A Survey on Offline Hand Written Signature Verification

Mallegowda M[1], Nandini K H[2], Anita kanavalli[3]
[1]*Faculty of Department of Computers Science & Engineering, MSRIT, Banglore, Karnataka, India*
[2]*M.Tech Student, Department of Computers Science, MSRIT, Banglore, Karnataka, India*
[3]*Head of the Dept of AI &DS, MSRIT, Banglore, Karnataka, India*

***Abstract*— Automatic signature verification is one of the major research areas in biometrics. It deals with establishing the authenticity of a person based on his/her signature. The handwritten signature is a widely used behavioral biometric trait for personnel authentication. It is used in many day-to-day applications such as authentication of documents, forgery detection, bank cheques, credit cards, entry to secured zone, etc. Manual proof of signature through visual inspection requires more time and human effort, whereas automation of signature verification minimizes the human struggle and eliminates fraud (Impedovo and Pirlo, 2008).**

Researchers have been proposed many models for automatic signature verification over the last four decades. These models vary in the features used, classifier adopted, and the usage of similarity threshold also. Despite many available models, signature verification is still a challenging problem due to its more intra-class variation and less inter-class variation. Still, there is an increasing demand for a reliable automatic signature authentication system.

In this paper, a detailed survey carried out on automatic signature verification is presented with qualitative and quantitative analysis. It serves as an aid for researchers working in this direction. This paper exhaustively covers works related to automatic signature verification categorized them based on features used, and a technique adopted, classifier used, dataset, and performance measure.

I. INTRODUCTION

Biometric authentication refers to a security method involving individuals' physiological or behavioral characteristics. Authentication based on an individual's physical biometric characteristics includes fingerprint, face, retina, iris, ear, DNA, hand geometry, palm print, etc. In contrast, behavioral biometric traits of an individual comprise voice, signature, gait, etc. (Jain et al., 2011).

Generally, the biometric authentication system can be done either in verification or recognition mode. In a verification mode, a user of the system claims an identity by providing his/her biometric sample. Whereas in the recognition mode, a user of the system provides a biometric sample, and the system has to identify among all users enrolled in the system (Impedovo and Pirlo, 2008). The handwritten signature is the commonly used behavioral biometric trait due to its wide acceptance. Some of the critical challenges in signature verification are: signature samples of a particular class have significant intra-class variation and less inter-class variation when skilled forgeries are considered. Preserving this intra-class variation is challenging. It is not easy even for a forensic expert to tell correctly whether a signature is authentic just by visual inspection. Availability of genuine signatures for training purposes is usually less in many applications, and signature is easier to forge than other biometrics. Signature verification remains an open challenge since a signature is judged genuine or forgery only based on a few available reference specimens (Alaei et al., 2017).

II. RELATED WORK

Signature verification is a multistage process, which includes data acquisition and preprocessing, feature extraction, and classification (Impedovo and Pirlo, 2008). The block diagram of a signature verification system is as shown in Figure-1. In this review, we focus mainly on the research work concerning these steps. A comparative study of various signature verification systems reported in the literature is also presented.

Signature acquisition

A signature can be acquired through two modes: online or offline mode. In an offline mode, optical scanning devices or cameras are used to obtain the signatures written on paper (Bajaj and Chaudhary, 1997; Kalera et al., 2004; Hanmandlu et al., 2005;

Shanker et al., 2007). Whereas in an online mode, a signature is acquired through special hardware such as pressure-sensitive tablets, PDA(Personal digital assistant), etc., which can record dynamic features of the signature such as velocity, pressure, acceleration, writing force, etc. (Jain et al., 2002; Parodi and Gomez, 2014). Due to the non-availability of dynamic properties of a writer, verification based on offline signature is more challenging.

Pre-processing

Prior to the application of feature extraction methods, the preprocessing step is employed on the signature images to make them noise-free and have invariant transition features. In addition, preprocessing step also determines the accuracy of the verification process. The various preprocessing techniques reported in the literature are: segmentation, binarization, filtering, thinning, skeletonization, normalization, resizing, cropping, morphological operations, and geometric corrections, etc. (Impedovo and Pirlo, 2008).

In any offline signature verification, one commonly used preprocessing technique is binarization (Guerbai et al., 2015; Ooi et al., 2016; Hadjadji et al., 2017; Sharif et al., 2018; Zois et al., 2019; Ruiz et al., 2020). In this step, the gray-scale signature image is converted into binary through the Otsu binarization algorithm (Otsu, 1979). Binarization separates the signature image's foreground and background and reduces the computational burden. Further, researchers have used filtering techniques to remove the single black pixels on the white background of the binarized image. Commonly used filters are mean filter(Nguyen et al., 2010; Pal et al., 2015), median filter(Ooi et al., 2016; Sharif et al., 2020), Gaussian filter(Mizukami et al., 2002), and average filter(AbdelRaouf et al., 2018). Filtering improves the quality of the signature. Generally, the signature images contain variations in pen thickness, ink, and position of strokes, size, and orientation. Hence, the signature images need to be normalized to their height and width (Hanmandlu et al., 2005; Yılmaz et al., 2016; Sharif et al., 2018).

Furthermore, morphological operations have been applied on normalized signature images to make the signature area more usable for features extraction(Ooi et al., 2016; Zois et al., 2016; Sharif et al., 2018; Zois et al., 2019; Ruiz et al., 2020). Sometimes the scanned signature images are not aligned properly. In order to make the appropriate changes in orientation, geometric correction techniques are applied on signature images (Yılmaz et al., 2016; Ghosh and Rajib, 2021) which improves the accuracy. Finally, the signature area is cropped, which reduces the storage requirement and computational burden (Baltzakisa and Papamarkos, 2001; Hanmandlu et al., 2005).

The preprocessing step improves the signature image's quality and makes it suitable for feature extraction. The preprocessing step is applied both in the training and testing phases.

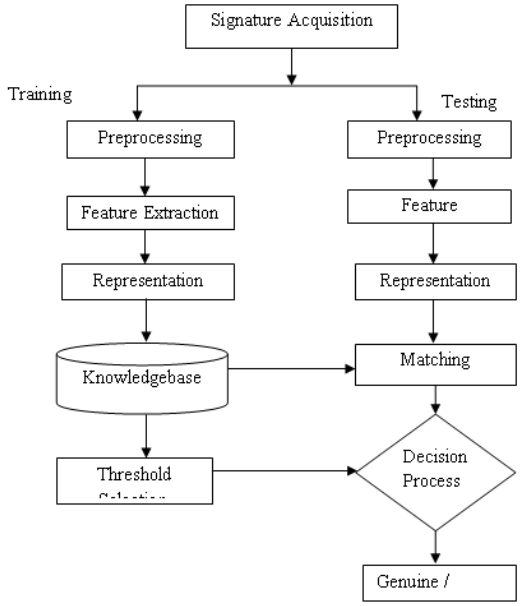

Figure-1 The System Architecture

Feature Extraction

In signature verification, features are broadly classified into function-based and parameter-based (Impedovo and Pirlo, 2008) features. Function-based features are used in online signature verification, representing the signature's local properties such as position, velocity, acceleration, pressure, force, the direction of pen movement, pen inclination, etc. Parameter-based features represent the local and global properties of the signature. Parameter-based features are extracted from both offline and online signatures. Function-based features generally perform better than parameter-based features due to the presence of dynamic information (Impedovo and Pirlo, 2008).

Parameter-based features are either global features or local features of the signature. Further, global features concern the geometric properties of the whole

signature image(Guler and Meghdadi, 2008; Ramachandra et al., 2009; Sharif et al., 2018; Zois et al., 2020). In contrast, local features give detailed information of pixel distribution in specific signature parts of the signature image(Ruiz-del-Solar, 2008; Sharif et al., 2018; Zois et al., 2020). Some of the global features proposed for offline signature verification are the geometric center of the signature(Majhi et al., 2006), the distances between geometric centroids(Prakash and Guru, 2009), area, aspect ratio, histogram, number of edge points, pure width, pure height(Sharif et al., 2018), slant angle, loops((Kovari and Charaf, 2013), number of closed loops(Pal et al., 2015), number of endpoints(Baltzakis and Papamarkos, 2001), baseline(Kovari and Charaf, 2013), number of strokes (Zois et al., 2019), etc.

Many authors focused on global features. However, global features are less sensitive to noise and signature variations. They do not give a high accuracy for skilled forgeries as they can provide limited information of the signature image. Classification of signature features are shown in Figure-2.

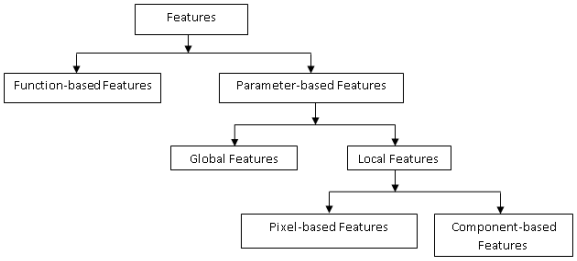

Figure-2: Classification of signature features

Various mathematical transformations have been recommended to compute parameter-based features for offline signature verification. The most frequently used mathematical transformations in offline signature verification are: wavelet transform(Deng et al., 1999; Ghandali et al., 2008), Discrete Radon transform (DRT) (Fick et al., 2016; Ooi et al., 2016; Soleimani et al., 2016), Gabor Wavelet transform(Sigari et al., 2011), Fractal transform (Zouari et al., 2014) and curvelet transform(Guerbai et al., 2015; Hadjadji et al., 2017). Apart from the above mathematical transformations, Discrete Fast Fourier transform (DFFT)(Wen et al., 2009) was employed to obtain ring-peripheral features from signature images. Rotation-invariant features from signature images are extracted by adapting Discrete Fourier Transform (DFT)(Parodi et al., 2011). Pourshahabi et al. (2009) and Hamadene et al. (2016) have applied contourlet transform on signature images to capture smooth contours as feature vectors.

Local features are extracted from a specific portion of a signature image in offline signature verification. Depending on the level of detail considered, local features are classified as pixel-based and component-based features. Pixel-based features are computed at the pixel level, and component-based features are extracted at the level of each component (Impedovo and Pirlo, 2008) of a signature image. Pixel-based features (Huang and Yan, 2002) represent the signature images' visual patterns. Pixel-based features include key-points(Ruiz-del-Solar et al., 2008), texture-based features(Yilmaz et al., 2011; Serdouk et al., 2014; Yılmaz et al., 2016; Alaei et al., 2017), shadow code features(Sabourin and Genest, 1994; Eskander et al., 2013; Rivard, 2010), run-length features, grid-based(Bertolini et al., 2010; Parodi et al., 2011; Zois et al., 2016; Diaz et al., 2019), and directional features(HOG)(Tomar and Singh, 2011; Zhang, 2010; Dutta et al., 2016), etc.

Further, Vargas et al. (2011) have used grey-level information of signature images as features for offline signature verification. Ferrer et al. (2012) have obtained good results by combining LBP features and GLCM features for offline signature verification. In Bouamra et al.'s (2018) work, sequences of connected pixels in a given direction, all having the same intensity, are obtained from binary images of signatures as features called Run-length distributions. Bhunia et al. (2019) proposed two types of texture features: discrete wavelet and local quantized patterns (LQP) for offline signature verification.

The literature shows that texture features, key points, and directional features(HOG) have successfully increased the accuracy of offline signature verification systems.

Various component-based features reported in the literature for offline signature verification include geometric features(Schafer and Viriri, 2009; Ferrer et al., 2017; Jain et al., 2021), projection features (Fang et al., 2003; Shanker and Rajagopalan, 2007), etc. Furthermore, Kalera et al. (2004) presented a model for offline signature verification by combining gradient, structural, and concavity features. Chen and Srihari (2006) have used Zernike moments as features. Gilperez et al. (2008) presented a method for offline signature verification based on contour features. Nguyen et al. (2009) implemented a model combining

global features and direction features, improving verification accuracy with the side effect of computational overheads. Vargas et al. (2009) have proposed a new offline signature verification model using pseudo-cepstral coefficients as features representing information about pressure distribution in a signature image.

Ji et al. (2010) presented a model for offline signature verification is based on stroke-based features. In this work, features are extracted from every segment of the signature image. Zois et al. (2011) added local line features like orientation and curvature on a curvature feature extracted from the parts of the signature image for the offline signature verification system. Kumar et al. (2012) presented a novel feature set by exploiting the surroundedness property of a signature image, which contains both the shape and texture property of a signature. Prashanth et al. (2012) proposed the offline signature verification technique based on the angular features and achieved good results than the existing techniques. Pal et al. (2015) used Connected Components (CC), Enclosed Regions (ER), Basic Features (BF), and Curvelet Feature (CF)-based approaches to characterize signatures for offline signature verification. Soleimani et al. (2016) have presented a method for offline signature verification using Histogram of Oriented Gradients (HOG) and Discrete Radon Transform (DRT) features. Serdouk et al. (2016) exploited LBP features and the Longest Run features, which describe the signature topology by considering the longest suites of text pixels. Okawa et al. (2018) proposed a new set of KAZE features for offline signature verification, which contains information on the structure of strokes.

Some models have utilized grapho-metric features(Oliveira et al., 2005; Bertolini et al., 2010; Diaz et al., 2019) to detect a signature's authenticity. Most of the verification models have used the same features for all writers and the same dimension. However, only using the global or local features is hard to discriminate between a genuine signature sample and the corresponding skilled forgery. Hence, most of the recent models recommended for offline signature verification are deep learning frameworks based(Khalajzadeh et al., 2012; Bonde et al., 2020).

Alvarez et al. (2016) have used VGG16 CNN architecture as a base architecture to extract the suitable features from the signature. This network consists of 16 layers with learnable parameters. Zhang et al. (2016) designed a deep learning architecture named deep 'Convolutional Generative Adversarial Networks(DCGANs)' to extract features from signature images. DCGANs have a strong generalization ability compared to other feature extraction techniques. Dey et al. (2017) proposed a 'Signet' network to extract features from signatures for offline signature verification. Hafemann et al. (2017) have extracted features employing 'Signet,' efficiently separating the genuine signatures and forgeries in different regions of the feature representation space. Souza et al. (2018) designed a method for offline signature verification based on deep convolutional neural network features.

In Shariatmadari et al. (2019) work, authors have presented a hierarchical one-class convolutional neural network to extract features from genuine signature samples. This network presents lower-level features with high visual quality at the boundary area of the signatures. Jagtap et al. (2020) used 'Siamese network(SNN)' to obtain the features from signatures. 'Siamese network is a twin network frame having identical CNNs which share the same parameters and weights. Jain et al. (2020) used a custom 'shallow Convolutional Neural Network(sCNN)' to automatically learn the features from training signature samples. The proposed architecture is simple but efficient in terms of accuracy. Liu et al. (2021) designed a 'Mutual Signature DenseNet'(MSDN) to extract features from signatures.

'Siamese network is one of the most popular deep learning networks as it can learn robust features from one input image and one target image, giving better results. The proposed deep CNN models can extract relevant features from the given signature data and are robust concerning changes in location and scale. Extraction of appropriate features enhances the performance of a system and reduces the time required to verify a signature.

After extraction of features, the extracted features are stored in a knowledgebase as a representative of the particular signature for the subsequent matching process.

Representation schemes and feature selection

After feature extraction, the extracted features should be properly represented in a feature space. The signature image is transformed into a compact and meaningful description using a proper representation scheme (Impedovo and Pirlo, 2008). Researchers have

been proposed different feature representation schemes for offline signature verification, such as template representation(Shankar et al., 2007; Eskander et al., 2013; Zois et al., 2016), interval-valued representation (Prakash and Guru, 2009; Pal et al., 2015) and BovW(Bag-of-words)(Okawa, 2018; Zhang et al., 2018), sparse representation(Zois et al., 2019) and cluster representation(Wessels and Omlin, 2000; Prakash and Guru, 2009; Suryani et al., 2017; Pandya, 2019). Proper representation minimizes the memory required to store signatures in the knowledgebase and reduces the comparison time during verification.

All the extracted features may not be suitable for verification, and hence one of the challenging issues in signature verification is selecting the most relevant feature for a signer. Different feature selection techniques have been adopted to select discriminating features that distinguish forgeries from genuine. Such as filter-based (Kumar et al., 2012), boosting feature selection (BFS)(Rivard et al. 2013), wrapper feature selection(Kumar et al., 2012; Banerjee et al., 2021), embedded(Kumar et al., 2012), rough set theory based feature selection algorithm(Das and Roy, 2016), genetic algorithm(Sharif et al., 2018), maximum relevance (MRMR)(Zhang et al., 2018), PCA (Principal component analysis)(Ooi et al. 2016; Okawa, 2018), genetic algorithm(Sharif et al. 2018), Gentle Ada-Boost algorithm (Zhang et al., 2016; Zois et al. 2019).

The best feature selection technique reduces the model's training and testing time and increases the classification accuracy.

III DIFFERENT APPROACHES

Researchers have proposed many matching strategies to establish the authenticity of a test signature in offline signature verification. Each matching strategy is designed on a suitable similarity or dissimilarity measure. Since signature verification is a 1:1 matching process, the features of the test signature are compared against the corresponding features of its reference signature sample stored in the knowledge base. In offline signature verification systems generally, three matching approaches are employed: 1) Template Matching, 2) Statistical techniques, and 3) Structural techniques (Impedovo and Pirlo, 2008).

1) Template Matching: The template matching approach is the earliest and straightforward approach. In this matching approach, a single template of genuine or forgery specimen signature for each writer is created and stored in the knowledge base during the development process. Verification is done by comparing a test signature sample against genuine or forgery signature samples templates. Typical template-matching approach for offline signature verification includes the strategies like Dynamic Time Warping (DTW), Euclidean distance, Relaxation matching, and fuzzy logic pattern matching. In some works for matching purposes, the Dynamic Time Warping (DTW) (Herbst and Coetzer,1998; Fang et al., 2003; Shankar et al., 2007; Guler and Meghdadi, 2008) algorithm is adopted. Dynamic programming finds an optimal match between a test signature and its reference signature by allowing for stretching and compression of feature vectors. It can better separate other signatures from genuine ones. The primary objective of DTW is to align feature vectors of signature samples in feature space non-linearly.

Euclidean distance(Qi and Hunt, 1995; Ferrer et al., 2005; Majhi et al., 2006) has been considered a simple template matching strategy in offline signature verification. It does not perform well in all cases since the Euclidean distance block is the only one supplied by all features groups; it enables the system to have a simple and relatively stable metric of the distribution of classes in the whole feature space.

Huang and Yan(2002) proposed a model for offline signature verification based on relaxation matching. The fuzzy concepts(Ferrer et al. 2005; Hanmandlu et al. 2005; Alaei et al., 2017) are applied in the offline signature verification field at the matching stage. Since decision-making uncertainty derives from the fuzzy similarity between genuine and forged samples, system performance has improved through fuzzy logic pattern matching strategies instead of having a threshold separating forged and genuine samples.

The literature shows that template matching can detect random forgeries but is not suitable for detecting skilled forgeries.

2) Statistical approach: When statistical information between the signature images is used as features, authors have employed statistical methods to match the test signature with its corresponding reference signature. In literature, the most commonly used statistical-based matching techniques are simple

distance measures, a Hidden Markov Model(HMM), a Neural Network(NN) approach, Bayesian classifiers, and Support Vector Machine(SVM).

In the case of simple distance measures, each pattern class is characterized by a Gaussian probability distribution function (PDF). It is represented by the mean vector and covariance matrix of the feature vectors belonging to the particular class. One of the commonly used simple distance measures is Euclidean distance (Kalera et al., 2004; Majhi et al., 2006) is considered when only the mean vector of the pattern class is known. The other simple distance measure is Mahalanobis distance (Wen et al., 2009) is applied when the full covariance matrix is available for each signature class. Some authors have adopted Canberra distance(Hamadene et al., 2016) due to its relative efficiency compared to the Euclidean distance.

The Hidden Markov model(HMM) has been applied for offline signature verification(Justino et al., 2000; Coetzer et al., 2004; Alonso-Fernandez et al., 2007; Wen et al., 2009; Batista et al., 2012). HMM-based classifiers are well suited for signature modeling since they capture individual variability. Bayesian classifiers (Kalera et al., 2004; Ruiz-Solar, 2008; Banerjee et al., 2021) are used to carry out matching. It is a statistical classifier, and it reduces the false acceptance rate only if the similarity between the genuine and a forgery is less than 0.74.

Support Vector Machine(SVM) is another widely used statistical classifier for offline signature verification classification. Many researchers adopted the SVM for matching purposes (Bertolini et al., 2010; Vargas et al., 2011; Kumar et al., 2012; Batista et al., 2012; Guerbai et al., 2015; Serdouk et al., 2016; Sharif et al., 2018; Bouamra et al., 2018; Jagtap et al., 2019; Bhunia et al., 2019; Zois et al., 2020). Generally, SVM performance is better than other classification methods when the data is small. However, the main limitations of SVMs are high algorithmic complexity and extensive memory requirements in large-scale tasks.

In literature, Neural networks (NNs) are suitable matching techniques for offline signatures because they can learn complex non-linear input-output relationships through sequential training procedures and adapt to the signature data. The fully connected feed-forward neural network (Bajaj and Chaudhary, 1997) with the classical backpropagation learning algorithm is known as the Backpropagation Network (BPN)(Drouhard et al., 1996). Unlike conventional classifiers such as the k Nearest Neighbour (kNN)(Pal et al., 2016; Shariatmadari et al., 2019) classifier, BPN has a fast response time since it does not memorize all signature samples. However, the learning phase of BPN classifiers is a relatively difficult task in offline signature verification. Baltzakisa and Papamarkos (2001) designed an offline signature verification technique based on a two-stage neural network classifier. In the first stage, the classifier combines the decision results of the neural networks. The results of the first-stage classifier feed a second-stage radial base function (RBF) neural network structure, which makes the final decision. Few researchers have applied MLP (Multi Layer Perceptron) (Khalajzadeh et al., 2012; Tahir et al., 2021) for classification in offline signature verification. These MLPs are relatively simple, containing only one hidden layer, and learning is not done through backpropagation. Serdouk et al. (2016) proposed a novel method for offline signature verification based on the Artificial Immune System (AIS). AIS can detect forgeries; hence it is successful in signature verification.

From the literature, we can found support vector machine(SVM) is one of the best classifiers for offline signature verification as they are suitable for binary classification problems. SVM can identify simulated and straightforward forgeries without previous knowledge and work with high-dimensional data.

In traditional machine learning models, classification accuracy directly depends on features, and this dependency is considered the major drawback of conventional models (Nanni et al., 2017). Most of the recent offline signature verification attempts have applied the different convolutional neural network-based architectures for classification. Such as basic CNN(Dey et al., 2017; Jagtap et al., 2020; Yapıcı et al., 2021; Vohra et al., 2021), convolutional Siamese neural network(Xing et al., 2018), shallow architecture (sCNN) (Jain et al., 2020). Recurrent Neural Network (RNN)(Ghosh et al., 2021) is adopted as a matching strategy for offline signature verification.

Although CNN improves the accuracy, the training process of a CNN model is time-consuming.

3) Structural techniques: Structural techniques are helpful when the signature image is considered a whole entity in offline signature verification. The structural approach describes the given signature image pattern. The commonly used structural methods

in offline signature verification are string and graph matching.

In the string-matching approach(Chen and Srihari, 2005; Shankar et al., 2007; Guler and Meghdadi, 2008), the signature images are represented as a string of points obtained from the signature's exterior contour. Then the similarity between the signature images is computed by comparing an alignment between the points in the two strings. A graph matching approach (Chen and Srihari, 2006; Abuhaiba, 2007; Ramachandra et al., 2008; Maergner et al., 2019) is applied to find the similarity between two signature images in offline signature verification. In this approach, both the reference signature image and the test signature images are represented as a point set, including the local extremas along the signature contours. The graph matching approach depends on the intensities of the pixels, and it avoids using complex features. The drawback of graph matching involves evaluating the similarity of two graphs of signature images, which is time-consuming.

Structural approaches show good performance in detecting genuine signatures and forgeries. But this approach requires a huge training set, leading to a computational burden.

Apart from the widely used matching strategies above, various matching methods were adopted to distinguish forgery signatures from genuine signature samples, like elastic matching(Fang et al., 2003), the symbolic classifier (Prakash and Guru, 2009; Pal et al., 2015). Ooi et al. (2016) employed PNN (Probabilistic Neural Network) to compute the similarity between a test signature with its reference signature. In general, a PNN consists of 4 layers: the input layer, a pattern, summation, and output layers. The pattern layer consists of one neuron for each feature vector in the training set, while the summation layer contains one neuron for each writer class to be recognized. The output layer holds the probability score (i.e., the outcome). PNN is a simple high-speed classification technique.

The literature study shows that all the features used for signature representation are the same for all writers in all the verification models. That means every writer is represented using the same features, either local or global. In addition, the number of features used for representation is also the same for all writers. During verification, the authenticity of a test signature is determined by comparing the test signature and a reference signature using a suitable classifier. The verification models used the same classifier or combinations of classifiers for every writer are referred to as Writer-Independent (WI) models.

However, in reality, every individual has the characteristic of signing. Hence, using the same features for all writers may not be practical, and also, the number of features used for representation need not be the same for all writers. Since the performance of a classifier depends on the usage of the different sets of features for each writer, it may be adequate to verify a signature of an individual using a specific classifier, also known as the Writer-Dependent (WD) model. In this WD classification approach, the model is trained for each writer through an individual classifier. During verification, the features of the test signature are matched with the features of that reference signature. The drawback of the WD classification approach is that the model needs retraining when a new writer is added to the system. To address these problems, some researchers focused on utilizing writer-dependent (WD) characteristics such as features (Manjunatha et al., 2019), classifiers(Parodi et al., 2011; Vargas et al., 2011; Batista et al., 2012; Pirlo et al., 2013; Kumar and Puhan, 2014; Zois et al., 2016; Serdouk et al., 2016; Bhunia et al., 2019; Manjunatha et al., 2019).

Some authors have been explored by combining WI and WD approaches for offline signature verification. The proposed models are trained with a WD classifier, followed by a WI classifier (Eskander et al., 2013; Zhang et al., 2016). Soleimani et al. (2016) have combined the idea of multitasking and transfer learning for offline signature verification, which combines both WI and WD approaches. Hafemann et al., 2017 presented a two-phase approach for offline signature verification: a writer-independent feature learning phase followed by writer-dependent classification. The concept of combining WI and WD approaches in offline signature verification improved system performance with decreased computational complexity.

Further, fusion-based approaches have been proposed for offline signature verification to improve system accuracy. Fusion may be either at feature level (Fierrez-Aguilar et al., 2004; Prakash and Guru, 2009; Kumar et al., 2010; Yilmaz et al., 2011; Rivard et al., 2013; Yılmaz et al., 2016; Dutta et al., 2016; Okawa et al., 2018), classifier level (Bertolini et al., 2010; Yilmaz et al., 2011; Fick et al., 2016), decision level

(Oliveira et al., 2007; Rivard et al., 2013; Batista et al., 2012) and Score level fusion(Prakash and Guru, 2010; Yılmaz et al., 2016).

Very few public datasets are available for offline signature verification. MCYT-75 is an offline signature dataset consisting of handwritten signatures of 75 writers. Many models have used MCYT-75 for evaluation purposes (Vargas et al., 2011; Ooi et al., 2016; Hafemann et al., 2017; Sharif et al., 2018; Zois et al., 2020; Jain et al., 2021).

CEDAR is another offline signature dataset consists of signatures samples of 55 writers. CEDAR dataset is used in models (Kumar and Puhan, 2014; Guerbai et al., 2015; Serdouk et al., 2016; Hafemann et al., 2017; Zois et al., 2019; Zois et al., 2020).

GPDS offline signature corpus consisting of handwritten signatures of 960 writers. The authors used the GPDS database for the evaluation purpose of their model (Zois et al., 2016; Serdouk et al., 2016; Soleimani et al., 2016; Hafemann et al., 2017; Dey et al., 2017; Sharif et al., 2018; Zois et al., 2019; Ruiz et al., 2020). Almost all of the existing models are demonstrated only on small datasets.

IV Different datasets used for signature verification are shown in Table-1

Data set	Configuration
MCYT-75 (Ministerio de Ciencia YTecnologia) (Ortega-Garcia et al., 2003)	75 Users, 15 Genuine and 15 Skilled forgeries from each user (Database size =75x15 + 75x15 = 2250)
CEDAR (Center of Excellence for Document Analysis and Recognition) created at CEDAR, Buffalo University (Kalera et al., 2004)	55 Users, 24 Genuine and 24 Forgeries from each user (Database size = 55x24+55x24=2640)
GDPS-960 Digital Signal Processing Group (GPDS) of The Universidad de Las Palmas de Gran Canaria (ULPGC-Spain) developed the GPDS(Vargas et al., 2007)	960 Users, 24 Genuine and 30 forgeries (Database size = 960 x 24 + 960 x 30 = 51840)

The sizes of these datasets are not enough to study the consistency and commonality of features across a large population. The study of consistency and commonality of features among writers across a large population is a challenging issue, which requires the creation of sufficiently large data sets. The collection of signature data from individuals requires significant time and effort. Researchers have proposed different approaches to generate synthetic signatures from handwritten signatures to overcome this problem (Rabasse et al., 2008; Ferrer et al., 2013; Diaz-Cabrera et al., 2014; Diaz et al., 2016; Ruiz et al., 2020).

V OBSERVATIONS

From the literature on offline signature verification, it is observed that

- Most of the verification models are writer-independent.
- Availability of the number of genuine signatures for training purposes is usually less in many applications.
- It is difficult even for a forensic expert to tell correctly whether a signature is authentic or not just by the visual inspection of the signature.
- Signature is easier to forge compared to other biometrics.
- The fusion approach yielded a better result. Very few attempts on selecting suitable thresholds, features, and suitable classifiers for each writer.

Performance Evaluation

The performance of any signature verification system is evaluated based on its ability to differentiate genuine accurately and forgery signatures. Signature verification is a two-class pattern recognition problem, and one class is a genuine signature class, and the other is the forgery class. Most signature verification processes consider three types of forgeries: Skilled forgery, Casual forgery, and Random forgery (Impedovo and Pirlo, 2008).

a. Skilled forgery:-This type of forgery is produced by the forger who has access to the genuine signature of the person. Skilled forgeries are produced after good practicing of the writer's original signature, and hence they are challenging to detect.

b. Casual forgery:-This type of forgery is produced by an imitation who is familiar with the names of a genuine person but does not have access to actual authentic signatures.

c. Random forgery:- Random forgeries are generated by a forger who does not know about the signer and their signatures. They are the most common type of forgery encountered in fraudulent cases, and they are straightforward to detect even by the naked eye. A signature verification system usually results in two types of error.

The performance of the signature verification model is given in terms of FAR, FRR, AER, EER, and ROC.

• FAR (False acceptance rate) – Percentage of forgery signatures falsely accepted as a genuine signature. It is also known as type-I error.

• FRR (False rejection rate) – Percentage of genuine signatures falsely accepted as forgery signature. It is also known as type-II error.

- AER(Average Error Rate) is the point where FAR is equal to FRR(Souza et al., 2018; Sharif et al., 2020; Arab et al., 2020).
- Plot of FAR v/s FRR for varying threshold is known as ROC Curve(Oliveira et al., 2007; Kumar et al., 2010; Sam et al., 2019; Banerjee et al., 2021). The point at which FAR and FRR intersect is known as Equal Error Rate (EER).

Most of the verification systems have used EER as a performance measure (Fawcett, 2006; Oliveira et al., 2007; Ooi et al., 2016; Zois et al., 2019; Jain et al., 2021). ROC curve is shown in Figure-3.

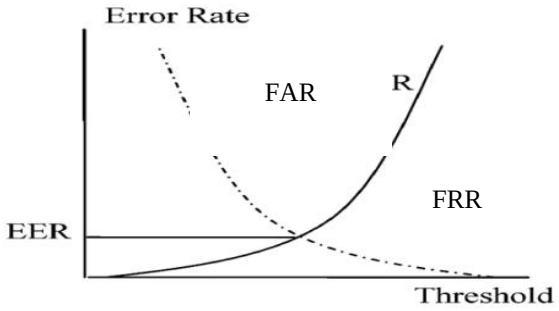

Figure-3: ROC curve

VI CONCLUSION

During the last four decades, signature verification has attracted many researchers due to its commercial and scientific applications. Hence, the literature survey extensively covers various pre-processing steps, features used, feature selection strategies, matching techniques, and adapted performance measures. Although many models differ in the features used and the classifiers adopted, deciding the best feature set and the best classifier for verification is still a challenging research problem.

In summary, the models focused on a writer-dependent offline signature verification system effectively capture an individual writer's characteristics by using image processing and pattern recognition techniques.

REFERENCE

[1] AbdelRaouf, A., & Salama, D. (2018, December). Handwritten Signature Verification using Haar Cascade Classifier Approach. In 2018 13th International Conference on Computer Engineering and Systems (ICCES) (pp. 319-326). IEEE.

[2] Abuhaiba, I. S. (2007). Offline signature verification using graph matching. Turkish Journal of Electrical Engineering & Computer Sciences, 15(1), 89-104.

[3] Alaei A, S. Pal, U. Pal, "An Efficient Signature Verification Method Based on an Interval Symbolic Representation and a Fuzzy Similarity Measure", IEEE Transactions on Information Forensics and Security, Vol. 12, No. 10, pp. 2360-2372, 2017.

[4] Alonso-Fernandez, F., Fairhurst, M. C., Fierrez, J., & Ortega-Garcia, J. (2007, September). Impact of signature legibility and signature type in off-line signature verification. In *2007 Biometrics Symposium* (pp. 1-6). IEEE.

[5] Alvarez, G., Sheffer, B., & Bryant, M. (2016). Offline signature verification with convolutional neural networks. *Technical report, Stanford University*.

[6] Arab, N., Nemmour, H., & Chibani, Y. (2020, November). MultiScale Fusion of Histogram-based Features for Robust Off-line Handwritten Signature Verification. In *2020 IEEE/ACS 17th*

International Conference on Computer Systems and Applications (AICCSA) (pp. 1-5). IEEE.

[7] Bajaj R and S. Chaudhary, "Signature verification using multiple neural classifiers", Pattern Recognition, Vol.30, No.1, pp.1-7, 1997.

[8] Baltzakis, H., and N. Papamarkos. "A new signature verification technique based on a two-stage neural network classifier." *Engineering applications of Artificial intelligence* 14.1 (2001): 95-103.

[9] Banerjee, D., Chatterjee, B., Bhowal, P., Bhattacharyya, T., Malakar, S., & Sarkar, R. (2021). A new wrapper feature selection method for language-invariant offline signature verification. *Expert Systems with Applications*, *186*, 115756.

[10] Banerjee, D., Chatterjee, B., Bhowal, P., Bhattacharyya, T., Malakar, S., & Sarkar, R. (2021). A new wrapper feature selection method for language-invariant offline signature verification. *Expert Systems with Applications*, *186*, 115756.

[11] Batista L, E. Granger, R. Sabourin, "Generative-Discriminative Ensembles for Off-Line Signature Verification", Pattern Recognition, vol.45, pp.1326-1340, 2012.

[12] Bertolini D, L. S. Oliveira, E. Justino, R. Sabourin, "Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers", Pattern Recognition, No. 43, pp. 387-396, 2010.

[13] Bhunia, A. K., Alaei, A., & Roy, P. P. (2019). Signature verification approach using fusion of hybrid texture features. *Neural Computing and Applications*, *31*(12), 8737-8748.

[14] Bonde, S. V., Narwade, P., & Sawant, R. (2020, March). Offline Signature Verification Using Convolutional Neural Network. In *2020 6th International Conference on Signal Processing and Communication (ICSC)* (pp. 119-127). IEEE.

[15] Bouamra, W., Djeddi, C., Nini, B., Diaz, M., & Siddiqi, I. (2018). Towards the design of an offline signature verifier based on a small number of genuine samples for training. *Expert Systems with Applications*, *107*, 182-195.

[16] Chen, S., & Srihari, S. (2005, August). Use of exterior contours and shape features in off-line signature verification. In *Eighth International Conference on Document Analysis and Recognition (ICDAR'05)* (pp. 1280-1284). IEEE.

[17] Chen, S., & Srihari, S. (2006, August). A new off-line signature verification method based on graph. In *18th International Conference on Pattern Recognition (ICPR'06)* (Vol. 2, pp. 869-872). IEEE.

[18] Coetzer J, B. M. Herbst, J.A. du Preez, "Offline Signature Verification Using the Discrete Radon Transform and a HiddenMarkovModel", EURASIP Journal on Applied Signal Processing No.4, pp.559–571, 2004.

[19] Das, S., & Roy, A. (2016). Signature verification using rough set theory based feature selection. In *Computational Intelligence in Data Mining—Volume 2* (pp. 153-161). Springer, New Delhi.

[20] Deng, P. S., Liao, H. Y. M., Ho, C. W., & Tyan, H. R. (1999). Wavelet-based off-line handwritten signature verification. *Computer vision and image understanding*, *76*(3), 173-190.

[21] Dey, S., Dutta, A., Toledo, J. I., Ghosh, S. K., Lladós, J., & Pal, U. (2017). Signet: Convolutional siamese network for writer independent offline signature verification. *arXiv preprint arXiv:1707.02131*.

[22] Diaz, M., Ferrer, M. A., Eskander, G. S., & Sabourin, R. (2016). Generation of duplicated off-line signature images for verification systems. *IEEE transactions on pattern analysis and machine intelligence*, *39*(5), 951-964.

[23] Diaz, M., Ferrer, M. A., Impedovo, D., Malik, M. I., Pirlo, G., & Plamondon, R. (2019). A perspective analysis of handwritten signature technology. *Acm Computing Surveys (Csur)*, *51*(6), 1-39.

[24] Diaz-Cabrera, M., Ferrer, M. A., & Morales, A. (2014, September). Cognitive inspired model to generate duplicated static signature images. In *2014 14th International Conference on Frontiers in Handwriting Recognition* (pp. 61-66). IEEE.

[25] Drouhard, J. P., Sabourin, R., & Godbout, M. (1996). A neural network approach to off-line signature verification using directional PDF. Pattern Recognition, 29(3), 415-424.

[26] Dutta, A., Pal, U., & Lladós, J. (2016, December). Compact correlated features for writer independent signature verification. In *2016 23rd*

international conference on pattern recognition (ICPR) (pp. 3422-3427). IEEE.

[27] Eskander, G. S., Sabourin, R., & Granger, E. (2013). Hybrid writer-independent–writer-dependent offline signature verification system. *IET biometrics*, *2*(4), 169-181.

[28] Fang B, C. H. Leung, Y.Y. Tang, K.W. Tse, P.C.K. Kwok and Y.K. Wong, "Offline signature verification by tracking of feature and stroke position", Pattern Recognition, Vol.36, pp.91-101, 2003.

[29] Fawcett, T. (2006). An introduction to ROC analysis. *Pattern recognition letters*, *27*(8), 861-874.

[30] Ferrer, M. A., Alonso, J. B., & Travieso, C. M. (2005). Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE transactions on pattern analysis and machine intelligence*, *27*(6), 993-997.

[31] Ferrer, M. A., Diaz, M., & Carmona-Duarte, C. (2017, November). Two-steps perceptual important points estimator in 8-connected curves from handwritten signature. In *2017 Seventh International Conference on Image Processing Theory, Tools and Applications (IPTA)* (pp. 1-5). IEEE.

[32] Ferrer, M. A., Diaz-Cabrera, M., & Morales, A. (2013, June). Synthetic off-line signature image generation. In *2013 international conference on biometrics (ICB)* (pp. 1-7). IEEE.

[33] Ferrer, M. A., Vargas, J. F., Morales, A., & Ordonez, A. (2012). Robustness of offline signature verification based on gray level features. *IEEE Transactions on Information Forensics and Security*, *7*(3), 966-977.

[34] Fick, C., Coetzer, J., & Swanepoel, J. (2016, November). Efficient curve-sensitive features for offline signature verification. In *2016 Pattern Recognition Association of South Africa and Robotics and Mechatronics International Conference (PRASA-RobMech)* (pp. 1-6). IEEE.

[35] Fierrez-Aguilar, J., Alonso-Hermira, N., Moreno-Marquez, G., & Ortega-Garcia, J. (2004, May). An off-line signature verification system based on fusion of local and global information. In *International workshop on biometric authentication* (pp. 295-306). Spring