Hindawi
Scientific Programming
Volume 2022, Article ID 8170424, 17 pages
https://doi.org/10.1155/2022/8170424

Review Article

A Comparative Study among Handwritten Signature Verification Methods Using Machine Learning Techniques

Zainab Hashim,[1] **Hanaa M. Ahmed**,[1] **and Ahmed Hussein Alkhayyat**[2]

[1]*Department of Computer Sciences, University of Technology, Baghdad, Iraq*
[2]*Qaultiy Assurance Department, The Islamic University, Najaf, Iraq*

Correspondence should be addressed to Zainab Hashim; cs.20.16@grad.uotechnology.edu.iq

Received 19 July 2022; Revised 25 September 2022; Accepted 29 September 2022; Published 15 October 2022

Academic Editor: Punit Gupta

Nowadays, the verification of handwritten signatures has become an effective research field in computer vision as well as machine learning. Signature verification is naturally formulated as a machine-learning task. This task is performed by determining if the signature is genuine or forged. Therefore, it is considered a two-class classification issue. Since handwritten signatures are widely used in legal documents and financial transactions, it is important for researchers to select an efficient machine-learning technique for verifying these signatures and to avoid forgeries that may cause many losses to customers. So far, great outcomes have been obtained when using machine learning techniques in terms of equal error rates and calculations. This paper presents a comprehensive review of the latest studies and results in the last 10 years in the field of online and offline handwritten signature verification. More than 20 research papers were used to make a comparison between datasets, feature extraction, and classification techniques used in each system, taking into consideration the problems that occur in each. In addition, the general limitations and advantages of machine-learning techniques that are used to classify or extract signature features were summarized in the form of a table. We also present the general steps of the verification system and a list of the most considerable datasets available in online and offline fields.

1. Introduction

Biometrics literally can be defined as biological features of people that can be utilized for recognition purposes. There are two major purposes that biometric recognition systems are basically evolved for: identifying and verifying people [1, 2].

Generally, the applications of biometrics have been deployed for access control as well as monitoring. These applications are yet to become popular in various organizations, such as airports and financial institutes. Biometric systems can be classified based on the physical or behavioral characteristics of people. The physical characteristics refer to the person's biological features like fingerprints, deoxyribonucleic acid (DNA), iris, and facial features. These biological characteristics are so unique to each person and are constant throughout a long time period. Therefore, the biometric systems that rely on physical traits are mostly precise and sufficiently reliable for the purposes of identification, which includes one-to-various comparisons. While behavioral traits refer to the individual's behavior like signature, gait, and voice. These characteristics are subject to change over time, making them easily imitated by a skilled impostor. Hence, it would be a challenging task to design an accurate biometric system that relies on behavioral traits [3].

Even with technological advancements, the handwritten signature remains the most widely accepted means of authentication for legal documents, financial transactions, cheques, loan and mortgage documents, insurance and compliance documents, business contracts, and so on [4]. The purpose of the verification of a signature is to recognize the forged signature so as to decrease the hacking risk and crime. Signature verification systems should differentiate automatically in the case that the biometric sample is indeed

from a claimed individual. In simple terms, this method is utilized for checking whether the query signature is genuine or forged [5].

The objective of this review paper is to offer a comparative overview of the latest studies and results in the field of handwritten signature verification, as well as the limitations and advantages of machine learning techniques that have been used to classify or extract the signature features. The comparison is done between over 20 papers, in which can be useful in finding the gaps in research and giving a chance to improve them.

This paper is organized as follows: In Section 2, the related works are introduced. In Section 3, the idea of identification and verification is presented, and the types of signature features and the types of forgeries are explained. Section 4 discusses the four stages of the verification system. A comparison between the most used online and offline datasets is made in Section 5. In Section 6, another comparison is made between the latest signature verification systems. Section 7, presents the role of machine learning in signature verification as well as the advantages and limitations of the most commonly used classifiers and feature extraction techniques in signature verification. Finally, Sections 8 and 9 present the verification system's most common limitations and performance metrics, as well as a conclusion, suggestions, and future work.

2. Related Work

In 1977, one of the earliest studies on signature verification was conducted. The work was done on features extracted from signatures that have been sectioned into horizontal and vertical areas [6]. Then the studies continued.

2.1. Motivations. Until now, there have been many review and survey articles published on the field of a handwritten signature, such as verification and identification techniques, feature selection and extraction methods, the most famous signature datasets, and the common challenges in this field.

Mushtaq and Mir [7] presented a comparison between the results of various writer-dependent (WD) signature verification systems. Kumar and Bhatia [8] presented a survey paper comparing both Writer-Dependent (WD) and Writer-Independent (WI) handwritten signature verification systems.

Mohammed et al. [9] presented a state-of-the-art the methods that were used for capturing signature data as well as methods and techniques that were used in preprocessing, feature extraction, and verification of handwritten signatures. Sharma et al. [10] presented a comprehensive study on offline signature verification as well as the challenges in that field. Nehal and Heba [11] presented a comparative study of recent off-line and online identification and verification systems; also discussed the stages of verification and identification systems. Our comparative study offers a comprehensive review of the latest studies in the last 10 years in the field of online, offline, and combined handwritten signature verification. The comparison takes place between feature extraction and classification techniques, taking into consideration the dataset, results, and problems of each system.

3. Identification and Verification

The identification and verification of signatures is considered a type of biometric system that is utilized for the identification of individuals. A person can be authenticated using his signature by analyzing the handwriting style, which is subjected to intra-personal and inter-personal variation [12]. Figure 1 shows a biometric handwritten signature verifier.

The applications of biometric identification and verification [13–16] are present in documents and actions of everyday life such as passports, driver's licenses, migration, applications of security, personal device login, voter registration, medical records, and smart-cards [12].

In the process of signature identification, the system should be provided with a user's signature to compare it with the various signatures registered in the dataset, and the similarity results will be calculated. The most similar result will indicate the identified user, whereas there are two basic approaches for signature verification.

These are writer-dependent and writer-independent approaches. In the writer-independent approach, one paradigm is trained for the whole user population and the query signature is matched with the reference signatures in a similarity/dissimilarity space. For the reason that it does not require the systems to be retrained when adding a new writer, this approach is preferred by most researchers [11, 14].

The problem of signature identification and verification goes into three phases: dataset preprocessing, feature extraction, and classification.

The general method of detecting the holder of a signature is identification (recognition), which is a multi-class classification issue. The first stage of the identification system includes scanning and preprocessing the input signatures, then extraction of the special features to be stored in the database. The last stage, also known as the classification stage, involves the comparison of the extracted features to the template signature that has been stored in the database and studies to which class the tested signature is affiliated. Figure 2 shows the identification stages [15].

While the method of decision-making regarding the signature and determining if it is genuine or forged is called verification; therefore, it is considered a two class classification issue. The stages of signature verification resemble the stages of signature identification except in the classification stage, where the tested signature class will be known and its authenticity to that class will be checked [11]. Figure 3 shows the verification stages.

The verification process involves two main methods: model-based verification and distance-based verification. In the model-based approach, the distribution of data is described by generating models like convolutional neural network (CNN), hidden Markov model (HMM), and support vector machine (SVM). While in the distance-based

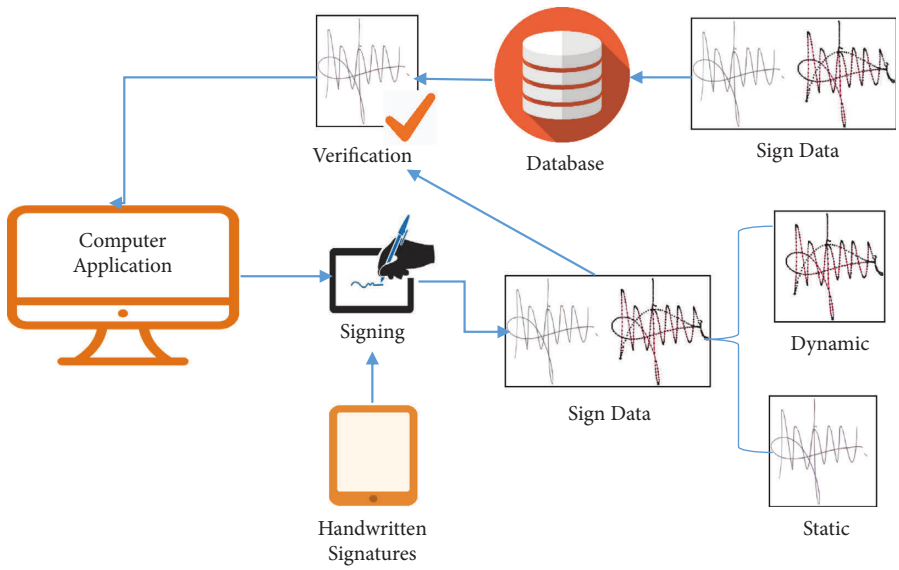
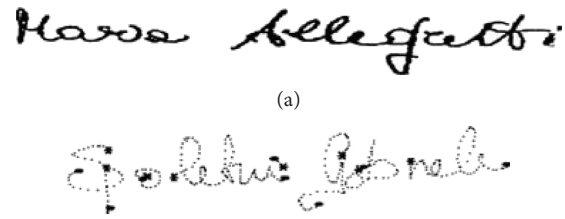


Figure 1: A biometric handwritten signature verifier.

Figure 2: Identification system stages.

Figure 3: Verification system stages.



(a)

(b)

Figure 4: Samples of signature. (a) Offline signature. (b) Online signature [18].

method, the distance measures are utilized for the comparison of the test signature with the reference signature by dynamic time wrapping (DTW) [17].

3.1. Types of Signature Features. Based on the acquisition method, the classification of signatures is made into off-line (static) and online (dynamic) signatures as shown in Figure 4. When signatures are obtained with an ordinary pen and then paper, and then transferred into a digital file by scanning, they are called offline signatures. While the offline signatures represent the signatures that are captured with digital devices such as electronic pens or tablets, representing the online signatures where the real-time features (like pressure, vertical and horizontal position, azimuth, and time) captured [19]. Off-line signature image features are referred to as static features, which are mainly divided into

(i) Local Features.

(ii) Global Features.

The local features include texture features and gradient features. While the global features are predominantly geometric [17]. Online signature data is called dynamic features, which are mainly divided into:

(i) Parameter-based Features.

(ii) Function-based Features.

The parameter-based mainly refers to the duration of the signature and the number of pen-tips across the paper. Function-based features usually refer to signature trajectories and pressure data. Dynamic features based on functional features generally have better results [20].

In the framework of parameter-based features, the signature is described as a vector of elements, and each one is a representative of the value of one feature. Width, height, and average speed are examples of such attributes. The signature dimensions of parameter-based features are all equal [20].

In the framework of function-based features, the signature is described as a multi-dimensional feature set modeled by many time functions. Coordinate, time-stamp, and pressure are examples of function-based features. In general, the function-based feature methods are more preferable because of their dynamic information application. However, these types of features waste a lot of processing time and memory [21]. Figure 5 shows the types of signature verification.

3.2. Types of Signature Forgeries. The handwritten signature forgeries have been classified based on their characteristic features. [22] Many signatures might have the same features.

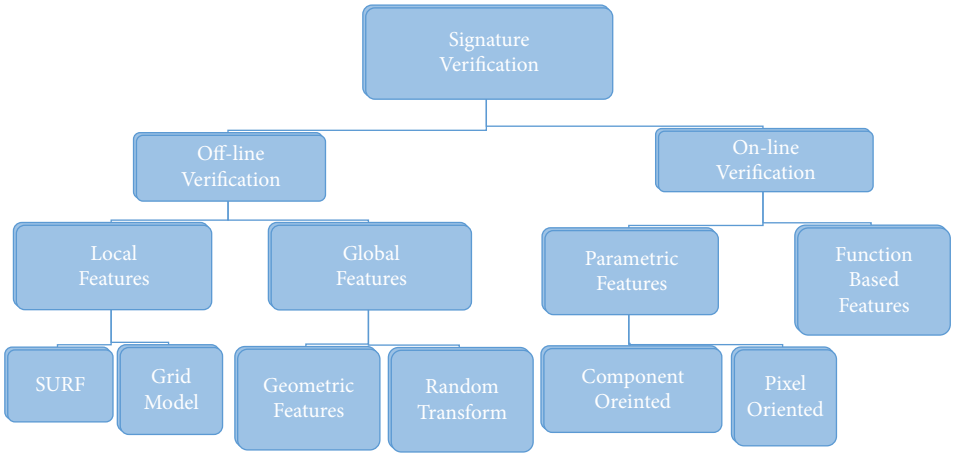


Figure 5: Types of signature verification features.

However, there are many techniques to distinguish between them. The forgeries of handwritten signatures can be divided into three categories :

(1) Random Forgeries: Usually the forger signs without any information about the signer's name and the appearance of the signature. This kind of forgery can be detected very easily, even by human eyes.

(2) Unskilled Forgeries: The forger of a signature knows only the name of the signatory without any other previous information.

(3) Skilled Forgeries: The forger of a signature has full information about the signer's name and the appearance of the original signature. Only professional impostors or people who have experience in copying can imitate this signature in the hardest way. Figure 6 shows each signature forgery type [23].

4. Stages of Signature Verification System

In general, the offline and online signature verification processes consist of the following steps, as shown in Figure 7:

(1) Data acquisition: It is the first step in signature verification and is considered very important. In offline signature verification systems, data can be collected by utilizing off-line acquisition devices, for example, a camera or optical scanner, to scan the signature image to convert it into a digital image. In the online category, the data can be obtained by utilizing many digitizing devices, for example, tablets, electronic pens, and personal digital assistants (PDAs), as shown in Figure 8. However, the researcher can evaluate the performance of the system by using datasets that are publicly available on the Internet [24].

(2) Data preprocessing: preprocessing of datasets is the operation of improving the signature data after reading it. In both online and off-line verification systems, it is considered a very significant stage. In image preprocessing, various operations are applied to signature images; for example, color image to gray image conversion, noise removal, thresholding, morphological operations, cropping, binarization, and signature size normalization [25].

(3) Feature extraction: Some features of the signature are extracted in this step. These extracted features are the inputs to the training and recognition stages. The features can be categorized into global, mask, and grid features. Global features give wavelet coefficients and Fourier coefficients. Mask features give information about the signature lines' directions. Grid features give information about the overall appearance of a signature. The selection of feature sets in signature verification systems is a complicated task due to the fact that the user features must be appropriate for the application [26].

The main techniques of feature extraction for signature are given as follows:

(a) Local and global feature techniques: Global features can be computed from the whole signature, while local features can be computed from a specific signature region.

(b) Functional techniques: In these techniques, the online signature features can be considered as temporary sequences which include information about signature time changes.

(c) Combined Techniques: These techniques are also called hybrid methods, and they depend on merging various techniques from the previous techniques [25, 26].

(4) Classification: Classification is a method for determining the validity of a query signature. After the feature extraction stage, features are matched with those already stored in the database. Features are classified as genuine if they are matched, otherwise forged [27]. Support vector machines, template matching, hidden Markov model, and neural networks or deep learning are the most widely used classification methods [28, 29].

Figure 6: Signature forgery types [22].

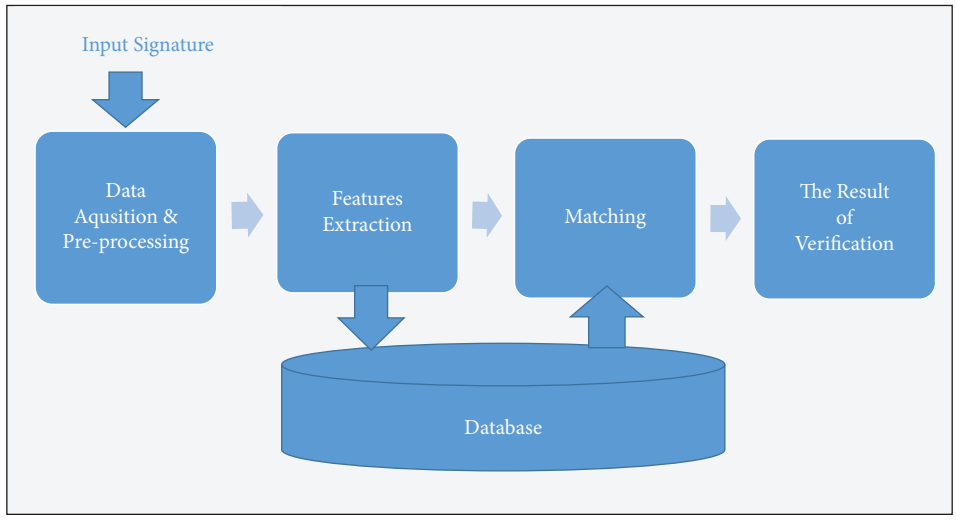


Figure 7: Signature verification system [18].

5. Source of Data and Databases

There is a variation in the size, quality, and characteristics of signature databases. The more signatures for each signer, the more accurate the verification system becomes. The signatures in the database are classified into genuine (genuine symbolize the signer's real signature) and forged (forged are fake copies of the real signature done by skilled forgers). In the verification process, these signatures are utilized for training and testing. In order to provide both training and testing samples, the number of genuine signatures should be large enough [30].

5.1. OnLine Signature Databases. The online database has variations in signer and signature number, sampling rate (which is one of the major properties of the online signature input device), and characteristics. Table 1 shows a comparison between the most used online databases.

5.2. Off-Line Signature Databases. The off-line signature databases, which are normally scanned images, may have variations in color and resolution. The offline signatures have a limited number of features, which makes them

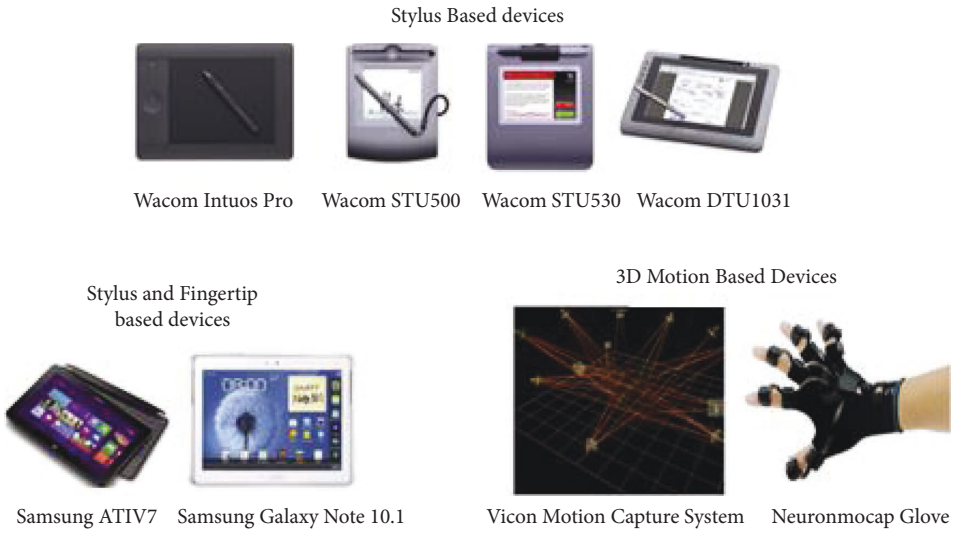


Figure 8: Signature acquisition tools [24].

Table 1: Online datasets comparison.

Dataset name	Language	Features	No. of signers	Genuine	Forge	Total
SVC2004 [31]	English, Chinese	Pressure, azimuth and altitude	40	20	20	1600
SUSIG [32]		x, y, and timestamp	100	20	10	3000
SIGMA [33]	Malaysian	x and y coordinates, pressure, instances of pen-up and pen-down during the signing process.	200	10	5	3000
ATVS [20]	Follow the pattern of the western signatures, which are left-to-right concatenated handwritten signature.	X and Y coordinates, pressure, azimuth, and altitude.	350	25	25	17500
MYCT-100 [32]	Spanish	x, y, pressure, azimuth, and altitude	100	25	25	5000
MCYT-330 [32]	Spanish	x, y, pressure, azimuth, and altitude	330	25	25	16500
Japanese dataset [34]	Japanese		30	42	36	2340
SigComp'11 [19]	Dutch	Position, pressure	64			1905
SigComp'11 [19]	Chinese	Position, pressure	20			1339
DOODB [35]	Hungarian	x, y coordinate and time interval	100	30	20	5000
MOBISIG [36]	Hungarian	x, y coordinate, pressure, finger area, velocities, acceleration, gyroscope and timestamp	83	45	20	5395
SigWiComp'13 [34]	Japanese		30	42	36	2340
AccSigDB1		Acceleration and angular momentum data	40	10	5	600
AccSigDB2		Acceleration and angular momentum data	20	10	5	300

hard to forge as compared to online signatures. Table 2 shows a comparison between the most popular offline databases.

6. Literature Review

Researchers from many universities and organizations have been attracted to the signature verification field because of the important role of handwritten signatures in biometric technologies as personal verifiers. The summarization of the massive work achieved in this field has been presented in a very good review in [39] for the years (up to 1989) and in [40] for the years (1989 to 1993).

In this section, we review the novel advances and emerging issues of handwritten verification systems in the last 10 years, from 2012 up to now. A comparison is made between techniques used in research for feature extraction and classifiers in identification and verification systems as presented in Table 3.

(i) Hamadène et al. proposed a method based on both the contourlet transform and the co-occurrence matrix. First, for computing contour segment directions of the handwritten signature, the contourlet transform was applied. Then, for computing the direction number, the co-occurrence

Table 2: Offline datasets comparison.

Dataset name	Language	No. of signers	Genuine	Forge	Total
CEDAR [37]	Belongs to versatile cultural backgrounds.	55	24	24	2640
MCYT-75 [37]	Spanish	75	15	15	2250
GPDS-syntheses [38]	Computer-generated dataset		24	30	4000
SigComp'11	Dutch	64			1932
SigComp'11	Chinese	20			1177
SigWiComp'13	Japanese	30	42	36	2340

Table 3: Comparison between the latest signature verification systems.

Author	Dataset	Features extraction techniques	Classification techniques	Problems	Results
Hamadène et al. [41] off-line	CEDAR dataset	Contourlet transform (CT) and cooccurrence matrix features	Support vector machines (SVM) classifier	Feature extraction methods do not allow capturing contours contained into an image.	(1) AER of 0.07 for writer dependent approach (2) AER of 0.18 for writer independent approach
Nemmour and Chibani [6] off-line	CEDAR dataset	Ridgelet transform and grid features	Support vector machines (SVM) classifier	The system can achieve higher accuracies but requires larger runtime.	EER is equal to 4.18
Kamihira et al. [42] Combined	Collected signature from 19 persons, 798 genuine samples and 684 skilled forgeries samples	Gradient features	Support vector machine (SVM) classifier	Few signature samples will increase the FRR of genuine signatures while too many samples will be labor intensive for the user.	Accuracy is equal to 97.22%
Griechisch et al. [43] online	SigComp2011	x, y coordinates, pressure, and velocity features	Kolmogorov-Smirnov distribution distance	Some reference signature which differed the most from the other reference were excluded, so it was not used during the decision process	EER is less than 13%.
Fayyaz et al. [20] online	SVC2004	Method based on learned signature features using autoencoder classifier	One-class classifiers	The system has been designed base on one hidden layer.	EER is equal to 2.15
Radhika and Gopika [4] combined	The dataset used is collected from 13 different writers. For each person 30 genuine and 25 forged signatures are collected.	(1) Pen tip tracking features were utilized in online case (2) Gradient and projection features were utilized in off-line case	Support vector machines (SVM) classifier		(1) FAR is equal to 11.54 (2) FRR is equal to 34.62 (3) AER is equal to 23.08
Lech and Czyzewski [44] online	Collected signatures using a wacom tablet from 10 persons for each person 5 signatures	Static features and time-domain functions of signals	Dynamic time warping (DTW)	The main drawback associated with using a graphical tablet with no display is lack of the visual feedback while putting down a signature.	
Hamadene and Chibani [45] off-line	(1) CEDAR (2) GPDS	Contourlet transform (CT) based directional code Co-occurrence matrix (DCCM) technique.	Writer-independent decision thresholding	The verification step is performed using only the feature dissimilarity measure	(1) AER for CEDAR is 2.10 (2) AER for GPDS is 18.42

Table 3: Continued.

Author	Dataset	Features extraction techniques	Classification techniques	Problems	Results
Taşkiran and Çam [46] off-line	Collected signature images at Yildiz technical university from 15 person, 40 sample from each.	Histogram of oriented gradients (HOG) features	Generalized regression neural networks (GRNN) algorithm	Large implementation costs and processing time	Accuracy is equal to 98.33%
Suryani et al. [47] off-line	They use 80 samples of signatures obtained from 8 persons	Moment invariant features	Efficient fuzzy Kohonen clustering network (FKCN) algorithm.	The accuracy of the training data is smaller than the accuracy of the test data.	Accuracy is equal to 70%
Serdouk et al. [37] off-line	(1) CEDAR (2) MCYT-75	Histogram of template (HOT) features	Support vector machine (SVM) classifier	Highlight strokes orientation in handwritten signatures.	(1) For CEDAR AER is 1.03%. (2) For MCYT-75 AER is 6.40%
Sharif et al. [38] off-line	(1) CEDAR (2) MCYT (3) GPDS	Global and local features selected using genetic algorithm	Support vector machine (SVM) classifier	High error rate	(1) AER for CEDAR is 4.67 (2) AER for MCYT is 5.0 (3) AER for GPDS is 3.75
Antal et al. [36] online	(1) MOBISIG (2) DOODB	(1) Function-based system use local features (2) Feature based system use global features	(1) In function-based system DTW was utilized for distance calculation among the test signature and the reference signatures. (2) In feature-based system euclidean distance used in training and manhattan distance is used in testing.	Feature-based methods offer poor results in the case of global threshold.	(1) EER is equal to 0.01% for random forgeries and 5.81% for skilled forgeries when user-specific thresholds is used. (2) EER is equal to 1.68% fort random forgeries and 14.31% for skilled forgeries when global thresholds is used.
Jia et al. [21] online	SVC2004 Task2	(1) Shape context features (2) Function–based features	SC-DTW was used to compare the test signature with the all the reference signatures	Require more training samples and consumes more computation costs.	EER is equal to 2.39%
Mersa et al. [48] off-line	(1) MCYT (2) UTsig (3) GPDS-synthetic	Convolutional neural network (CNN)	Support vector machine (SVM) classifier	Deep networks need rich and plentiful training data, which is rare in signature datasets.	(1) UTsig EER is 9.80% (2) MYCT EER is 3.98% (3) GPDS-synthetic EER is 6.81%
Saleem and Kovari [19] online	(1) MCYT-100 (2) SVC2004 (3) SigComp'11 (Dutch) (4) SigComp'11 (Chinese) (5) SigComp'13 (Japanese)	(1) Horizontal position (2) Vertical position (3) Pressure (4) Horizontal and vertical positions combination (5) Horizontal position, vertical position, and pressure combination	DTW and sampling frequency for each signer	External factors may affect the accuracy of the results	Accuracy improved in about 70% of the total 500 tests and 92% in the chosen system.

Table 3: Continued.

Author	Dataset	Features extraction techniques	Classification techniques	Problems	Results
Semih et al. [49] online	The dataset was created from scratch and examples were collected from 40 persons.	Time sequential peak values were used to construct the feature vector.	Dynamic time warping (DTW) algorithm	Classification difficulty caused by different paper types pen types and phone models.	(1) EER vary between %8.14–% 16.61 when signer-specific thresholds is used. (2) EER vary between %15.29–% 28.45 when single threshold for all signers is used.
Foroozandeh et al. [50] off-line	(1) GPDS-synthetic (2) MYCT-75 (3) UTSig	(1) Circlet transform (CT) (2) Statistical properties was calculated by the gray level co-occurrence matrices (GLCM)	(1) Support vector machine (SVM) (2) k-Nearest neighbor (k-NN)	The proposed method did not outperform on MYCT-75 dataset.	(1) EER with GDS-synthetic is 5.67 (2) EER with MYCT-75 is 7 when $r = 1$ and 8.20 when $r = 10$ (3) EER with YTSig is 6.72
Bonde et al. [51] off-line	(1) GPDS (2) MYCT-75 (3) UTSig	Fine-tuned CNN was used as signature features extraction technique	Support vector machine (SVM) classifier		(1) Accuracy for GPDS is 92.03 (2) Accuracy for MYCT-75 is 90.78 (3) Accuracy for UTSig is 85.46
Kurowski et al. [52] online	Hand-corrected dataset containing 10,622 signatures were obtained with electronic pen	Convolutional neural network to extract meaningful features from signatures	Deep convolutional network, the triplet loss method was used to train a neural network	The algorithm used in the proposed method becomes progressively slower as the training procedure continues.	(1) EER is equal to 5.77% for random forgery (2) 11.114% EER for skilled forgery
Zhou et al. [17] combined	Collected off-line images and online data of 1200 signatures	(1) For offline features the texture and geometric features are extracted using GLCM and HOG (2) For online features velocity, acceleration, angle and radius of curvature are extracted	(1) Support vector machine (SVM) classifier (2) Dynamic time warping (DTW) (3) SF-A (4) SFL	Large intra-class and inter-class variability.	(1) Accuracy for SVM is 81.17% (2) Accuracy for DTW is 89.17% (3) Accuracy for SF-A is 93.08% (4) Accuracy for SF-L is 92.58%
Melhaoui and Benchaou [53] off-line	Collected dataset from 12 person, 20 signature from each	Histogram of oriented gradients (HOG) features	Fuzzy min max classification (FMMC) method	The recognition rate depends highly on the choice of the sensitivity parameter which regulates how fast the membership value decreases.	Recognition rate is equal to 96%

matrix was applied. Tests were applied on the CEDAR dataset by using a support vector machines (SVM) classifier. The outcomes showed an AER of 0.07 for the writer -dependent approach and 0.18 for the writer-independent approach [41].

(ii) Nemmour and Chibani investigated their applicability for handwritten signature verification. Ridgelet transform and grid features were used to extract important characteristics. Performance evaluation was applied to the CEDAR dataset relative to SVM classifiers. The results showed that the EER of the proposed system was 4.18 [6].

(iii) Kamihira et al. proposed a signature verification technique called "combined segmentation-verification" based on both offline and online features. Three different off-line feature vectors were extracted from the images of the Japanese signature (full name) and the images of the Japanese signature (first name and last name). Then, for each off-line feature vector, the Mahalanobis distance was computed for verifying the signature. The approach of online features uses a dynamic programming matching method for signature time-series data. The last decision of verification was carried out using an SVM classifier based on the Mahalanobis metric and dynamic programming matching [42].

(iv) Griechisch et al. proposed an online signature verification technique that utilized simple statistical tests and time constraints. They tested the x, y coordinates, pressure, and velocity features in a separate way and combined them. System performance was estimated based on the Dutch dataset [43].

(v) Fayyaz et al. presented a system dependent on learning the features using an autoencoder that tries to learn signature features. These features were used to show users' signatures. Then, one class classifier has been utilized for classifying users' signatures. The proposed verification process was evaluated on the SVC2004 signature database. The experimental results showed a reduction in errors and an enhancement in accuracy [20].

(vi) Radhika and Gopika focused on combining online and off-line handwritten signature features to verify them. A webcam was used to collect online data, and digital signature images were used to collect off-line data. First, online and off-line data went through preprocessing stages. Second, both features were extracted in which features based on pen tip tracking were utilized in the case of online and gradient and projection based features were utilized in the case of offline approach. Finally, signatures were verified using both techniques separately, and their outputs were merged and inputted to the SVM classifier [4].

(vii) Lech and Czyzewski presented a signature verification system that uses both static features and time-domain functions of signals acquired by a tablet. The proposed approach fundamentally depends on Dynamic Time Warping (DTW) merged with some features from signature images acquired by a Wacom tablet that provides pressure information. Experimental results of this approach indicated a 0.82 average decision [44].

(viii) Hamadene and Chibani proposed a signature verification system in a novel framework based on both the Contourlet Transform (CT) and the feature dissimilarity metric. A writer-independent approach was merged with one-class verification using a decreased number of genuine references. The system does not require any powerful classifier like SVM or neural networks for dissimilarities training. Instead, the verification stage was applied using only the feature dissimilarity metric for estimating signature's similarity [45].

(ix) Suryani et al. proposed a signature recognition and verification system divided into five phases: data acquisition, preprocessing, data normalization, clustering, and evaluation. The results of signature recognition utilizing a clustering technique and the efficient fuzzy kohonen clustering network (EFKCN) algorithm indicated comparatively improved results with 70% accuracy compared to the accuracy of the prior system, which was 53%. These results of signature recognition can be used to support the verification system [47].

(x) Taskiran and Çam designed an off-line signature identification technique that used histogram of oriented gradients (HOG) features. The datasets were collected from 15 individuals at Yildiz Technical University, in which 40 signatures were collected from each individual. First, two approaches (image size fixing and noise removing approaches) were performed on all images. Then, HOG features were extracted from the processed images. Finally, so as to reduce the computation time and to remove the excessive features, PCA was applied to the signature dataset. The results of the proposed method indicated a 98.33% accuracy rate [46].

(xi) Serdouk et al. proposed a novel histogram of templates (HOT) features that describe handwritten signature stroke orientations. Many previous templates were utilized to present handwritten stroke orientations. In order to enable HOT local computations, a quad-tree partitioning based on the center of gravity was used. The verification phase was done using an SVM classifier. The proposed system was tested on the CEDAR and MCYT-75 datasets [37].

(xii) Sharif et al. presented a system that consists of four main stages: preprocessing, extraction of signature features, feature selection, and verification of features. The presented system global features involve aspect ratio, signature region, pure width, and pure height. On the other hand, local features involve the centroid of signature, slope, angle, and distance. The genetic algorithm was used in the stage of feature selection, so that a suitable feature set could be found. Then, those features were later inputted to SVM for verification. The system was examined on three datasets: CEDAR, MCYT, and GPDS [38].

(xiii) Antal et al. evaluated the dataset by using two novel methods. The first one was a function-based method (based on local features) and the second was a feature-based method (based on global features). The EER calculations were divided into two types: global thresholds and user-specific thresholds. The minimum EER for random forgeries was 0.01%, while for skilled forgeries it was 5.81%, utilizing user-specific thresholds that were calculated later. Yet, these EERs were increased to 1.68% for random forgeries and 14.31% for skilled forgeries using global thresholds [36].

(xiv) Jia et al. evaluated a technique based on shape contexts and function features in addition to a two-step method for efficient verification of online signatures. First, the shape context features were computed from the input data and the distance metric was used for classification purposes. In order to make a comparison between the test signature and the enrolled reference signatures, the Shape Context-Dynamic Time Warping (SC-DTW) was used. Finally, the interval-valued symbolic representation was applied to make a decision on whether the test signature was genuine or forged. The experiment results were estimated on SVC2004 Task 2, obtaining an EER equal to 2.39% [21].

(xv) Mersa et al. proposed an off-line signature verification system that is composed of two steps: learning representation and verification of the input signature. First, the trained Residual CNNs were fed with signature images. Second, for the verification, the output representations were then used to train the SVM. The proposed system was tested on three different datasets, including MCYT, UTSig, and GPDS-Synthetic [48].

(xvi) Saleem and Kovari presented a verification system using signer-dependent sampling frequency by studying the impact of selecting different sampling frequencies for each signer. The system was examined on five different datasets, utilizing many features and preprocessing techniques. Experiments indicated a 70% improvement in accuracy of the total 500 tests and 92% in the chosen system using z-normalization and 6 examples utilized in the preprocessing stage [19].

(xvii) Foroozandeh et al. presented an approach for signature verification using the circlet transform and the statistical properties of the circlet coefficients. The proposed approach has been applied to 3 common datasets, which are GPDS synthetic, MCYT-75 for Latin signatures, and UTsig for Persian signatures. When the results were compared to previous work, they demonstrated the validity of the proposed approach [50].

(xviii) Bonde et al. proposed an approach that consists of two phases. These are writer-dependent and writer-independent methods. The method of Writer-independent was used as the fine-tuning phase of the VGG16 Convolutional Neural Network (CNN). Fine-tuned CNN was used for extracting the signature features in the writer-dependent phase. In order to gain the features that are accurate for signature classification, the thinned signature image pixels were exchanged by their Gaussian Weighting Based Tangent Angle (GWBTA) in writer-dependent and independent phases. The features that were calculated in a writer-dependent phase were inputted into the support vector machine (SVM) classifier so that handwritten signatures can be classified as genuine or forged. The experiment results of the proposed method indicate its authenticity for offline signature verification [51].

(xix) Sadak et al. utilized the friction sound that arises from the contact between paper and pen as biometric data for verifying signatures. The process of collecting data was done using many kinds of pens, papers and mobile phones. In the feature extraction stage, the values of time-sequential peaks were gained from the starting strength envelopes of sound signals. The similarity metrics of signatures were computed using the Dynamic Time Warping (DTW) method [49].

(xx) Kurowski et al. developed an automated analysis technique for representing handwritten signature authentication dynamically. The proposed algorithms were based on analyzing handwritten signatures dynamically using neural networks. In order to train these neural networks, the triplet loss approach was used for signature verification of writer-invariant. A hand-corrected dataset of 10,622 signatures was utilized for evaluating the proposed neural network. The triplet loss method that was utilized for teaching the neural network to produce embedding has been confirmed to show better outcomes in collecting identical signatures and splitting them from signatures to represent different people [52].

(xxi) Zhou et al. proposed an improved signature verification system that depends on combining off-line and online features. First, both types of features were extracted from the signature, and then the signature was verified using two methods, which are support vector machine (SVM) and dynamic time warping (DTW). They took advantage of choosing a few examples through the training phase to solve various difficulties in a deficient number of examples. Also, a score fusion technique was proposed depending on accuracy (SF-A) so as to merge the offline and online features. The results showed that the proposed techniques were better than the off-line or online verification results [17].

(xxii) Melhaoui and Benchaou proposed a signature recognition technique using offline features. This technique was depended on histogram of oriented gradients (HOG) and fuzzy min max classification (FMMC) algorithms. Initially, the signature image was preprocessed, then the HOG features were utilized for the feature extraction stage. The HOG works by partitioning the image into neighboring regions, for each region Histogram of Oriented Gradients features were extracted. The proposed system produced a recognition rate of 96% based on many datasets of signature images [53].

7. Machine Learning in Signature Verification

Computer Vision (CV) and Artificial Intelligence (AI) capabilities can be utilized to build a system for automating the task of verification. The signature learning procedure is divided into two types; these are:

(1) Person-independent Learning: also known as general learning, in which the training set consists of genuine and forged signatures from a general population of several signers. The learning procedure is based on the differences between genuine and forged signatures across all signers. The model of general learning allows a questioned signature to be compared to a single genuine signature. A general classifier is designed using an independent database [54].

(2) Person-dependent-learning: also known as special learning, in this type of learning, the signature of each person is learnt from multiple samples of only that person's signature, where person similarities are learnt. A special classifier is designed for each person [55].

In machine learning, the most commonly applied technique for analyzing signatures is the convolutional neural network (CNN). It is a class of deep-feed forward artificial neural networks. In general, neural networks (NN) have been used for either feature extraction or classification purposes [56].

Another method has been introduced for this task, such as dynamic time warping (DTW), which is an algorithm for measuring similarity between two temporal sequences, and is utilized to verify between genuine and forged signatures. Support vector machine (SVM), a machine learning algorithm used for classification and regression tasks, has also been considered for the classification of handwritten signatures. The structural approach is another method in which signatures are represented using trees and graphs. Statistical approaches are also used for the classification of a handwritten signature, such as the wavelet-based approach [57]. A comparison is made between the most common machine learning techniques that are used for feature extraction and classification techniques. They are shown in Tables 4 and 5.

7.1. Limitations in Signature Verification. There are two main limitations to signature verification: The first is that there is a large intra-class and inter-class variability. The person's original signature will change due to many factors, such as time and age. The imposter will also try to copy the signature with a lot of training in advance. Therefore, the extraction and selection of comprehensive and representative signature features is necessary. Second, in real-life scenarios, only a small number of real signatures can be obtained for training, and insufficient data is also a problem that needs to be solved [17].

In offline signature verification, researchers come across two limitations. First, most of the dynamic information in the signature is lost. Second, the low quantity of available signature samples versus the high number of extracted features [58].

The difficulties in both online and offline signature verification are summarized as follows: selection of the most suitable features for a signer; evaluation of signature verifier performance; forgery classification; signature variability and constancy analysis; reference set updating and large database creation; and result comparison using popular and reasonable protocols [28].

7.2. Signature Verification Performance Metrics. To estimate the outcomes of handwritten signature verification systems effectively, false rejection (called Type1 error) and false acceptance (called Type2 error) metrics are used. FRR and FAR can be utilized to compute the receiver operating characteristic curve (ROC curve) and equal error rate (EER). [59].

Further, the below error rates can be used for performance evaluation of verification system:

(i) False Rejection Rate (FRR): It is considered as the proportion of original signatures accepted as false by the verifier. FRR can be calculated as follows:

$$\mathrm{FRR} = 1 - \mathrm{TP}/(\text{number of genuine signatures}). \tag{1}$$

Table 4: Comparison between the most used classifiers.

Classifier	Advantages	Limitations
Support vector machine (SVM)	(1) Suitable for small and clean datasets (2) Effective in high dimensional spaces	(1) Less efficient on datasets that have noise (2) Unsuitable for big datasets (3) Hard to choose a suitable kernel-function that is robust to interpret
Dynamic time warping (DTW)	(1) It is time series averaging which makes the classification faster more accurate (2) Suitable for a smaller number of templates	(1) The number of templates is restricted (2) Actual training samples is required
Deep learning	(1) Computation power does not affect it (2) High dimensional (3) Can automatically adapt all data (4) Faster in obtaining results (5) Works on big and complex datasets	(1) Hard to understand (2) For training, it require large quantity of data for training (3) Large memory and computing resources is required (4) More costly (5) High errors rate
K-nearest neighbor (K-NN)	(1) The complete dataset is covered for finding K-nearest neighbors (2) Suitable for multi-class classification and regression problems	(1) Sensitive to outliers (2) Cannot handle the missing value issue (3) Mathematically costly (4) Large memory is required (5) Homogeneous features is required
Probabilistic neural network (PNN)	(1) Quicker and more accurate than MLPs (2) Insensitive to outliers (3) Representative training set is required	(1) More memory space is needed (2) When it compared to MLP it is slower in case of new classification samples
Euclidean distance	(1) Very popular method (2) Easy computation (3) Works good with compact or isolated clusters	Sensitive to outliers
Manhattan distance	Dealing good with datasets with compact or isolated clusters	Sensitive to the outliers
Hidden markov model (HMM)	Can handle inputs with variable length	More memory and time it requirement

Table 5: Comparison between the most used feature extraction techniques.

Feature extraction technique	Advantages	Limitations
Contourlet transform (CT)	(1) Proper for two-dimensional images processing. (2) More directions is used in the transformation (3) Able to remove noises in the smooth areas and along the borders of image in a very good way	Not proper for image coding because of redundant transform
Local features	(1) The texture in image areas are shown (2) Invariant to scale, rotation, and other transformations	(1) Key-points distinguishing is required (2) Comparing images may be more difficult because of the differing numbers of key-points images. (3) No spatial information
Global features	(1) Charachtarize the whole image (2) The descriptors of shape and texture are classified into this group of features (3) Very compact images representations are shown, in which every point in a high-dimensional space of features represent an image.	Sensitive to clutter and occlusion.
Structural features	Able to encode some information about the structure of the objects	Suitable with binary images only
Histogram of oriented gradient (HOG)	(1) Both shape and texture are shown (2) Suatable for objects in detecting when image is processed (3) Mainlly used for objects classification	(1) Produce a very big feature vectors resulting in large costs of storage (2) Cannot deal with scale and rotation (3) Time consuming when it extract features

Table 5: Continued.

Feature extraction technique	Advantages	Limitations
Statistical features	(1) Easily detected as compared with structural features. (2) Not influenced very much by noises or distortions as compared to statistical features.	Suitable only with gray-level and color images
Gray level Co-occurrence matrices (GLCM)	(1) It is a measurement of the various combination of brightness value pixels in an image. (2) GLCM features is direction independent because it can be gained for a one orientation as well as merging all the orientation together	Feature calculation is a time-wasting process in GLCM

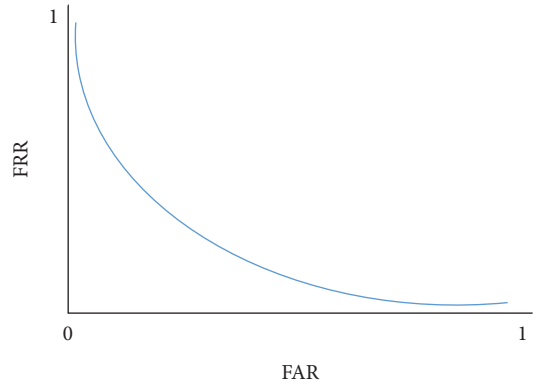


Figure 9: Receiver operating curve [60].

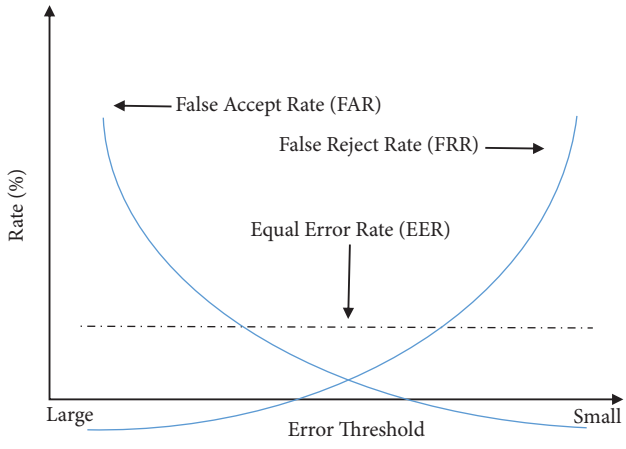


Figure 10: FAR, FRR and EER relation [61].

(ii) False Acceptance Rate (FAR): It considered as the proportion of forged signatures accepted as original by the verifier. FAR can be calculated as follows [59]:

$$\text{FAR} = \text{FP}/(\text{number of forge d signatures}). \quad (2)$$

(iii) Receiver Operating Characteristic curve (ROC): It is the most widely utilized metric for evaluating the performance of biometric systems. The ROC curve represents FAR according to FRR as shown in Figure 9. The benefit of this metric is that it produces an accurate representation of biometric system performance through only one curve, so that a comparison can be made between various biometric systems. If the region under the curve is equal to 1 and the ERR is equal to 0, then an optimal result is achieved.

(iv) Equal Error Rate (EER): It is the cross point between FAR and FRR, as shown in Figure 10. EER is commonly utilized to compare and estimate biometric verification systems. If EER is close to 0%, it means better performance of the target system [60].

8. Conclusions

In this paper, a review of the present advanced literature that is related to handwritten signature verification has been made. The main steps of the verification and identification systems were presented for both online and offline cases.

The most recent handwritten signature verification systems have been discussed and summarized in table form. Also, signature datasets that are commonly used in signature verification were tabled to be compared. Different feature extraction and classification techniques such as global features, local features, statistical and structural features, histogram of gradient, convolutional neural networks, support vector machines, K-nearest neighbor, etc. have been compared in terms of advantages and limitations. Finally, the general limitations in the field of signature verification were listed as well as the most common metrics that are used for evaluating these systems. These limitations can be summarized as the selection of the most proper features for a signatory, evaluation of signature verifier performance, forgery classification, signature variability and constancy analysis, reference set updating and large database creation, and result comparison using popular and reasonable protocols. Thus, the whole paper is useful in finding the gaps in research and giving a chance to improve them.

9. Future Works and Suggestions

Many points can be considered in future work to conduct research, such as increasing the number of reference signature images in the case of offline systems or signature features in the case of online systems for each user to improve a machine learning system's decision. The second point is to create a multilingual signature dataset with a large number of users because as we notice in this paper, some signature dataset have a limited number of users (usually ranging from 10 to 100 users).

Also, systems that verify signatures based on hybrid features need to be focused (both online and offline features). Finally, deep learning is used in order to achieve enhanced verification results.

Data Availability

All the data are available within the manuscript.

Conflicts of Interest

There are no conflicts of interest to declare.

References

[1] M. A. Taha and H. M. Ahmed, "Iris features extraction and recognition based on the local binary pattern technique," in *Proceedings of the 2021 International Conference on Advanced Computer Applications (ACA)*, pp. 16–21, Maysan, Iraq, July 2021.

[2] M. A. Taha and H. M. Ahmed, "A fuzzy vault development based on iris images," *Eureka: Physics and Engineering*, no. 5, pp. 3–12, 2021.

[3] V. Iranmanesh, S. M. S. Ahmad, W. A. W. Adnan, S. Yussof, O. A. Arigbabu, and F. L. Malallah, "Online handwritten signature verification using neural network classifier based on principal component analysis," *The Scientific World Journal*, vol. 20148 pages, Article ID 381469, 2014.

[4] K. Radhika and S B. Gopika, "Online and offline signature verification: a combined approach," *Procedia Computer Science*, vol. 46, pp. 1593–1600, 2015.

[5] L. G. Hafemann, R. Sabourin, and L. S. Oliveira, "Offline handwritten signature verification — literature review," in *Proceedings of the 2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)*, pp. 1–8, Montreal, QC, Canada, November 2017.

[6] H. Nemmour and Y. Chibani, "Off-line signature verification using artificial immune recognition system," in *Proceedings of the 2013 International Conference on Electronics, Computer and Computation (ICECCO)*, pp. 164–167, Ankara, Turkey, November 2013.

[7] S. Mushtaq and A. Mir, "Signature verification: a study," in *Proceedings of the 4th IEEE International Conference on Computer and Communication Technology, ICCCT*, pp. 258–263, Allahabad, India, September 2013.

[8] A. Kumar and K. Bhatia, "A survey on offline handwritten signature verification system using writer dependent and independent approaches," in *Proceedings of the 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall)*, pp. 1–6, Bareilly, India, September 2016.

[9] R. A. Mohammed, R. M. Nabi, S. M.-R. Mahmood, and R. M. Nabi, "State-of-the-Art in handwritten signature verification system," in *Proceedings of the 2015 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 519–525, Las Vegas, NV, USA, December 2015.

[10] N. Sharma, S. Gupta, and P. Mehta, "A comprehensive study on offline signature verification," *Journal of Physics: Conference Series*, vol. 1969, no. 1, Article ID 012044, 2021.

[11] H A B. Nehal and M. Heba, "signature identification and verification systems: a comparative study on the online and offline techniques," *Future Computing and Informatics Journal*, vol. 5, no. 1, 2020.

[12] H. Kaur and M. Kumar, "Signature identifcation and verifcation techniques: state-of-the-art work," *Journal of Ambient Intelligence and Humanized Computing*, 2021.

[13] M A S. Hanaa and H. Shrooq, "Eye Detection Using Helmholtz Principle," *Baghdad Sci.J*, vol. 16, p. 18, 2019.

[14] H. M. Ahmed and R. T. Rasheed, "A raspberry PI real-time identification system on face recognition," in *Proceedings of the 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*, pp. 89–93, Baghdad, Iraq, July 2020.

[15] H. Mohsin and S. H. Abdullah, "Pupil detection algorithm based on feature extraction for eye gaze," in *Proceedings of the 2017 6th International Conference on Information and Communication Technology and Accessibility (ICTA)*, pp. 1–4, Muscat, Oman, December 2017.

[16] H. Mohsin and H. Bahjat, "Anti-screenshot keyboard for web-based application using cloaking," Edited by M. Bouhlel and S. Rovetta, Eds., in *Proceedings of the 8th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT'18)*, vol. vol 146, July 2020.

[17] Y. Zhou, J. Zheng, H. Hu, and Y. Wang, "Handwritten signature verification method based on improved combined features," *Applied Sciences*, vol. 11, p. 5867, 2021.

[18] D. Impedovo and G. Pirlo, "Automatic signature verification: the state of the art," *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 38, no. 5, pp. 609–635, Sept. 2008.

[19] M. Saleem and B. Kovari, "Online signature verification based on signer dependent sampling frequency and dynamic time warping," in *Proceedings of the 2020 7th International Conference on Soft Computing & Machine Intelligence (ISCMI)*, pp. 182–186, Stockholm, Sweden, November 2020.

[20] M. Fayyaz, M. H. Saffar, M. Sabokrou, M. Hoseini, and M. Fathy, "Online signature verification based on feature representation," in *Proceedings of the 2015 The International Symposium on Artificial Intelligence and Signal Processing (AISP)*, pp. 211–216, Mashhad, Iran, March 2015.

[21] Y. Jia, L. Huang, and H. Chen, "A two-stage method for online signature verification using shape contexts and function features," *Sensors*, vol. 19, 2019.

[22] M. Hanmandlu, M. H. M. Yusof, and V. K. Madasu, "Yusof "Off-line signature verification and forgery detection using fuzzy modeling," *Pattern Recognition*, vol. 38, no. 3, pp. 341–356, 2005.

[23] T. Wilkin and O. S. Yin, "State of the art: signature verification system," in *Proceedings of the 2011 7th International Conference on Information Assurance and Security (IAS)*, pp. 110–115, Melacca, Malaysia, December 2011.

[24] R. Tolosana, R. Vera-Rodriguez, J. Fierrez, and J Ortega-Garcia, "DeepSign: deep on-line signature verification," *IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE*, vol. 3, no. 2, pp. 229–239, APRIL 2021.

[25] A. Beresneva, A. Epishkina, and D. Shingalova, "Handwritten signature attributes for its verification," in *Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 1477–1480, Petersburg, Russia, January 2018.

[26] H. M. Ahmad and S. R. Hameed, "Eye diseases classification using hierarchical MultiLabel artificial neural network," in *Proceedings of the 2020 1st. Information Technology To Enhance e-learning and Other Application (IT-ELA*, pp. 93–98, Baghdad, Iraq, July 2020.

[27] M. R. Deore and S. M. Handore, "A survey on offline signature recognition and verification schemes," in *Proceedings of the 2015 International Conference on Industrial Instrumentation and Control (ICIC)*, pp. 165–169, Pune, India, May 2015.

[28] G. Padmajadevi and K. S. Aprameya, "A review of handwritten signature verification systems and methodologies," in *Proceedings of the 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, pp. 3896–3901, Chennai, India, March 2016.

[29] T. Wilkin and O. S. Yin, "State of the art: signature verification system," in *Proceedings of the 2011 7th International Conference on Information Assurance and Security (IAS)*, pp. 110–115, Melacca, Malaysia, December 2011.

[30] M. Saleem and B. Kovari, "Survey of preprocessing techniques and classification approaches in online signature verification," in *Image Analysis and Recognition. ICIAR 2020. Lecture Notes in Computer Science*, A. Campilho, F. Karray, and Z. Wang, Eds., Vol. vol 12131, Springer, Cham, New York, NY, USA, 2020.

[31] DY. Yeung, "SVC2004: first international signature verification competition," in *Biometric Authentication. ICBA 2004*, D. Zhang and A. K. Jain, Eds., Vol. vol 3072, Springer, Heidelberg, Germany, 2004.

[32] B. Yanikoglu and A. Kholmatov, "Online signature verification using fourier descriptors," *EURASIP Journal on Applied Signal Processing*, vol. 2009, no. 1, Article ID 260516, 2009.

[33] S. M. S. Ahmad, A. Shakil, A. R. Ahmad, M. Agil, M. Balbed, and R. M. Anwar, "SIGMA - A Malaysian Signatures' Database," in *Proceedings of the 2008 IEEE/ACS International Conference on Computer Systems and Applications*, pp. 919-920, Doha, Qatar, March 2008.

[34] M. I. Malik, M. Liwicki, L. Alewijnse, W. Ohyama, M. Blumenstein, and B. Found, "ICDAR 2013 competitions on signature verification and writer identification for on- and offline skilled forgeries (SigWiComp 2013)," in *Proceedings of the 2013 12th International Conference on Document Analysis and Recognition*, pp. 1477–1483, Washington, DC, USA, March 2013.

[35] M. Martinez-Diaz, J. Fierrez, and J. Galbally, "The DooDB graphical password database: data analysis and benchmark results," *IEEE Access*, vol. 1, pp. 596–605, 2013.

[36] M. Antal, L. Z. Szabó, and T. Tordai, "Online signature verification on MOBISIG finger-drawn signature corpus," *Mobile Information Systems*, vol. 2018, Article ID 3127042, 1 page, 2018.

[37] Y. Serdouk, H. Nemmour, and Y. Chibani, "New histogram-based descriptor for off-line handwritten signature verification," in *Proceedings of the 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*, pp. 1–5, Aqaba, Jordan, October 2018.

[38] M. Sharif, M. A. Khan, M. Faisal, M. Yasmin, and S. L. Fernandes, "A framework for offline signature verification system: best features selection approach," *Pattern Recognition Letters*, vol. 139, pp. 50–59, 2020.

[39] 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.

[40] F. Leclerc and R. . Plamondon, "Automatic Signature Verification: The State of the Art - 1989-1993", Progress in Automatic Signature Verification," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 8, pp. 3–20, 1994.

[41] A. Hamadène, Y. Chibani, and H. Nemmour, "Off-line handwritten signature verification using contourlet transform and Co-occurrence matrix," in *Proceedings of the 2012 International Conference on Frontiers in Handwriting Recognition*, pp. 343–347, Bari, Italy, September 2012.

[42] Y. Kamihira, W. Ohyama, T. Wakabayashi, and F. Kimura, "Improvement of Japanese signature verification by combined segmentation verification approach," in *Proceedings of the 2013 2nd IAPR Asian Conference on Pattern Recognition*, pp. 501–505, Naha, Japan, November 2013.

[43] E. Griechisch, M. I. Malik, and M. Liwicki, "Online signature verification based on Kolmogorov-smirnov distribution distance," in *Proceedings of the 2014 14th International Conference on Frontiers in Handwriting Recognition*, pp. 738–742, Hersonissos, Greece, September 2014.

[44] M. Lech and A. Czyzewski, "A handwritten signature verification method employing a tablet," in *Proceedings of the 2016 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, pp. 45–50, Poznan, Poland, September 2016.

[45] A. Hamadene and Y. Chibani, "One-class writer-independent offline signature verification using feature dissimilarity thresholding," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 6, pp. 1226–1238, 2016.

[46] M. Taxkiran and Z. G. Çam, "Offline signature identification via HOG features and artificial neural networks," in *Proceedings of the 2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Article ID 000083, Herl'any, Slovakia, January 2017.

[47] D. Suryani, E. Irwansyah, and R. Chindra, "Offline signature recognition and verification system using efficient fuzzy kohonen clustering network (EFKCN) algorithm," *Procedia Computer Science*, vol. 116, pp. 621–628, 2017.

[48] O. Mersa, F. Etaati, S. Masoudnia, and B. N. Araabi, "Learning representations from Persian handwriting for offline signature verification, a deep transfer learning approach," in *Proceedings of the 2019 4th International Conference on Pattern Recognition and Image Analysis (IPRIA)*, pp. 268–273, Tehran, Iran, March 2019.

[49] M. S. Sadak, N. Kahraman, and U. Uludag, "Handwritten signature verification system using sound as a feature," in *Proceedings of the 2020 43rd International Conference on Telecommunications and Signal Processing (TSP)*, pp. 365–368, Milan, Italy, July 2020.

[50] A. Foroozandeh, A. A. Hemmat, and H. Rabbani, "Offline handwritten signature verification based on circlet transform and statistical features," in *Proceedings of the 2020 International Conference on Machine Vision and Image Processing (MVIP)*, pp. 1–5, Iran, February 2020.

[51] S. V. Bonde, P. Narwade, and R. Sawant, "Offline signature verification using convolutional neural network," in *Proceedings of the 2020 6th International Conference on Signal Processing and Communication (ICSC)*, pp. 119–127, Noida, India, March 2020.

[52] M. Kurowski, A. Sroczyński, G. Bogdanis, and A. Czyżewski, "An automated method for biometric handwritten signature authentication employing neural networks," *Electronics*, vol. 10, p. 456, 2021.

[53] O. E. Melhaoui and S. Benchaou, "An efficient signature recognition system based on gradient features and neural network classifier," *Procedia Computer Science*, vol. 198, pp. 385–390, 2022.

[54] H. Srinivasan, S. N. Srihari, and M. J. Beal, "Machine learning for signature verification," in *Computer Vision, Graphics and Image Processing*, P. K. Kalra and S. Peleg, Eds., vol. vol 4338, Heidelberg, Germany, Springer, 2006.

[55] G. S. Eskander, R. Sabourin, and E. Granger, "Eskander, Robert Sabourin and others, "Hybrid writer-independent–writer-dependent offline signature verification system"," *IET Biometrics*, vol. 2, no. 4, pp. 169–181, 2013.

[56] S. Jahandada, S. M. Sam, K. Kamardin, N. N. Amir Sjarif, and N. Mohamed, "Offline signature verification using deep learning convolutional neural network (CNN) architectures GoogLeNet inception-v1 and inception-v3," *Procedia Computer Science*, vol. 161, pp. 475–483, 2019.

[57] A. Cohen and A A A. Mohamed, "On wavelet-based statistical process monitoring," *Transactions of the Institute of Measurement and Control*, SAGE Publications, vol. 44, no. 3, pp. 525–538, 2022.

[58] H. Saikia and K. Chandra Sarma, "Approaches and issues in offline signature verification system," *International Journal of Computer Application*, vol. 42, no. 16, pp. 45–52, March 2012.

[59] A. Kumar and K. Bhatia, "A survey on offline handwritten signature verification system using writer dependent and independent approaches," in *Proceedings of the 2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall)*, pp. 1–6, Bareilly, India, September 2016.

[60] M. El-Abed and C. Charrier, *Evaluation of Biometric Systems*, Intech open science, Massachusetts, MA, USA, 2012.

[61] M. N. Yaacob, S. Z. S. Idrus, W. N. A. W. Ali, W. A. Mustafa, M. A. Jamlos, and M. H. A. Wahab, "Syed zulkarnain syed idrus and others "decision making process in keystroke dynamics," *Journal of Physics: Conference Series*, vol. 1529, no. 2, Article ID 022087, Apr 2020.