods

Zainab A. Yakoob
Department of Computer Sciences, University of Technology, Baghdad, Iraq
Zainab.a.yakoob@uotechnology.edu.iq

Abstract*— Nowadays, with the development of correspondence via the Internet and the crises that occurred after 2019, many institutions in various fields, whether public or private, and banks and financial transactions, began to carry out most of them via the Internet and needed to sign various documents electronically. There are many problems with the signature images, documents, transactions, or files that make the verification process difficult or require preprocessing for signature. One important part of biometric authentication is signature verification, which tries to separate genuine signatures from fraud. Both online and offline signature verification techniques are examined in this survey. In offline systems, properties like size, shape, and texture are extracted for comparison from static representations of signatures. On the other hand, online systems collect dynamic data such as pen pressure, acceleration, and velocity. This paper gives a comprehensive assessment of the current studies and outcomes in the last 8 years in the subject of online and offline handwritten signature verification. It is possible to improve verification accuracy by creating a hybrid system that combines the advantages of both methods. This study investigates cutting-edge strategies to enhance the functionality of signature verification systems, such as machine learning algorithms and feature extraction techniques. The ultimate objective is to create dependable and strong systems that can successfully thwart intricate forgery efforts. Whereas the accuracy in most offline research may reach 100%, and this may be mostly due to the fact that the matching is of one-to-one type, while in online methods is one-to-many.*

Index Terms*— Online signature verification, offline signature verification, genuine, forgeries.*

I. INTRODUCTION

One of the most ancient biometric used during decades is signature. It used in various authenticated legal support applications include bank checks and documents, authors identification, face and iris recognition and medical detection in addition to numerous other application [1]. Handwriting is one of the most important identities for the human it shows its learning behavior, Researchers in the fields of forensic sciences and biometrics are very interested in writer identification and authenticity [2] [3]. Identification and verification are two different processes. Verification uses a person's biometric to confirm that the person is who they believe they are, whereas identification uses the person's biometric to identify the person from a batch that is available. verification of an individual by way of signatures. The genuine signatures and the forgery signatures are part of the verification procedure [3]. Handwritten signature is widely used nowadays, different methods are developed and applied recently in order to verify or identify signatures. Many methods in machine learning and artificial intelligence are used to get the best verification [4]. Thus, the signature characteristic can be used to construct authentication systems for security and fraud protection [5]. Compared to alternative verification technologies,

Received 20/August/2024; Accepted 06/October/2024
 ISSN (Print) 1811-9212 *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

signature verification systems (SVS) offer several benefits, such as reduced time and energy consumption, decreased fraud risk during authentication, and less chance of human error during the signature process [6]. The verification of signatures presents two primary challenges. One is that there is a lot of variety both intra-class and inter-class. It is vital to extract and choose more thorough and representative signature elements since the author's true signature will alter with time, age, and other variables, and the forger will likewise copy the signature with enough training. Secondly, in real-world circumstances, genuine signatures might be gathered in tiny groups for training, and unqualified data is another issue that needs to be resolved [4].

The aim of this review paper is to offer a comparative summary of the most recent research and findings in the subject of handwritten signature verification. together with the methods employed to categorize or extract signature traits, is. Over ten papers are compared, which can be helpful in determining the most favorable result and providing an opportunity to enhance them. This paper is organized as follows: In Section II, types of signature verification are introduced. In Section III, the types of forgeries are explained. Section IV: Literature review is presented, with a comparative table between them. In Section V, present the verification system's most common limitations and better performance, as well as a discussion and conclusion.

II. TYPES OF SIGNATURE VERIFICATION

A biometric authentication technique called signature verification verifies the validity of a signature by comparing it to a reference signature. Knowing these kinds and their traits can help you select the best approach for the circumstances surrounding your use case [5]. There are basically two kinds:

A. Online Signature Verification

Online verification is the term for dynamic verification signatures that collect and process information in real-time. It includes four stages. The first stage is data acquisition, which takes a capture of the signature after signing using modern devices such as tablets or digital pens. The capturing process takes the pressure of the pen, velocity, and time as dynamic features and the shape and size of the signature as static features. These features make for good data for authentication by comparing it with previously stored data [1]. The second step extracted features from the signature image through a pre-processing stage. This process includes a lot of different operations like scaling, thinning, cropping, rotating, and binarization. The image will be clean and clear for the next step [7]. The third stage, which is the backbone of signature verification, is feature extraction, which involves the extraction of local and global features; each of them has its own specific features. These features are extracted from the signature image as a forgery factor [8]. The verification process includes multiple processing steps, such as applying classification methods where the signature image is trained using one or more classifiers. In order to train the input, the majority of researchers have provided a variety of learning strategies. The test input signature image computes a score and is compared to the trained image score. After that, the decision is made to decide whether the signature is original or forged. This is done by computing the distances between these scores using the Euclidean measure, the City Block measurement, or others [7] [9] [10].

Online signature verification even though it has a major importance but also has several problems. First, security issues require special devices like smart phones or tablets, which can be easily exposed to malware or other threats. Also, the key exchange needs a strong cryptography algorithm. And secondly, a technically skilled forger can replicate the signing and trick the system, so the system must be trained enough against simple forgeries. Third, user acknowledgment for the use of hardware and software for the online verification system must be good enough to be able to solve the network problem

Received 20/August/2024; Accepted 06/October/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

immediately. Fourth, the authentication of the legal documents needs more factors. Finally, the cost of the system, which needs hardware devices and software implementation with continuing maintenance for them [11] [12]. *Fig. 1* shows Signature verification system.

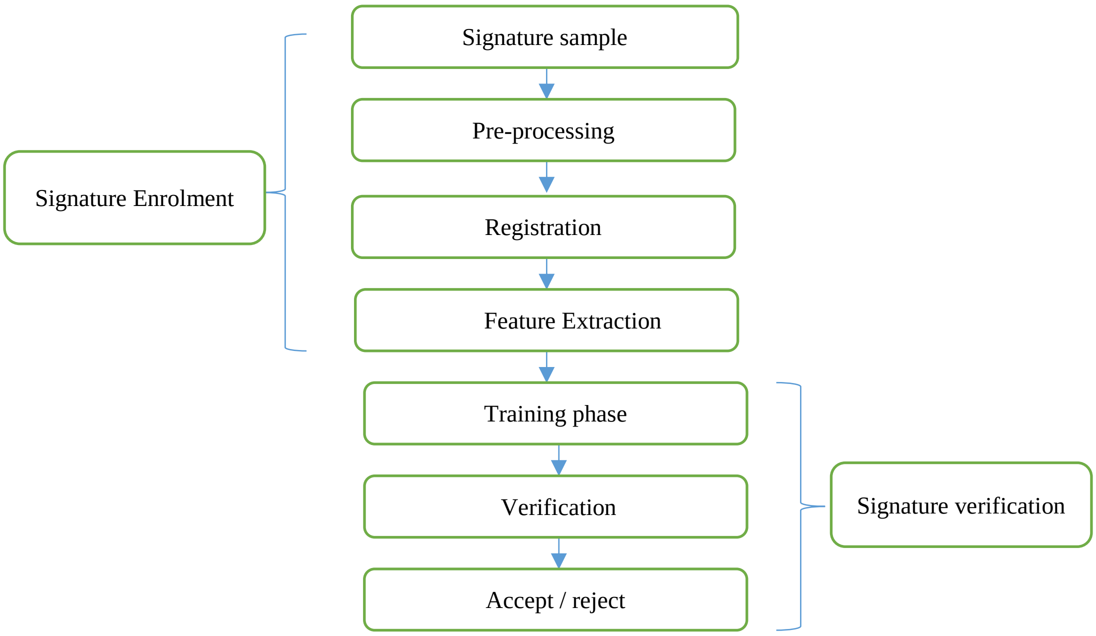

FIG. 1. SIGNATURE VERIFICATION SYSTEM [14].

B. Offline Signature Verification

Offline verification is the term for static verification signatures, it does not require real-time operation because the recognition works offline. Offline verification depends on digitizing the signed paper by the user using a camera or any other device that converts it to a digital copy. It operates only on two dentitional image data [13]. As a consequence, offline signature verification becomes an increasingly difficult task. Signatures can differ between samples taken from the same person due to a number of characteristics, such as age, physical condition, psychological state, and health. Researchers will find it much harder to achieve offline signature verification as an effect of all of this [14]. Regardless, there are some clear benefits to offline signature verification, even with its reduced accuracy. Because it doesn't require specific input devices, it is more widely applicable and more accessible. Additionally, the potential uses of offline signature verification are wide, allowing it to distinguish between authentic signatures written by authorized authors and forged signatures generated by dishonest people [15].

One of the most typical problems and challenges when using signature verification is the lack of transparency and illegibility of the signature. There are many explanations why a signature cannot be read. Among these explanations are: First, old documents containing pen and paper signatures have begun to fade with time, making the written signatures unrecognizable. Secondly, a written signature loses its structure, transparency, and clarity when liquids like water, coffee, or tea are dropped over. Third, writing something, like a title, address, pattern, or stamping, on the signed signature makes it more difficult or, in rare situations, impossible to recognize the entire signature. Fourth, using light-colored pens or an environment where the signature's structure and readability are covered by a loss of written color over time [16]. Fifthly, there is a need for an image-based signature to be

Received 20/August/2024; Accepted 06/October/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

submitted [13]. Finally, offline handwritten signatures include a large user base (classes), and there are just a few training examples per writer with a significant level of intra-class variability. Also, the vector length for each signature image has a high-dimensional value [17].

III. TYPES OF FORGERIES

- **Random forgery** Usually, the forger signs without sharing information about the signer's personality or what their signature looks like. Even a normal person is able to recognize this type of forgery.
- **Skilled Forgery** A signature forger is fully aware of the signer's identity and the original signature's appearance. Only those with copying experience can most closely replicate this signature.
- **Unskilled Forgery** A signature forger is just aware of the signatory's name; they have no previous information about the signature, these types explained in *Fig. 2*. [18] [19].

FIG. 2. SIGNATURE FORGERY TYPES [18].

IV. LITERATURE REVIEW

In [20] discussing online recognition of handwritten signatures. It was applied to the touch feature in mobile devices, where the properties were modified in the phone settings to operate the database built by the researchers. The researchers worked on representing the signature as a discriminative feature vector derived from various properties taken from the histogram. This research was first applied to the well-known MCYT-100 and SUSIG data sets. The results showed simplicity and effectiveness in implementation on the State-of-the-Art algorithm. Then, the researchers built a database of signatures taken from different mobile phones and applied the system to it. The results illustrate the problem of intra-user variation in signature through training strategies to mitigate these problems.

In [21] , they used area, Euler's number, eccentricity, standard deviation, centroid, skewness, kurtosis, and orientation to get geometrical features. For recognition and verification, they use an artificial neural network. The system applied to signatures obtained from persons whose signature the system requires for authentication. The efficiency is about 86.67%, with a threshold of 80%. Simulation result. The method is reliable and distinguishes between genuine and fake signatures with clarity.

Received 20/August/2024; Accepted 06/October/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

In [22] , the two GoogLeNet architecture methods (Inception-v1 and Inception-v3) are used. The GPDS database was used, which contains signatures for 1000 users: 24 genuine and 30 forged. The features extracted in Inception-v1 are averaging from mapping 7*7 to 1*1. In Inception-v3, feature maps are created using convolutions and separate pooling; both sets of feature maps are then concatenated and sent to the subsequent inception module. The accuracy rate was 83% for Inception-v1 and 75% for Inception-v3.

In [8] , the researchers use two methods to extract texture features (discrete wavelet and local quantized patterns). then Support vector machines of one class are used to generate two distinct authenticity scores for a given signature. The scores from the two one-class SVMs are then integrated to provide the final verification score through a score-level classifier fusion based on the average approach. Four different datasets are used to get the results for the proposed method. The accuracy was high, and depending on the kernel function values used.

In [9], protecting mobile transactions on multi-touch mobile devices, they suggest an online signature verification system based on crucial segments. To capture the intrinsic signing behavior encoded in every user's signature, our system finds and takes advantage of the segments that stay the same within a user's signature. This method is able to extract meaningful aspects from a user's signature that characterize the user's behavior and physiological state throughout the signing process, in addition to the geometric arrangement of the signature. In order to provide reliable signature verification even when there are geometric distortions in the signature due to variations in writing sizes, orientations, and placements on touch screens, we create methods for normalizing and interpolating signatures. The experimental study, which involved 25 subjects over the course of six months, demonstrates how accurate and resilient this system is against signature forging attempts.

In [14] , the dataset is collected from 10 people, and they get from each of them 10 different signatures using traditional ink stamps. Then, these signatures are pre-processed to get ready for verification. Preprocessing images and removing noise using a median filter, extracting features, and matching the original image with the forgery image. discrete wavelet transforms used for feature extraction. The recognition rate for this paper was 100%.

In [16] , they are trying to solve the problem of unreadable signatures by adding noise using Salt and Pepper, Gaussian, and Gaussian Blur filters. They use the Generative Adversarial Network as a high-quality data synthesis method, and for the unique signatures, they use lightweight deep learning architectures. The system was evaluated using different convolutional neural network approaches. The accuracy rate was registered for each CNN method, and it was between 83% and 91%.

In [23] researches implemented a system for bank’s customer’s transaction which must have their signature on the documents, so the system verified their signature in offline situation depending on clean reference signatures. This paper has two essential steps remove the stamp from signature using CycleGAN and represent the signature using CNN. A system tested on customers database and on public dataset Tobacco-800 dataset. They improve the signature verification performance because of the use of stamp cleaning, which is more effective than collecting images for different stamps in order to remove them from the signature space. Accuracy rate computed in a group of documents and images was 91.66 and computed as individual with rate 89.25.

In [4] extract static features using support vector machine (SVM), it extracted geometric features to represent the general image information. This paper use gray-level Co-occurrence matrix and histogram of oriented gradient to get the texture features. These features are combined together to obtain a vector contain image content. Also, dynamic features extracted using dynamic time warping (DTW). Static and dynamic are unified online and offline features using score fusion and use the integrity of the classifier, then produce a score fusion method based on accuracy (SF-A). A smart pen used in the same time to get offline and online signature. This work collected 1200 online and offline images as dataset because it’s difficult to find simultaneously offline images with its corresponding online images. The

Received 20/August/2024; Accepted 06/October/2024
 ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

result was tested on 3,5,8, and 10 real signature images as samples for training, using SVM, once as positive samples and another as negative samples. The accuracy rate using SF-A was respectively for 3,5,8, and 10 samples, 93.08,94.92,97.33 and 97.83. the limitation is there no obvious time execution.

In [13], a verification mechanism for handwritten image-based signatures is suggested in this work to determine whether the image-based signature is authentic or replica. The system compares the examined image-based signature with the live stream of an audio-based signature and provides the matching findings. Classification and/or correlation between the two signatures are used to match. The authenticity of the image-based signature is confirmed if the matching displays a similar class or a score higher than a set threshold; if not, it is marked as fabricated. Twenty people in all took part in the experiment; each person signed four documents in different contexts and produced a genuine signature. The system demonstrated 95% accuracy with a one-class SVM and 100% accuracy in a double-blind scenario.

In [7] two approaches are used in order to solve the problem of signature verification—digital, manual, or some other method. These methods (decision tree and support vector) were used to identify the different properties of the signature and produce a proposed method named DT-SVM. Furthermore, the characteristics were enumerated following the measurement of the impacts. The features that are extracted may be global, depending on shape, dynamics, geometry, and miscellaneous, or local, depending on time, velocity, loop, and baseline. The proposed DT-SVM resulted in an accuracy rate equal to 96.6 when tested on 192 sets of signatures.

In [17] , the signatures are normalized using a histogram orientation gradient in order to enhance accuracy. For prediction, deep learning is used for better verification. The system was applied using the SIGMA dataset, which was collected from 200 individuals and contains 4000 genuine and 2000 skilled forged. The results were successful and higher than 97.1%.

In [24] Optical Mark Recognition (OMR) was used a tool in python and multiclass convolutional neural network methods. This paper applied as offline signature verification, it trained real images got form dataset for attendance sheets created by the campus academic management platform. This dataset contains a paper sheet for student attendance, the header of the sheet have a barcode contain information about that class. The problem here that the signature field is small about 30*215 pixels. The small size makes it difficult to gain the most features from the student signature. This problem was solved by using machine learning. A MLP classifier was used for mark recognition to improve the binary classification model. After that, CNN was used to specify if the signature is legitimate or not. The best verification rate was 85%. The problem with this was that time accuracy was not mentioned.

In [25] implemented a system for offline signature verification based on extracted features by merge local ridge feature and two level Haar wavelet. Overlapping applied on the Haar image sub-band with fragmented it into blocks. This paper got 6 different signatures from 100 person for each and collect 600 signature sample for its database in a bitmap image format. The accuracy rate for this paper 100% with false reject rate was 0.025 while the acceptance rate was 0.03.

In [26] , they introduce a method using a deep convolutional neural network and extract local features using CNN in order to enhance the verification method. The dataset was built by getting different signatures in different situations from various people. The registered results were successful and equal to 95.5%.

In [5] , the signature boundary pixels are extracted from the quasi-straight line segments using simple combinations of the directional codes. The feature comes from different quasi-straight line classes. The quasi-straight line segments combine tiny curvatures with straightness to produce a strong feature set that can be used for signature verification. SVM is used for classification, and the tested datasets are CEDAR and GPDS-100. Many people (100 signers) achieve good results; however, the poor performance of certain individuals reduces the average accuracy overall. Different results are

Received 20/August/2024; Accepted 06/October/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

registered depending on the number of signatures collected by different persons from the previously mentioned dataset.

In [27] , They tried to solve the problem of processing large documents in less time, so they proposed a method by using convolutional neural networks and backpropagation in image processing. The features are extracted from documents, files, checks, and other legal ones by extracting relevant features from them like size, curvature, shape, and orientation. The Kaggle dataset was used, which contains 300 images, of which 150 are genuine and 150 are forgeries. They used support vector machines, artificial neural networks, or random forests to retrieve features from genuine and fake signatures. The model introduces 95% training accuracy and 60% validation.

In [28] a study for writer independent offline signature verification has been proposed with the goal of enhancing the overall accuracy measurements. Thus, to verify signatures and maximize overall accuracy measurements, a validated approach relies on deep learning through convolutional neural networks (CNNs). An English signature dataset is used to train the newly presented model, which used a dataset of scanned handwritten signature photos from several people to test a method for differentiating real signatures from fakes. To be utilized for training and validating the suggested model, the 720 photos in the dataset were gathered, 360 of which were photographs of real signatures and another 360 of which were images of fake signatures. The deployable model is used to predict new information from the Arabic signature dataset in order to determine if the signature is authentic or fake. This process is known as model assessment. Based on the validation dataset, an overall accuracy of 95.36% was obtained.

After studying The previous papers, Table I introduced in order to shows a compression between them.

TABLE I. A COMPRESSION BETWEEN LITERATURE REVIEW

Reference	Dataset	Methods	Features	Accuracy %
[20]	MCYT-100 SUSIG	the State-of-the-Art	discriminative feature vector derived from various properties taken from the histogram، applied on touch feature in mobile devices	93%
[21]	signatures got from persons whose signatures the system requires for authentication	artificial neural network (ANN)	Geometric features(Area, Euler’s Number, Eccentricity, Standard deviation, Centroid, Skewness, Kurtosis and Orientation)	86.67
[22]	GPDS Synthetic signature	Two versions of CNN (Inception-v1 and Inception-v3) of GoogleLeNet architecture	In Inception-v1 each feature are averaging from map 7*7 to 1*1. in Inception-v3 feature maps are created using convolutions and separate pooling; both sets of feature maps are then concatenated and sent to the subsequent inception module.	83% (Inception-v1) 75% (Inception-v3)
[8]	MCYT GPDS-300 BHSig260 CEDAR	Bi-class SVMs (B-SVM)	discrete Wavelet (DWT) local quantized patterns (LQP)	Accuracy was high and depending on the used Kernel function values
[14]	data based on collecting samples of 10 people and 10	Preprocessing image and remove noise using median filter, extracted features	DWT	100

Received 20/August/2024; Accepted 06/October/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

	signatures for each person	and matching the original image with the forgery image		
[16]	Indic scripts	Generative Adversarial Network (GAN) + Lightweight Deep Learning Architecture ((MobileNet, SqueezeNet, ShuffleNet))	geometric features after adding noise by Gaussian , Gaussian Blur and salt and paper	With Gaussian in (MobileNet=91.01 SqueezeNet=89.39 ShuffleNet=83.33) With Gaussian Blur in (MobileNet=93.68 SqueezeNet=89.68 ShuffleNet=87.04) With salt and paper in (MobileNet=89.37 SqueezeNet=87.21 ShuffleNet=85.28)
[23]	A system tested on customers database and on public dataset Tobacco-800	remove the stamp from signature using CycleGAN and represent the signature using CNN	fully-connected layer of VGG-16, convolution layer of ResNet-50	Rate in a group of documents (91.66) as individual (89.25)
		SVM	GLCM	90.33
			HOG	93.33
	GPDS		Geometric	78.92
[4]	(with ten training samples)		GLCM+HOG	94.67
			Geometric+texture	95.17
		DTW		92.42
		SF-L		97.58
		SF-A		97.83
[13]	The system maps the live stream of an audio‐based signature with the investigated image‐based signature	VSHIS	Correlation coefficient One-class SVM	100 95
[7]	performed in various language databases which contain 192 set signatures	machine learning (SVM and decision tree)	Global (shape and geometry) Local (time , velocity, Loop and baseline)	96.6
[17]	SIGMA	signature length normalization	Histogram Orientation Gradient (HOG)	97.1%
[24]	attendance sheets created by the campus academic management platform	Optical Mark Recognition + multiclass convolutional neural network	local feature extraction + CNN	85%
[25]	600 signature prints collected from 100 persons	Haar Wavelet Transform and overlapping partitions algorithms	merge local ridge feature and two level Haar wavelet energies.	100%
[26]	Build new dataset by signatures got from different persons	deep convolution neural network	local feature extraction + CNN	95.5%
[5]	CEDAR GPDS-100	SVM	Quasi-straight line segments	Good results depending on the number of signatures collected by different persons

Received 20/August/2024; Accepted 06/October/2024

ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

[27]	Kaggle	Convolution Neural Networks(CNN) , Backpropagation	extract relevant features like size, curvature, shape, and orientation	95% training 60% validation
[28]	English signature dataset, Arabic signature dataset	Construct Model Architecture based on CNN	Max pooling layer is proposed after each convolution layer to preserve worthy features	95.36%

V. DISCUSSION AND CONCLUSIONS

In this research, many recently published papers were studied, and it was concluded that there are different datasets that were used, some of which are available on the Internet and contain many pictures of signatures for different types of people with various numbers of genuine and forgery signatures. These datasets differ in the number of pictures used, some of which are original and some of which are forged, and this data is used by researchers to compare the results they obtain. Some of them built a database specific to their research, and the results were studied by them. Many preprocessing methods even it has some limitation like, Information could be Loss like in smoothing or thinning may cause information to be lost that is crucial for verifying signatures. The outcomes can be greatly impacted by the preprocessing parameters selected. Erroneous parameter configurations may result in artifacts or a reduction in image quality.

A number of preprocessing methods can be computationally costly, particularly if they include complex computations. Otherwise, preprocessing is used in order to exploit its advantages; some of them are used to remove noise or enhance the images to save time and improve the efficiency of the verification system, and others, like normalization, are used to prepare the dataset or test images for high-feature extraction. Preprocessing gives feature extraction algorithms a cleaner input so they can concentrate on data that is relevant. which will lead to a better accuracy rate.

Preprocessing may speed up the verification process. Some preprocessing adds noise to signatures in order to study various situations in signature verification. Preprocessing contributes to a reduction in the system's total error rate. The chosen level of security, the resources that are available, and the particular application needs all heavily influence the signature verification method. In machine learning there are many methods like SVM which is good for high-dimensional data, capable of handling feature connections that are both linear and nonlinear and excellent achievement in prediction; Neural networks are capable of recognizing intricate patterns and connections within data. It’s extremely flexible with many feature sets, and it is suitable for verifying online and offline signatures. while Convolutions Neural Networks (CNNs) provides best results in image-based applications and can automatically extract from the image the pertinent elements and tolerant of changes in vision. These are the most important methods used nowadays and there are many others. If the system is online, it must study the security requirements using advanced machine learning techniques that are resistant to forgeries.

This is generally favored for high-security applications. Artificial signatures can be produced by Generative Adversarial Networks (GANs) for testing or training. It can be applied to strengthen the verification system's resilience. If the system chooses to be offline, then offline approaches may sometimes be easier to utilize because they don't require specialist technology. Systems usually require deep learning, especially if the data is huge. This will require specal hardware and significant computational power, but the results will be high, and deep learning gives good results in online and offline signature verification. The system must test on data that is available in order to compare between works. The

Received 20/August/2024; Accepted 06/October/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

state-of-the-art is frequently represented by machine learning for signature verification; the best option will depend on the particular use case. Before choosing a method, you must carefully consider the limits and requirements of your application in order to get the better verification.

REFERENCES

[1] M. Saleem and B. Kovari, "Online signature verification using signature down-sampling and signer-dependent sampling frequency," *Neural Computing and Applications,* vol. 1, no. 1, pp. 1-14, 2021.

[2] A. Rehman, S. Naz, MI. Razzak and IA. Hameed, "Automatic visual features for writer identification: a deep learning approach," *IEEE Access,* vol. 7, no. 1, pp. 17149-17157, 2019.

[3] R. Kumar, M. Saraswat , D. Ather, M. N. Bhutta ,S. Basheer and R. N. Thakur, "Deformation Adjustment with Single Real Signature Image for Biometric Verification Using CNN," *Hindawi,Computational Intelligence and Neuroscience,* vol. 12, no. 1, pp. 1-12, 2022.

[4] Y. Zhou, J. Zheng , H. Hu and Y. Wang, "Handwritten Signature Verification Method Based on Improved Combined Features," *Applied Sciences (MDPI),* vol. 11, no. 13, pp. 5867-5881, 2021.

[5] M. Ajij, S. Pratihar, S. R. Nayak, T. Hanne and D. S. Roy,, "Off-line signature verification using elementary combinations of directional codes from boundary pixels," *Neural Computing and Applications,* vol. 35, no. 1, pp. 4939-4956, 2023.

[6] V. Hindumathi, J. Chalichemala, E. Ameya, V. Kavya Sri and B. Vaibhavi, "Offline Handwritten Signature Verification using Image Processing Techniques," in *IEEE 8th International Conference for Convergence in Technology (I2CT),*, India, 2023.

[7] U. Jindal, S. Dalal, G. Rajesh, N. Us Sama, N. Z. Jhanjhi and M. Humayun, "An integrated approach on verification of signatures using multiple classifiers (SVM and Decision Tree): A multi-classification approach," *International Journal of Advanced and Applied Sciences,* vol. 9, no. 1, pp. 99-109, 2022.

[8] A. Bhunia, A. Alaei and P.P. Roy, "Signature verification approach using fusion of hybrid texture features," *Neural Computing & Application,* vol. 31, no. 1, pp. 8737-8748, 2019.

[9] Y. Ren, Ch. Wang, Y. Chen, M. Chuah, and J. Yang, "Signature Verification Using Critical Segments for Securing Mobile Transactions," *IEEE Transaction on Mobile Computing,* vol. 19, no. 3, pp. 1536-1233, 2020.

[10] F. Alsuhimat and F. S. Mohamad, "Offline Signature Verification using Long Short-Term Memory and Histogram Orientation Gradient," *Bulletin of Electrical Engineering and Informatics,* vol. 12, no. 1, pp. 283-292, 2023.

[11] K. Egerszegi and P. Erdo, "Problems In The Implementation Of The Electronic Signature," *Periodica Polytechnica Social and Management Sciences,* vol. 11, no. 1, pp. 67-82, 2003.

[12] R. Punam and V. Bhushan, "A Review - Signature Verification System Using Deep Learning: A Challenging Problem," *International Journal of Scientific Research in Science, Engineering and Technology,* vol. 8, no. 2, pp. 295-298, 2021.

[13] A. Almehmadi, "A biometric-based verification system for handwritten image-based signatures using audio to image matching," *The Institution of Engineering and Technology,* vol. 11, no. 1, pp. 124-140, 2021.

[14] S. Muhamed S and M. Al-Ani Sh , "Signature Recognition based on Discrete Wavelet Transform," *UHD Journal of Science and Technology,* vol. 3, no. 1, pp. 19-29, 2019.

[15] A. Al-Azzani O and A. M. Q. Musleh, "Offline Signature Verification Using Deep learning and Genetic Algorithm," *Journal of King Abdulaziz University (Computing and Information Technology Sciences),* vol. 13, no. 1, pp. 86-102, 2024.

[16] J. Majidpour, F. Ozyurt, M. Abdalla, Y. M. Chu and N. D. Alotaibi, "Unreadable offline handwriting signature verification based on generative adversarial network using lightweight deep learning architectures," *Fractals,* vol. 31, no. 6, pp. 1-14, 2023.

[17] Z. Alkattan M., G. Mohammad and T. Aldabagh,, "Offline Signature Biometric Verification with Length Normalization using Convolution Neural Network," *Baghdad Science Journal,* vol. 19, no. 5, pp. 1100-1110, 2022.

[18] H. Salman M. and Z. Hashim, "A Comparative Study among Handwritten Signature Verification Methods Using Machine Learning Techniques," *Hindawi, Scientific Programming,* vol. 10, no. 11, pp. 1-17, 2022.

[19] N. Sharma. K. M , "Review on Off-Line Signature Verification Techniques for Reducing Forgeries/Fraud," *Advances in Computing & Inf. Technology,* vol. 178, no. 1, pp. 161-165, 2013.

[20] S. Akila and A. Sankari , "Signature Verification Through Smartphones", *International Journal of Computer Techniques,* vol. 3, no. 4, 2016.

[21] S. Panchal and V. Yerigeri, "Offline Signature Verification Based on Geometric Feature Extraction Using Artificial Neural Network," *IOSR Journal of Electronics and Communication Engineering,* vol. 13, no. 3, pp. 53-59, 2018.

[22] S. Jahandad , M. Sam, K. Kamardin, N. N. A. Sjarif and N. Mohamed, "Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet Inception-v1 and Inception-v3.," in *Procedia Computer Science: The Fifth Information Systems International Conference*, Malaysia, 2019.

Received 20/August/2024; Accepted 06/October/2024

DOI: https://doi.org/10.33103/uot.ijccce.24.4.6

[23] D. Engin, A. Kantarcı, S. Arslan and H. Ekenel, "Offline Signature Verification on Real-World Documents," in *IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Turkey, 2020.

[24] J. Lopes A.P., B. Baptista, N. Lavado and M. Mendes, "Offline Handwritten Signature Verification Using Deep Neural Networks," *Energies,* vol. 15, no. 1, p. 7611, 2022.

[25] M. Abdul-Haleem, "”Offline Handwritten Signature Verification Based on Local Ridges Features and Haar Wavelet Transform," *Iraqi Journal of Science,* vol. 63, no. 2, pp. 855-865, 2022.

[26] Q. Saad and M. Mukti, "Offline Handwritten Signature Recognition Using Deep Convolution Neural Network," *European Journal of Engineering and Technology Research (EJ-ENG),* vol. 7, no. 4, pp. 44-47, 2022.

[27] B. Shaik, J. M. Katikireddy, V. Kambham and K. Sravani, "Offline Signature Verification Using Image Processing," in *E3S Web of Conferences*, India, 2023.

[28] W. AlKarem, E Khalid and K. Ali, "Handwritten Signature Verification Method Using Convolutional Neural Network," *Iraqi Journal for Electrical and Electronic Engineering,* vol. 20, no. 2, pp. 77-84, 2024.

Received 20/August/2024; Accepted 06/October/2024
