ISSN: 2633-4828 Vol. 5 No.4, December, 2023

International Journal of Applied Engineering & Technology

A COMPARATIVE STUDY ON SIGNATURE IDENTIFICATION AND VERIFICATION SYSTEM

Hemant A. Wani[1], Kantilal Rane[2] and V. M. Deshmukh[3]
[1]Research Scholar Electronics Engineering, KBCNMU Jalgaon, India
[2]Associate Professor E & TC Department, Bharati Vidyapith College of Engineering, Navi Mumbai, India
[3]Associate Professor E & TC Department, SSBT COET Bhambori, Jalgaon, India
[1]wanihemant1983@gmail.com

ABSTRACT
Among the biometric systems used for personal identification are signature identification and verification. An individual's signature can be verified through the examination of their handwriting, which might vary between and among people. An in-depth, methodical review of online and offline signature identification and verification methods is provided in this study. Surveys on two approaches in online signature verification—writer-dependent and There are writer-independent methods offered. Additionally, a compilation of research on feature extraction and classification methods used to the identification and verification of signatures has been included. Numerous databases were released. The evaluation of several signature identification and verification systems, together with their associated this article reports the findings. Lastly, recommendations for future research are given.

Keywords: Signature identification, Signature verification, Handwritten signature, Biometric.

I. INTRODUCTION
One way to identify a person is through biometric identification, according to behavioral and physiological characteristics. The physiological attributes are a person's biological qualities, or the traits that they possess and comprise the hand, iris, fingerprint, DNA, and facial characteristics. Behavioral characteristics show how a person behaves and Voice, signature, dynamics, etc. are all included. When it comes to accuracy, biometric technologies outperform traditional security systems that depend on passwords and personal information, Smart cards, or personal identification numbers (PINs). This elevated precision stems from an individual's biological characteristics are distinct, making them difficult to transfer and incapable of be misplaced, taken, or damaged. Applications for biometric recognition can be found in many of the documents and activities we use on a regular basis, such as voter registration, passports, immigration papers, driving licenses, personal device logins, smart cards, and security applications. Confidential financial transactions and personal data privacy can be achieved with biometric-based solutions. A handwritten signature is one of the most popular biometric systems features and is legally accepted as a form of personal identification in financial and administrative entities. Every person's signature is defined as a unique combination of symbols and strokes that serve as both an identifying characteristic and a reflection of their writing style. A person's identity and the authenticity of a document are both confirmed by their signature. There are two ways to obtain signatures: online and offline. In the online mode, a writing pad and stylus connected to a computer are used to electronically take signatures. Online mode, commonly known as dynamic mode, captures dynamic aspects of signature photos such as writing speed, angle, number of pen-ups, time spent to place a signature, etc. Given how challenging it is to mimic the dynamic aspects, this information improves accuracy. In the off-line mode, signatures are written on paper documents and then scanned, photographed, etc. to record the signature. Since the features from the signature images are recovered after they are written on a paper sheet, the Offline mode analyzes the shape-related static features of the photos. As a result, another name for it is a static model of signature acquisition. Signatures can be used for a variety of things, such as document retrieval, personal identification and verification, etc. Numerous signature identification and verification techniques were consequently created and published in the literature. In the section that follows, these algorithms are covered in great detail. This is how the remainder of the paper is structured. Section 2 presents reader motivations pertaining to this poll. The feature extraction and classification methods used for signature identification and verification are described in Section 3. Results of the survey are shown in Sect. 4. The

comparison between the survey that is being presented and the most recent survey works is shown in Section 5. Section 6 presents a conclusion to this paper as well as some suggestions for future work.

II. MOTIVATION

In the past, several methods such as names, social security numbers, PINs, passwords, and tokens were employed to identify a person under various conditions. Nevertheless, approving someone using a password or token only serves as a stand-in for confirming their identity because tokens can disappear or be shared. Therefore, the main reason for utilizing a signature as a biometric on papers is that each person has a distinct signature that sets them apart from others. Furthermore, there are numerous uses for signature authentication, such as in financial transactions, access control, security, etc. Therefore, the authors have reviewed the numerous methods for signature identification and verification in this study, which have been helpful in distinguishing between real and fake signatures. The authors of this survey have examined a number of feature and classification strategies that can be used in various combinations to account for the increase in signature identification and verification rates. This article evaluates the performance of signature identification and verification approaches using a number of databases and their sources. Additionally, as this survey is useful in identifying research needs in the signature identification and verification area, it will be beneficial to all academics with an interest in this field.

III. DESCRIPTION OF FEATURE EXTRACTION/ SELECTION, CLASSIFICATION TECHNIQUES AND DISTANCE MEASURES FOR SIGNATURE IDENTIFICATION AND VERIFICATION

It has been proposed to verify signatures offline using a novel feature extraction approach [1]. This technique made use of the idea of feature extraction by determining the geometric center and Euclidean distance of various signatures. This classifier performs better and faster when it comes to feature extraction. This procedure produces better results than any other method now in use. The average and standard deviation are used to aid in the threshold selection procedure. Based on the description of the signature envelope and the inner stroke distribution in polar and Cartesian coordinates, a different technique for off-line signature identification and verification is put forth [2]. A new geometrical feature for an offline signature verification system (ASV) is employed in this paper. A fixed point microprocessor can be used to calculate the suggested attributes. As a result, the functionalities can be taken out of a personal gadget like a smart card. Several classifiers, including SVM, HMM, and EDC, are used to examine the system in order to detect forgeries. In comparison to other suggested approaches, the Improved Offline Signature Verification Scheme Using Feature Point Extraction Method [3] is suggested as a way to lower FAR. The method selects 60 feature points from the signature's COG and compares them to feature points that have been learned. The mean and variance determine how the feature points are classified. The values of the threshold distance from the COG alter significantly in response to a slight change in a signature. As a result, this technique increases the FRR value. One of the initial processing stages a computer vision system generally takes when trying to extract information from an object in an image is the creation of a digital skeleton. A number of algorithms have been put out to create the basic structure of a digital binary pattern. The Hilditch thinning algorithm [4] is a frequently employed technique for preparing images that is suggested to expedite real-time processing. An algorithm for obtaining an object's skeleton from an image was proposed by Hilditch. This algorithm exists in two versions: one that uses a 4×4 mask and the other that uses a 3×3 mask. The output of the operation can be saved to a memory table using a 3x3 mask picture. The output outcomes obtained from each distinct 3x3 mask. When an application is started, the output results of all the various 3×3 masks are recorded to this ―table‖. The ―looking for table‖ approach can be used to extract the thinning results of each 3x3 mask in an image after it has been processed. As a result, the process speed is high but the thinning outcome is the same. In paper [5], a multi-feature, multi-stage verification method is provided for Chinese signature. In order to reach a decision, this study uses two levels of verification. Using the aid of directive features, the input sign is compared in the first step. If the result is false, the remaining execution will cease. However, if it approves the signature, the second stage verification will proceed, and the outcome of that step will be considered the final decision. Another method of verifying a real signature is by the application of the Cross-validated Graph Matching algorithm [6]. This work used a normalized box near signatures to identify the high intensity. The process of comparing the

signatures involves creating a bipartite graph, from which the measure of mismatch, or Euclidean distance, may be calculated and a minimum cost complete matching can be established. It is suggested and tested to detect the position changes of the signature geometry's strokes for the purpose of verifying signatures [7]. Two approaches are suggested. While the second method helps identify the real positioning variations of individual strokes in the 2-D signature patterns, the first method aids in determining the positional variation of the projection profiles of the signature. The statistics pertaining to these variations are calculated in both approaches. Potential variations are discovered here by using a variety of signatures as an input. Assessing the condition of the training sets allows one to determine how authentic the input is. The decision-making procedure entails calculating a distance measure that accounts for both location fluctuations and their association. A different approach based on image fusion, discrete wavelet transform, and image registration is put forth for the recognition and verification of Persian signatures offline [8]. Each person's training signature is registered in order to solve scaling and shifting issues.DWT is used to locate signature details in order to extract features in the first step. The following stage involves merging multiple registered signatures of each individual to create a reference signature of that person. Euclidean distance between the test image and each pattern is employed in separate bands throughout the verification stage. The suggested method's correctness was validated by the experimental outcomes. A suggested way for determining if a bank check signature is authentic is [9]. It explains how different verification algorithms are used to identify signatures on checks. The suggested algorithm in this case can be applied to a banking industry signature verification system that works well. The suggested approach identifies and examines the key components of a check, including the account holder's signature, in order to verify a check. The verification processes FAR, FRR, and success ratio are displayed in the results. The author of [11] introduced a novel method for pre-processing the signature predefines area. Based on the image view, he employed innovative auto cropping preparation, where the cropping parameter is the pixel intensity value. This method offers the ability to tailor the layout design of biometric systems to just utilize the region of interest in the used image, while also increasing the performance of security systems based on signature images.

IV. FLOW OF OFFLINE SIGNATURE RECOGNITION

Fig 1 shows the flow of offline signature recognition.

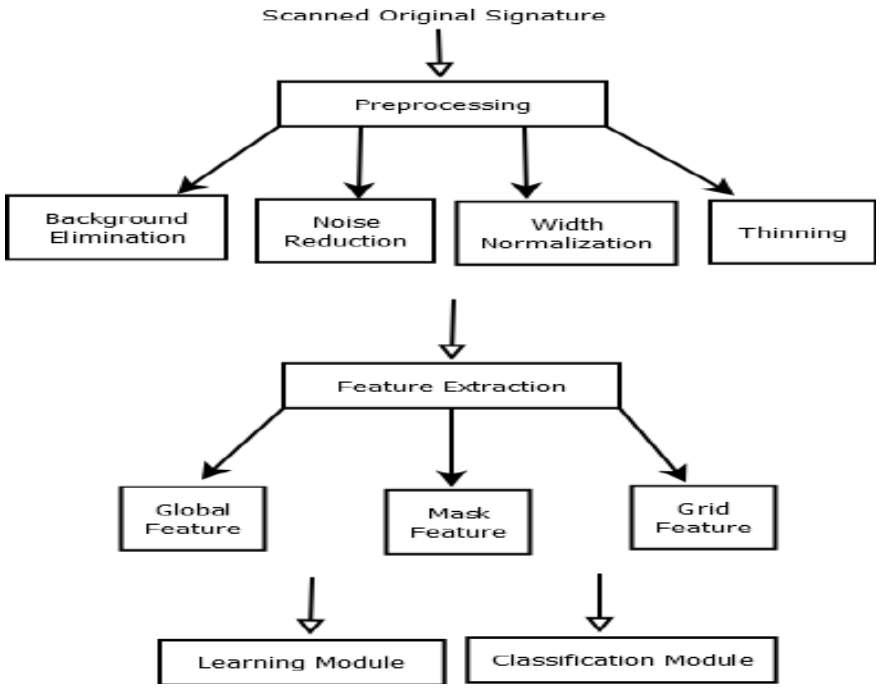

Fig 1. Flow of offline Signature Recognition

The procedure for recognizing a offline signature is as follows, according to the literature review:

4.1 Preprocessing

The pre-processing step is used in both the training and testing phases. A gray scan is used for signatures. Standardizing signatures and preparing them for feature extraction are the goals of this phase [12].

The following formulas are used to scan signatures in gray [13].

(0.299*Red) + (0.5879*Green) + (0.144*Blue) = Gray

The following processes are part of the pre-processing stage: skeletonization, scaling, noise reduction, background removal, and width normalization.

4.1.1 Background Removal

In order to extract features, data area cropping is required. In order to extract the signature from the background, ptile thresholding was used. Following thresholding, the background's other pixels would be "0" and the signature's pixels would be "1".

The following criteria can be met by the brightness threshold selection: [13]

Assume that the image's pixels are f (x, y). If (x, y)> T

Therefore, background = f (x, y)

Else Object = f(x, y)

4.1.2 Noise Reduction

Decoding errors or noisy channels are the source of contaminated images. Degradation of an image can also occur from the negative effects of surrounding objects and lighting. The median filter is widely used to restore and smooth out images that have been distorted by noise [15]. This nonlinear method works well for lowering impulsive noise [14]. A window slides across the image in a median filter, and the intensity of the pixel in the center of the window is determined by the median concentration of pixels within the window at each location. We recommend the median filter in our analysis because, when compared to the mean filter, it has remarkable qualities for suppressing impulse noise while maintaining edges.

4.1.3 Scaling

Let H and W represent the inputted image's height and width, respectively [14].

The equation Xnew = (Xold * 100)/H,

where Xnew & Xold are calculated & original X coordinate, and

Ynew = (Ynew * 100)/W,

where Ynew & Yold are calculated & original Y coordinate, can be used to fit the image uniform at 100*100 pixels.

The input image is converted to a uniformed 100*100 pixel image using these equations [14].

4.1.4 Normalization of Width

Both intrapersonal and interpersonal variations may exist in signature dimensions. As a result, the image's width is set to its default value and the height changes without affecting the ratio of height to width. The width dimension is set to 100 after width normalization is complete.

The following equations were used in the normalization process:

(Xold-Xmin)/ (Xmax-Xmin) = Xnew M*

(Yold-Ymin)/ (Ymax-Ymin) = Ynew M*

Where the normalized pixel coordinates for Xnew and Ynew signature

Xold, Yold = Original Signature's pixel coordinates, M= Measured in width and height for the standard signature

4.1.5 Thinning

By making the image one pixel thicker, the thinning process aims to remove pen thickness variations. Hilditch's Algorithm is employed in this system.

4.2 Feature Extraction

The inputs from the training phase are the extracted features in this step. This system has three types of features: grid, mask, and global features. Global characteristics give details about particular instances of the signature shape. The orientations of the lines in the signatures are indicated by the mask characteristics. The overall appearance of a signature is provided by grid features.

4.2.1 Global Features

The quantity of pixels that make up the signature is known as the signature area. The signature density is disclosed by this feature. By dividing signature height by signature width, one can find the signature height-to-width ratio. The width and height of a signature might vary. The proportions of a single person's height to width are roughly equal.

Maximums of the vertical and horizontal histograms: Every row has a horizontal histogram, and the row with the highest value is considered to have the maximum horizontal histogram. Each column's vertical histogram is computed, and the column with the highest value is designated as the maximum vertical histogram.

The equations in Eq. 1 [16] are used to determine the signature's horizontal and vertical center.

Xmax Ymax

Ymax Xmax

Centrex = $\sum x \sum b[x][y]$

Centery= $\sum y \sum b[x][y]$

x=1 y=1, y=1 x=1

Xmax Ymax

Ymax Xmax

$\sum \sum b[x][y]$

$\sum \sum b[x][y]$

x=1 y=1 y=1 x=1

Local signature maximum numbers: It is computed how many local maxima there are in the vertical and horizontal histograms. Numbers on the signature's edge points: In an 8-neighbor system, an edge point is a pixel with just one neighbor that is part of the signature.

4.2.2 Mask Features

The directions of the signature lines are revealed by the mask features. There are interpersonal variations in the angles of the signatures. This system makes use of eight distinct 3x3 mask features [13]. Every mask is captured encircling the signatures, and the number of identical 3x3 signature parts is computed.

4.2.3 Grid Features

Densities of signature parts are found using grid features [10]. This system makes use of sixty grid features. The image area in each of the 60 evenly divided portions of the signature is computed.

V. SURVEY RESULTS ACCORDING TO CONSIDERED CLASSIFICATION TECHNIQUES AND DISTANCE MEASURES

To date, a great deal of effort has been spent into creating sophisticated signature verification systems using soft computing and computer vision methods. The automation and integration of numerous processes and representations for visual perception are referred to as computer vision.

Since computer graphics creates image data from 3D models, computer vision is thought of as the opposite of computer graphics, which frequently creates 3D models from the image data. The term "soft computing" describes a broad range of methods that formalize cognitive processes by taking advantage of the human mind. In order to achieve practicability, resilience, and low solution costs, it deals with imprecision, uncertainty, partial truth, and approximation. There exist Soft computing methods that have received a lot of attention include Artificial Neural Networks and Fuzzy Logic. in the written word. We have included the literature on signature identification and verification in this part. The literature has a few surveys that have been provided. Within the subsections that follow, an assessment of signature recognition and verification using classification methods that are adhered to by Findings and a discussion are provided.

5.1 Nearest neighbor (NN)

Pal et al. (2016) [17] used texture features to assess the accuracy of the offline signature verification method on the BHSig260 dataset, a sizable collection of fine signatures in Hindi and Bangla. By using the Nearest Neighbor approach as a similarity measure to validate signatures, the proposed approach reported AER (Average Error Rate) of 32.72% independently for LBP (Local Binary Patterns) and ULBP (Uniform Local Binary Patterns) based features. They achieved EERs of 24.47% and 33.82% on Hindi and Bengali words, respectively, based on k-NN. Rajput and Patil (2017) [18] have suggested an approach for offine signature recognition that is writer-independent. To identify the signature photos, they have employed the K-Near-est Neighbor (K-NN) classifier and the Histogram of Oriented Gradient (HOG) features extraction technique. A database of beautiful handwritten signatures—100 during the learning phase and 60 during the testing phase—are used to assess the suggested system, and the results show good recognition accuracy.

5.2 Hidden Markov model (HMM)

A Hidden Markov Model (HMM)-based online signature verification method was proposed by Fierrez et al. (2007) [19]. Seven dynamic time functions—x, y, pressure, path tangent angle, path velocity magnitude, log curvature radius, and total acceleration magnitude—are the foundation for the feature extraction process. Research is carried out using the bimodal biometric database of MCYT. For skilled and random forgeries, the suggested approach produced EERs of 0.74% and 0.05%, respectively. The suggested method is contrasted with other cutting-edge systems based on the findings of the First International Signature Verification Competition (SVC2004).

5.3 Support vector machine (SVM)

In order to identify the correlation between the pixels of various signatures, Narwade et al. (2018)[20] created an offine signature verification system based on shape correspondence. This scheme uses an adaptive weighted mixture of shape context distance and Euclidean distance. The SVM classifier is then used to determine whether the signature is authentic by using the computed distances as an input. Through assessment of the suggested methodology using the GPDS synthetic signature database, they attained an accuracy rate of 89.58%. In order to improve the ability of the machine signature verification to distinguish between different photos, Okawa (2018) [21] suggested a new method that involved fusing Fisher Vector characteristics from the background and foreground signature images. They thought of using PCA to make Fisher Vectors and SVM less dimensional in order to classify signature photos as authentic or fraudulent. On the MCYT-75 dataset, they achieved an EER of 5.47%, which is higher than the results published in the most advanced machine signature verification systems (Ferrer et al. 2012[22]; Okawa 2016a[23], 2016b[24]; Soleimani et al. 2016 [25]). Global and local features are retrieved from the ofine signatures, and Sharif et al. (2018) [26]presented a framework to verify the ofine signatures. The genetic algorithm feature selection method is then used to reduce the extracted features, and the

features that are left are passed into an SVM classifier for validation. These trials are carried out on the CEDAR, MCYT, and GPSS synthetic datasets. They achieved rates on the CEDAR dataset. representing 4.67% (FRR), 4.67% (FAR), and 4.67% (AER) according to Table surpasses the current methods for verifying digital signatures

5.4 Fuzzy classifier

An strategy to choose a predetermined number of the most important global elements of a dynamic signature was presented by Zalasiński and Cpałka (2018)[27]. The selected worldwide characteristics were subsequently utilized to confirm the dynamic signatures using the fuzzy approach. Utilizing the MCYT-100 signature database, the studies yielded an average EER of 2.20%, which is higher than that of Zalasińskietal.(2016)[28].***In 2020, Zalasiński***et al[29] introduced **a** novel method **for** enhancing the effectiveness **of *the dynamic signature verification process:*** using **populationbased algorithms (PBA) to** divide **online signatures.**A fuzzy classifier based on the BioSecure DS2 database was used to test the suggested approac h, and the results showed an average error rate of 3.08%, which is better than the results of earlier studies (Cpałka et al. 2014[30]; Cpałka et al. 2014 [31]; Cpałka et al. 2016[32]). In order to represent feature vectors, Alaei et al. (2017)[33] developed a writer-dependent signature verification method employing interval-valued symbolic data. Next, the fuzzy similarity metric is used to confirm the signature test sample. The suggested method is assessed using the GPDS and BHSig260 benchmark datasets, with an AER of 11.74% on the GPDS-160 dataset. According to the findings, the suggested strategy—which takes into account eight or more training samples—performs better than more current signature verification techniques. By Kumar and Dhandapani (2017)[34], an offline signature verification method for bank checks has been created. They have incorporated properties like Zernike moments, circularity, and aspect ratio for the purpose of authenticating the signatures. The results are obtained from a database containing a total of 72 signatures which is further divided into three sets each containing 24 signatures. The results show that the proposed system achieved an average accuracy value of 0.46.

5.5 Neural Network /Deep Learning

Shariatmadar et al. (2019)[35] proposed a writer-dependent approach for signature verification using images from handwritings. This method uses a hierarchical one class-based CNN to learn genuine signatures. Wei et al. (2019) [36]presented an Inverse Discriminative Networks model for verifying writer-independent handwritten signatures. Jain et al. (2020)[37] proposed a language-independent shallow Convolutional Neural Network (CNN) approach for verifying handwritten signatures. These methods were evaluated on various databases and datasets. Kao and Wen (2020)[38] developed a deep CNN approach for offline signature verification and forgery detection based on a single known signature specimen. The approach achieved accuracies between 94.37% and 99.96% on the ICDAR2011 SigComp dataset. Poddar et al. (2020)[39] proposed a deep learning-based approach for offline signature recognition and forgery detection, with accuracies of 90-94% and 85-98%, respectively. Voruguntiet al. (2020)[40] used Convolutional Autoencoder (CAE) and handcrafted features to create a lightweight Online Signature Verification (OSV) framework. The results showed superior performance compared to state-of-the-art OSV approaches, making this work the first to consider hybrid fusion of features and few shot learning. Ghosh (2021) [41]proposed a Recurrent Neural Network (RNN)-based deep learning model for offline signature recognition and verification. The model extracts structural and directional features and uses long-short-term memory (LSTM) and bidirectional long-short-term memory (BLSTM) models for classification. The model achieved average EERs of 2.27%, 1.46%, 0.34%, 0.01%, 0.43%, and 0.36% on six public signature datasets. Ghosh et al. (2021)[42] proposed a novel spatio-temporal Siamese Neural Network (ST-SNN) for 3D signature recognition. Liu et al. (2021) [43]proposed a region-based deep metric learning network for offline signature verification using deep Convolution Siamese Network.

to comply with the journal paper formatting requirements is to use this document as a template and simply type your text into it.

Survey

VI. SOURCES OF DATA AND SIGNATURE DATABASES

Databases listed below shall be extensively searched in order to conduct the survey, as well as their studies reported. It is shown that the most popular signature datasets are employed.

CEDAR dataset: This dataset contains data from 55 writers, with 24 genuine signatures and 24 skilled forgeries for each writer. It is in a grayscale PNG format.

MCYT: There are two subsets of the MCYT signature dataset. MCYT-100 contains data from 100 writers, with 25 genuine and 25 forged online samples for each writer. MCYT-75 contains data from 75 writers, with 15 genuine and 15 forged offline signatures for each writer.

GPDS Signature: It is a Spanish offline signature dataset with different subsets. GPDS-100 contains data from 100 writers, GPDS-150 contains data from 150 writers, and GPDS-960 contains data from 960 writers (but it is no longer available). These datasets have 24 genuine signatures and 30 forged signatures for each writer in black and white and grayscale versions.

GPDS-Synthetic: This dataset contains data from 4000 writers. Similar to GPDS Signature, it has 24 genuine signatures and 30 forged signatures for each writer in black and white and grayscale versions.

UTSig: It is a Persian offline Signature dataset from the University of Tehran. It contains data from 115 writers, with 27 genuine and 45 forged signatures for each writer in gray scale TIF files.

SigComp2009: This dataset was used in a signature verification competition. The training set contains data from 12 writers, with 5 genuine and 5 forged signatures for each writer. The evaluation set contains data from 100 writers, with 12 genuine and 6 forged signatures for each writer.

SigComp11: It includes two subsets of dataset: Chinese and Dutch signature samples. It contains both online and offline signature samples in RGB colored images. The number of signatures in the online dataset differs from the offline dataset, and the number of signatures in the Chinese dataset differs from the Dutch dataset.

BHSig260 signature dataset: This dataset contains signatures of 260 writers, with 100 signed in Bengali and 160 signed in Hindi. Each writer has 24 genuine and 30 forged signatures.

SVC2004: It was the first international signature verification competition. There are two datasets of online handwritten signatures, with the first containing only coordinate information and the second containing additional information such as pen orientation and pressure. Each dataset contains data from 100 writers, with 20 genuine signatures and 20 skilled forgeries for each writer.

SUSIG: This dataset is divided into two subcorpora: visual and blind. The visual sub corpus contains data from 100 writers, with 20 genuine and 10 forged samples (5 skilled and 5 very skilled) for each writer. The blind subcorpus contains data from 100 writers, with 10 genuine samples from 70 writers, 8 genuine samples from 30 writers, and forged samples similar to the visual subcorpus. Data stored for both subcorpora includes the x-y coordinates, pressure level, and time stamp for each writer.

ATVS dataset: An online signature dataset that contains data from 350 users, with 25 signatures for each user.

VII. CONCLUSIONS AND FUTURE SCOPE

The paper has attempted to survey the existing literature related to signature identification and verification to know the advances in this field. This literature has been surveyed for both online and offline signature acquisition methods. In offline signature verification, a survey related to both writer-dependent (WD) and writer-independent (WI) approaches has been done. The feature extraction techniques have been elaborated with pros and cons. Different existing classification approaches such as Hidden Markov Model (HMM), Support Vector Machine (SVM), template matching, vector quantization, fuzzy approach, Neural Networks, deep learning, hybrid approaches, etc. have been discussed in this survey. Some significant signature identification and verification systems have been summarized in the form of a table for further comparisons. The most widely used signature

datasets have also been discussed in this survey paper. Thus, the whole survey is helpful in finding the research gaps in signature identification and verification and highlights the need to develop more robust and more constructive signature identification and verification approaches. So, in the future, the following points can be considered as reference to carry out the research:

• The increase in number of users in the dataset decrease the performance of signature identification and verification systems.

• The increase in the number of samples per user enhances the system performance.

• There is better performance with the utilization of deep learning techniques in extracting the features.

• All the mentioned classifiers can be utilized for both offline and online systems except Dynamic Time Warping (DTW) which can only be employed in online systems.

• Although DTW is considered as a standard procedure for online signature verification, but String Edit Distance (SED) can also be experimented for online signature verification. Careful selection of cost model for SED can lead to better results than employing DTW for online signature verification.

• A hybrid approach can be proposed by combining the different dissimilar models.

• In order to verify the signatures, graphs are rarely used due to the increased computational complexity involved in matching two general graphs. So, one can think of making improvements to the graph matching framework, both in terms of approximation accuracy and computational complexity

• Signature database of people having neurological disorders can be developed apart from the signature of normal people in order to evaluate the performance of signature verification system.

REFERENCES

[1] Banshidhar Majhi, Y Santhosh Reddy, D Prasanna Babu, ―Novel Features for Off-line Signature Verification‖ International Journal of Computers, Communications & Control, pp. 17-24, 2006.

[2] Migual A. Ferrer, Jesus B. Alonso and Carlos M. Travieso, "Off-line Geometric Parameters for Automatic Signature Verification Using Fixed-Point Arithmetic", IEEE Tran. On Pattern Analysis and Machine Intelligence, vol.27, no.6, June 2005.R. Chen et al., ―Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks,‖ IEEE Commun. Mag.,pp. 50–55, Apr. 2008.

[3] Ming Yin, Seinosuke Narita, ―Speedup Method for Real-Time Thinning Algorithm‖ DICTA2002: Digital Image Computing Techniques and Applications, Melbourne, Australia, 21--22 January 2002Y.-C. Liang et al., ―Sensing-Throughput Trade-off for Cognitive Radio Networks, ‖IEEE Trans. Wireless Commun., pp. 1326–37 ,April 2008.

[4] Yingna Deng, Hong Zhu, Shu Li, and Tao Wang, ―Signature Verification Method Based on the Combination of Shape and Dynamic Feature‖, Department of Automation and Information Engineering, Xi'an University of Technology, 710048 Xi'an China, 2005.

[5] Ramachandra, A. C. Pavithra, K. and Yashasvini, K. and Raja, K. B. and Venugopal, K. R. and Patnaik, L. M., ―Cross-validation for graph matching based Offline Signature Verification‖, In: INDICON 2008, India, pp: 17-22,2008.

[6] Fang, B., et al, ―Off-line signature verification by the tracking of feature and stroke positions‖, Pattern Recognition, pp. 91-101, 2003.

[7] Samaneh Ghandali, Mohsen Ebrahimi Moghaddam, ―Off-Line Persian Signature Identification and Verification Based on Image Registration and Fusion‖, Journal of Multimedia, June 2009.

[8] M.Jasmin Pemeena, Priya darsini ,K.Murugesan, Srinivasa Rao Inbathini, A.Jabeena, and K.Sai Tej ―Bank Cheque Authentication using Signature‖ ,International Journal of Advanced Research in Computer Science and Software Engineering , May 2013.

[9] Raman Maini & Himanshu Aggarwal, ―Study and Comparison of Various Image Edge Detection Techniques‖, International Journal of Image Processing (IJIP), 2010.

[10] Bassam Al-Mahadeen, Mokhled S. AlTarawneh and Islam H. AlTarawneh ―Signature Region of Interest using Auto cropping‖ IJCSI International Journal of Computer Science Issues, March 2010.

[11] Ravi J, Sundernag Hosamani and K B Raja ―Off-line Signature Identification Based on DWT and Spatial Domain Features‖ IEEE20180

[12] Emre Özgündüz, Tülin Şentürk and M. Elif Karslıgil. Off-line Signature Verification And Recognition by Support Vector Machine.

[13] Shiwani Sthapak1, Minal Khopade2, Chetana Kashid3. Artificial Neural Network Based Signature Recognition & Verification.ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 8, and August 2013 [14]M.A. Ferrer, M. Diaz-Cabrera, and A. Morales. Synthetic off-line signature image generation. In 2013 International Conference on Biometrics (ICB), pages 1–7, June 2013. [15]Ashwini Pansare, Shalini Bhatia "Off-line Signature Verification Using Neural Network", International Journal of Scientific & Engineering Research, Volume 3, Issue 2, February-2012 1 ISSN 2229-5518 [16] Luiz G. Hafemann, Robert Sabourin, and Luiz S. Oliveira. Analyzing features learned for offline signature verification using Deep CNNs. In International Conference on Pattern Recognition, pages 2989–2994, 2016. [17] Pal S, Alaei A, Pal U, Blumenstein M (2016) Performance of an off-line signature verification method based on texture features on a large Indic-script signature dataset. In: Proceedings of 12th IAPR workshop on document analysis systems (DAS), pp 72–77[18]Rajput GG, Patil P (2017) Writer independent offline signature recognition based upon HOGs features. Int J Electr Eng 9(1):59–67

[19] Fierrez J, Ortega-Garcia J, Ramos D, Gonzalez-Rodriguez J (2007) HMM-based on-line signature verification: Feature extraction and signature modeling. Pattern Recognit Lett 28(16):2325–2334

[20] Narwade PN, Sawant RR, Bonde SV (2018) Offline signature verification using shape correspondence. Int J Biom 10(3):272–289

[21] Okawa M (2018b) Synergy of foreground-background images for feature extraction: offline signature verification using Fisher vector with fused KAZE features. Pattern Recognit 79:480–489

[22] Ferrer MA, Vargas JF, Morales A, Ordónez A (2012) Robustness of offline signature verification based on gray level features. IEEE Trans Inf Forensics Secur 7(3):966–977

[23] Okawa M (2016a) Offline signature verification based on bag-of-visual words model using KAZE features and weighting schemes. In: Proceedings of 29th IEEE conference on computer vision and pattern recognition workshops, pp 252–258

[24] Okawa M (2016b) Vector of locally aggregated descriptors with KAZE features for offline signature verification. In: Proceedings of 5th IEEE global conference on consumer electronics (GCCE), pp 435–439

[25] Soleimani A, Araabi BN, Fouladi K (2016a) Deep multitask metric learning for offline signature verification. Pattern Recognit Lett 80:84–90

[26] Sharif M, Khan MA, Faisal M, Yasmin M, Fernandes SL (2018) A framework for offline signature verification system: best features selection approach. Pattern Recognit Lett 139:50–59

[27] Zalasiński M, Cpałka K (2018) A Method for genetic selection of the dynamic signature global features' subset. Adv Intell Syst Comput 655:73–82

[28] Zalasiński M, Cpałka K, Hayashi Y, 2016, A new approach to the dynamic signature verification aimed at minimizing the number of global features. In: Rutkowski L, Korytkowski M, Scherer R, Tadeusiewicz R, Zadeh LA, Zurada JM (eds) ICAISC 2016. LNCS, vol 9693, pp 218–231.

[29] Zalasiński M, Łapa K, Cpałka K, Przybyszewski K, Yen GG (2020) On-line signature partitioning using a population-based algorithm. J Artificial Intell Soft Comput Res 10(1):5–13

[30] Cpałka K, Zalasiński M (2014) On-line signature verification using vertical signature partitioning. Expert Syst Appl 41:4170–4180

[31] Cpałka K, Zalasinski M, Rutkowski L (2014) New method for the on-line signature verification based on horizontal partitioning. Pattern Recognit 47(8):2652–2661

[32] Cpałka K, Zalasinski M, Rutkowski L (2016) A new algorithm for identity verification based on the analysis of a handwritten dynamic signature. Appl Soft Comput 43(1):47–56

[33] Alaei A, Pal S, Pal U, Blumenstein M (2017) An efficient signature verification method based on an interval symbolic representation and a fuzzy similarity measure. IEEE Trans Inf Forensics Secur 12(10):2360–2372.

[34] Kumar DA, Dhandapani S (2017) Offline signature verification system for bank cheques using Zernike moments, circularity property and fuzzy logic. Int J Eng Comput Sci 6(9):22442–22449

[35] Shariatmadari S, Emadi S, Akbari Y (2019) Patch-based offline signature verification using one-class hierarchical deep learning. Int J Doc Anal Recognit 22:375–385

[36] Wei P, Li H, Hu P (2019) Inverse discriminative networks for handwritten signature verification. In: Proceedings of IEEE/CVF conference on computer vision and pattern recognition (CVPR), pp 5757–5765

[37] Jain A, Singh SK, Singh KP (2020) Handwritten signature verification using shallow convolutional neural network. Multim Tools Appl 79:19993–20018

[38] Kao H-H, Wen C-Y (2020) An offline signature verification and forgery detection method based on a single known sample and an explainable deep learning approach. Appl Sci 10(11):1–15

[39] Poddar J, Parikh V, Bharti SK (2020) Offline signature recognition and forgery detection using deep learning. Procedia Computer Sci 170:610–617

[40] Vorugunti CUSS, Pulabaigari V, Gorthi RKSS, Mukherjee PP (2020) OSVFuseNet: online signature verification by feature fusion and depthwise separable convolution based deep learning. Neurocomputing 409:157–172

[41] Ghosh R (2021) A recurrent neural network based deep learning model for offline signature verification and recognition system. Expert Syst Appl. https:// doi. org/ 10. 1016/j. eswa. 2020. 114249

[42] Ghosh S, Ghosh S, Kumar P, Scheme E, Roy PP (2021) A novel spatiotemporal Siamese network for 3D signature recognition. Pattern Recognit Lett 144:13–20

[43] Liu L, Huang L, Yin F, Chen Y (2021) Offline signature verification using a region based deep metric learning network. Pattern Recognit. https:// doi. org/ 10. 1016/j. patcog. 2021. 108009