A COMPREHENSIVE REVIEW OF OFFLINE SIGNATURE VERIFICATION

Abstract

Authors

Signatures are a means to represent a Sunil Kumar D S person either directly or indirectly in all the Department of Computer Applications legal documents and (as well as) legal Administrative Management College transactions. Signatures are a form of Bangalore, India biometrics characterized by their uniqueness. dssunil6@gmail.com Biometrics is a viable technology in various application domains where the identification Wincy Abraham or verification of an individual is contingent Department of Computer Science upon human characteristics. In the realm of Assumption College Autonomous biometrics, human traits are classified into Changanacherry, Kerala, India two categories: behavioral and physiological. wincya@gmail.com Within the realm of behavioral biometrics, we find signature, gait, and voice biometrics. Meanwhile, in the domain of physiological biometrics, we encounter traits such as face, palm, iris, finger or thumbprints, and DNA sequences. In this paper we are presenting a comprehensive review on offline signature verification by incorporating contributions from various authors. We have also discussed types of signatures and challenges involved in signature verification. This paper also describes steps involved in signature verification process.

I. INTRODUCTION

The use of signatures as a behavioral biometric attribute for authenticating and identifying individuals is widely accepted in society. Each person generates a unique signature, allowing for the differentiation of one signature from another. This distinctive characteristic has led people to employ their signatures in various aspects of daily life, including transactions, administrative tasks, and commercial activities. Signatures serve to enhance the authenticity and legality of documents when individuals sign them. However, in these applications, there exists a risk of signature forgery, where someone attempts to counterfeit another person's signature for personal gain. To address this issue and to verify the legitimacy of signatures and individuals, a biometric-based signature verification system can be employed. Signature verification finds application in various scenarios, including the authentication of checks, certificates, financial bonds, agreement notes, office documents, notifications, and letters, among others.

A forged signature is an imitation of a genuine signature created by a fraudulent signer. Forge signatures can be categorized into three main types: skilled, random, and simple forgery.

In skilled forgery, the forger carefully observes and analyzes the original signature. Subsequently, the forger practices replicating the original signature to the best of their ability before proceeding with the forgery. Simple forgery involves a forger who is already familiar with the pattern of the signature they intend to replicate. They attempt to recreate the signature without extensive practice. Random forgery, on the other hand, occurs when the forger lacks knowledge about the specific pattern of the original signature. In this case, the forger makes an educated guess or assumption while attempting to mimic the signature.

Handwritten signature verification can be categorized into two main types: Off-line Signature Verification and On-line Signature Verification. The primary distinction between these two methods lies in how the signature is acquired. In Off-line Signature Verification, signature samples are collected from a signer on paper, and the scanned copy of this paper is used for the verification process. Various image processing techniques are applied to determine whether the signature is genuine or forged in what is also known as Static Signature Verification.

Conversely, On-line Signature Verification allows the signer to write their signature on a sensor-based surface using digital devices such as a scanner or pen tablet. Subsequently, several image processing operations are conducted for signature verification, a method known as Dynamic Signature Verification.

In both types of verification, various image processing techniques are utilized at different stages, including preprocessing, feature extraction, and classification, to facilitate the verification process.

1. Challenges in Signature Verification: In signature verification, two distinct challenges are often encountered: inter-class variation and intra-class variation. Inter-class variation presents a significant threat to any signature verification system, as it pertains to situations where different individuals attempt to forge the signature of a successful individual. The extent of damage resulting from such forgeries depends on the specific application in which the signature is involved.

Conversely, intra-class variation occurs when the same individual writes their signature with slight variations. These variations may be attributed to factors such as old age, ill-health, or writing under pressure. Detecting whether a signature is genuine or forged in cases of intra-class variation can be challenging, much like the detection of skilled forgery.

II. STEPS INVOLVED IN OFF-LINE SIGNATURE VERIFICATION SYSTEM

The process involves several distinct steps, including Data Acquisition, Data Pre-Processing, Feature Extraction, Classification, and finally, Performance Evaluation. Figure 1 illustrates the general diagrammatic representation of an offline signature verification system.



Figure1: Signature Verification Model

1. Data Acquisition: Signature samples are obtained from signers using black or blue ballpoint pens on plain white paper. Subsequently, scanned copies of these papers are used in the signature verification process. Several publicly accessible signature databases are available for research purposes, including well-known ones like CEDAR, GPDS, and ICDAR2009 (as shown in Table-1). Sample signatures are shown in Figure 2.

Data	No.Signatures	No.	No.of	Total No.
Bases	Contributors	Genuine	Skilled	Signatures
		Signatures	Forgeries	_
CEDAR	55	24	24	2640
GPDS 160	160	24	30	8640
GPDS	4000	24	30	216000
MCYT100	100	25	25	5000
			CEDAR DATASE	r

 Table 1: Details of Offline Signature Datasets



Figure 2: Signature Samples of GPDS and CEDAR datasets.

- 2. Data Pre-Processing: The data samples collected (Figure 2) are inherently raw and may contain various imperfections such as noise, redundant areas, inappropriate colors, and high scaling, among others. Extracting significant features from these types of data samples can be challenging. Therefore, it is essential to apply several pre-processing techniques to prepare the data samples for further processing. Preprocessing plays a crucial role in facilitating the efficient extraction of relevant features, ultimately enhancing the model's performance. Additionally, it helps reduce the computational cost in the classification process. Some pre-processing techniques include resizing, binarization, thinning, and cropping.
- **3. Feature Extraction:** Features are attributes that describe an image, essentially representing the image's characteristics. When dealing with signature verification using conventional machine learning algorithms, it becomes essential to supply manually crafted features for training and testing the model. On the other hand, if a signature verification model utilizes a deep learning architecture, the architecture inherently handles feature engineering. Nevertheless, traditional machine learning techniques prioritize feature extraction for solving classification problems. After features are extracted from the data, they form a feature vector. These feature vectors serve as a knowledge base that is utilized to train the model. Subsequently, the trained model is tested with unseen data to evaluate its effectiveness.
- 4. Classification: This is a supervised machine learning algorithm in which data samples are categorized according to their labels. Classification, a traditional machine learning task, involves distinguishing data samples based on the features linked to their respective labels. Numerous classifiers are accessible for data classification, including Support Vector Machine, Multi-Layer Perceptron, Naïve Bayes, K-Nearest Neighbor, and Decision Tree, among others. When classifying data into two categories, it is referred to

as binary classification. On the other hand, if the classification encompasses more than two data classes, it is termed multi-class classification.

- **5. Performance Evaluation:** Evaluating the performance of the designed model is essential. Various performance metrics are accessible to assess the accuracy of the designed model, including the following:
 - **False Acceptance Ratio:** it's the ratio of number of false acceptance by total number of submission. It involves incorrect acceptance of forge signature as genuine.
 - False Rejection Ratio: it's the ratio of number of false rejection by total number of genuine signature. Here it measures the number of genuine signatures are incorrectly rejected.
 - Equal Error Rate: it's the average of both Type-I and Type-II error.
 - **ROC Curve:** it's pictorial comparative representation of true-positive rate and false-positive rate at different threshold.
 - Confusion Matrix: it's an M x M matrix consists of actual target values against predicted values.

III. EXISTING APPROACHES IN SIGNATURE VERIFICATION

Several authors have put forward diverse methods for signature verification, and a selection of them is discussed in this section. Kumar et al. [1] introduced an off-line signature verification approach based on the "surroundedness" property of signatures. Their method primarily focuses on the shape of a signature and analyzes the spatial distribution of black pixels around a candidate pixel. To assess its effectiveness, they employed two well-known classifiers, namely Multi-layer Perceptron and Support Vector Machine, and evaluated them using two publicly accessible datasets: GPDS 300 corpus and CEDAR.

Pushpalatha et al. [2] introduced a novel off-line signature verification approach. Their method incorporates a Polar feature descriptor for signatures, which includes radon transform and Zernike moments. To perform verification, they employed a Multiclass Support Vector Machine. By applying PLS regression on a sample against all samples in the database, they obtained a regression score. Additionally, a Hidden Markov Model was utilized to calculate the log likelihood of the sample in comparison to all other samples.

Hamadene et al. [3] proposed two different approaches of off-line handwritten signature verification (HSV) namely writer-dependent and writer independent HSV. Contourlet transform and the co-occurrence matrix are used in this approach. Experiments are conducted on CEDAR dataset. There are two approaches namely writer dependent and writer independent.

Shekar, B.H. et al. [4] introduced an approach for off-line signature verification based on the morphological pattern spectrum structured within a grid. In this method, the signature image is divided into eight equally sized vertical grids, and a structured morphological pattern spectrum is obtained for each grid. Each spectrum is represented by a 10-bin histogram.

Shekar, B.H. et al. [5] introduced an algorithm called Eigen-signature: A Robust and Efficient Offline Signature Verification Algorithm. This model consists of two stages: preprocessing and Eigen-signature construction. During the pre-processing stage, it transforms a scanned signature into a shape form, and the Eigen-signature construction is designed to extract the feature vector from a shape-form signature.

Bharathi et al. [6] proposed a Chain Code Histogram and Support Vector Machine model for Off-line Signature Verification. This approach relies on chain code histogram features that are improved using the Laplacian of Gaussian filter for off-line signature verification. In this proposed method, the four-directional chain code histogram of each grid along the contour of the signature image is extracted. The Laplacian of Gaussian filter is employed to enhance the extracted features of each signature sample. As a result, the enhanced features extracted from all signature samples in the off-line signature dataset form the knowledge base. Subsequently, the Support Vector Machine (SVM) classifier is utilized for the verification process.

Shekar, B.H. et al. [7] introduced an off-line signature verification system based on LOG-processed local features. The signature's contour is divided into four grids, and the fourdirectional chain code histogram for each grid is extracted and then processed with the Laplacian of Gaussian filter to enhance the features. Recognition is performed using multilayer perceptrons.

Bhattacharya et al. [8] proposed an off-line signature verification and recognition system using pixel matching technique. The proposed method uses sample signature from the database for the verification. The signature acquisition is done by capturing signature from a sheet of paper. During pre-processing a border to the boundary of the scanned signature is set. This will help to identify the exact boundary of the signature. Color and noise is removed. Then the images are converted in to binary images. This information can be stored in the database as a sample signature. A color normalization method is utilized to determine the color of each pixel. Noise resolution method is used to remove the noise. After color normalization some small black color pixel has been found which has been removed. Then the signature is adjusted to locate the exact position of the signature. The solution proposed to identify edges of the signature in the rectangular box from its left, right, top and bottom sides. The co-ordinate geometry is used to find the angle of the signature and to rotate the image accordingly. After all these steps the resulted signature images are compare with the sample database using the method Pixel Matching Technique.

Manoj Kumar et al. [9] proposed a method, which employs inter-point envelope based distance moments for offline signature verification. It exposes two types of features namely

A. DC- Line

B. Envelope – to – Envelope

The high-dimensional inter-point distances are utilized for the calculation of central moments, including variances, skewness, kurtosis, and mean. These resulting moment features are employed in the training process.

Hafemann et al. (Hafemann, 2017) [10] presents formulations learning features for offline signature verification. Learning features are used to train writer-dependent classifiers using deep convolutional neural networks. The Author's proposed two-way approach one is writer-independent feature learning stage and another is writer-dependent classification stage. The aim is to acquire data from different users to formulate learning features and subsequently train the classifier for each user using this feature space. Thus it exhibits the property of both writer independent and writer dependent. This approach introduces two formulations: one is to treat forgery of each user as an individual class and another is exploitation of multi-task learning methods. A deep CNN is constructed to perform learning features followed by classification.

J.F. Vargas et al. [11] introduced an off-line signature verification approach relying on grey level information and employing texture features. This method operates at the global image level, quantifying grey level fluctuations within the image through statistical texture characteristics. The analysis involves the examination and utilization of the co-occurrence matrix and local binary pattern as features. The process initiates with a proposed background removal step. Additionally, a histogram is processed to mitigate the impact of various writing ink pens employed by signers. To train an SVM model, genuine samples and random forgeries were employed, while testing involved random and skilled forgeries.

Rajesh Kumar et al. [12] Introduces a novel feature set for off-line signature verification, which is founded on the concept of the surroundedness property of a binary signature image. This newly proposed feature set characterizes the signature's shape by considering the spatial arrangement of black pixels surrounding a given pixel within the signature. Additionally, it incorporates a measure of texture, capturing the correlation among signature pixels in the vicinity of the candidate pixel. What sets this feature set apart is its unique combination of shape and texture properties, a departure from the majority of earlier proposed features for off-line signature verification. To streamline the feature set, it has also undergone evaluation using various feature selection techniques based on its intuitive problem-oriented design.

D. Bertolinia, et al. [13] suggested an approach to enhance the accuracy of writerindependent off-line signature verification by employing an ensemble of classifiers. The authors presented a novel graphometric feature set that focuses on capturing the curvature of the signature's most perceptually significant segments. This approach involves modeling the signature's shape using Bezier curves and subsequently extracting relevant features from these curves.

Kruthi.C, et al. [14] proposed Offline Signature Verification Using Support Vector Machine. From the pre-processed signatures, various features are extracted and stored individually in a database. These features include centroid, center of gravity, the count of loops, horizontal and vertical profiles, and normalized area. Subsequently, the values stored in the database are input into a support vector machine (SVM), which utilizes these values to establish a hyperplane for classifying the signature as either genuine or forged, based on specific feature values.

Mustafa Berkay et al. [15] the authors introduced an offline signature verification system that utilizes a combination of HOG and LBP features for classification. This system is based on local histogram features of the signature. To achieve this, the signature is divided into zones using both Cartesian and polar coordinate systems, and for each zone, two distinct histogram features are computed: the histogram of oriented gradients (HOG) and the histogram of local binary patterns (LBP).

Juan Hu et al.[16] The authors introduced an offline signature verification system that utilizes a real Adaboost classifier in combination with pseudo-dynamic features. These pseudo-dynamic features are based on gray level information and encompass three distinct components: local binary pattern (LBP), gray level co-occurrence matrix (GLCM), and histogram of oriented gradients (HOG).

Md. AsrafulHaquel et al. [17] They introduced an offline signature verification approach utilizing Weighted Blocks, which relies on the structural characteristics of various image segments. This method employs a novel technique for feature extraction, dividing the image into multiple blocks. The primary features pivotal in this approach encompass the image center, block center, the Euclidean distance between the image center and each block center, and the pixel count within each block. Each block is assigned specific weightages based on its contribution to the overall image composition.

GeethaGanapathi et al. [18] proposed a fuzzy framework for offline signature verification. Authors presents a similarity measure based person-dependent off-line signature verification using fuzzy techniques in image contrast enhancement, feature extraction and verification.

AtefehForoozandeh et al. [19] proposed Circlet Transform and Statistical feature based on offline handwritten signature verification. Circlet Transform is a new mathematical transform used to trace out circular pattern like objects in digital images. Authors extracted statistical properties by computing Gray Level Co-occurrence Matrix of circlet coefficients. The GLCMs values give relative position information about neighbouring pixels. This information is calculated in eight directions at an angle 0^{0} , 45^{0} , 90^{0} , 135^{0} , 180^{0} , 225^{0} , 270^{0} and 315^{0} . Five statistical features such as entropy, correlation, homogeneity, energy and contrast are extracted from obtained GLCMs.

Yasmine Guerbai et al. [20] propose a design of handwritten signature verification by using one class support vector machine i.e. OC-SVM. This method takes only genuine signature model. They consider a set of writers in order to train the samples, which find the parameters for handwritten signature verification. Each writer having their own parameter but generally all has same parameters. When new one enrols in/to the system, their signature parameters are automatically calculated. It is writer independent parameters for hand written signature verification system. The main advantage of OC-SVM is in descriptions of signature parameters. Based on these parameters it neither rejects nor accept the new signature.

Dilara Gumusab et al. [21] proposed offline signature verification based on capsule networks. This model requires few data samples for training. This model consists four functional parts where two convolutional layers, one primary capsule and one digit capsule with fully connected layers. Convolving the input image with different kernels gives different output which is local texture information. These information are kept in different capsule from primary cap. The output of primary cap is numerical information. The information is further squashed to keep only discriminative features. Digit cap keeps discriminative feature for each class. Finally these fully connected layers use the outputs for classification.

Hanmandlu et al. [22] proposed offline signature verification based on deep learning method. Proposed method exploits convolutional neural network for feature extraction and support vector machine for classification. This architecture consists 5 convolutional layers where fist layer consists 96 filters with size 11x11, stride 4 and zero padding. Second layer consists 256 filters with size 5x5, stride 1 and padding 2. The third and fourth convolutional layer consists equal number of 384 filters with size 5x5, stride 1 and padding 1. The fifth convolutional layer have 256 filters with size 3x3, stride 1 and padding 1. Next layer is maxpooling layer. Pooling is the process of keeping an element from the feature map window to reduce the dimensionality. Max-pooling keeps the maximum or largest element from each feature map window. Next is a fully connected layer, where each layers are interconnected so that output of previous layer will be input to the next layer. Authors use support vector machine classifier for classification of objects instead of softmax or sigmoid activation function for output layer.

Amrutha et al,[23] [2019] proposed offline handwritten signature verification using Convolutional Neural Network. Authors proposed method involves deep CNN architecture with Support Vector Machine for classification. The architecture consists total 18 layers, out of which 5 layers are convolutional, 6 layers are ReLu, 3 layers are max-pooling layers, 2 layers for normalization and 2 fully connected layers. The first convolutional layers consists 96 filters with 11x11 convolution filters with 4 stride and zero padding. The second convolutional layer consists 5x5 convolutional filters, 1 stride and 2 padding. The remain third, fourth and fifth convolutional layer consist 3x3 filter with 1 stride and 1 padding respectively. ReLu activation function used to activate the neurons. All the three max-pooing layers consists 4096 neurons each. Finally the output of the architecture is fed to support vector machine to classify the objects, here the objects are signature images.

Amrutha b. Jagatap et al. [24] proposed Siamese Neural Network for offline signature verification. Siamese Neural Network is a two identical (Twins) convolutional neural network, which possess same parameters and having same weights apart. The two deep CNN architecture includes convolution layers with max pooling layer and fully connected layers. Here convolutional layer uses filters to convolve; the input is the product of height, width and depth information of a signature image. ReLu is an activation function generates features from input data. Max-Pooling layer is used to down sample the data. Where it convolves with an M x M matrix and keeps the maximum element in a matrix form. The network is fully connected layers are embedded to the input image. The output will be in the binary form if the both signature are same then 1 is labeled otherwise 0 is labeled. Euclidian distance metric is used to compute similarity and dissimilarity index.

IV. CONCLUSION

We have briefly elaborated the working principle of Offline Signature Verification. We have also discussed types of signature verification. We have also elaborated phases involved in signature verification with detailed explanation. An intensive literature survey has been carried out and the research gaps that led us to carry out this research work are incorporated. The motivation and identified research objectives are presented. Offline signature verification plays a vital role in distinguishing or discriminating genuine signatures from forge. Signature is a most trusted biometric, therefore it's widely used in various applications. In this paper we briefly explained some of the existing approaches from the literature. We have also explained a few state-of-the-art deep learning papers proposed by several authors.

REFERENCES

- [1] Kumar, R., Sharma, J. D., & Chanda, B. (2012). Writer-independent off-line signature verification using surroundedness feature. Pattern recognition letters, 33(3), 301-308.
- [2] Pushpalatha, K. N., Gautham, A. K., Shashikumar, D. R., ShivaKumar, K. B., & Das, R. (2013). Offline signature verification with random and skilled forgery detection using polar domain features and multi stage classification-regression model. International Journal of Advanced Science and Technology, 59, 27-40.
- [3] Hamadene, A., Chibani, Y., &Nemmour, H. (2012, September). Off-line handwritten signature verification using contourlet transform and co-occurrence matrix. In 2012 International Conference on Frontiers in Handwriting Recognition (pp. 343-347). IEEE.
- [4] Shekar, B. H., Bharathi, R. K., Kittler, J., Vizilter, Y. V., &Mestestskiy, L. (2015, May). Grid structured morphological pattern spectrum for off-line signature verification. In 2015 international conference on biometrics (ICB) (pp. 430-435). IEEE.
- [5] Shekar, B. H., &Bharathi, R. K. (2011, June). Eigen-signature: A robust and an efficient offline signature verification algorithm. In 2011 international conference on recent trends in information technology (ICRTIT) (pp. 134-138). IEEE.
- [6] Bharathi, R. K., &Shekar, B. H. (2013, August). Off-line signature verification based on chain code histogram and support vector machine. In 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI) (pp. 2063-2068). IEEE.
- [7] Shekar, B. H., &Bharathi, R. K. (2013, January). Log-grid based off-line signature verification system. In Proceedings of the Fourth International Conference on Signal and Image Processing 2012 (ICSIP 2012) Volume 2 (pp. 321-330). India: Springer India.
- [8] Bhattacharya, I., Ghosh, P., & Biswas, S. (2013). Offline signature verification using pixel matching technique. Procedia Technology, 10, 970-977.
- [9] Kumar, M. M., &Puhan, N. B. (2014, July). Inter-point envelope based distance moments for offline signature verification. In 2014 International Conference on Signal Processing and Communications (SPCOM) (pp. 1-6). IEEE.
- [10] Hafemann, L. G., Sabourin, R., & Oliveira, L. S. (2017). Learning features for offline handwritten signature verification using deep convolutional neural networks. Pattern Recognition, 70, 163-176.
- [11] Vargas, J. F., Ferrer, M. A., Travieso, C. M., & Alonso, J. B. (2011). Off-line signature verification based on grey level information using texture features. Pattern Recognition, 44(2), 375-385.
- [12] Kumar, R., Sharma, J. D., & Chanda, B. (2012). Writer-independent off-line signature verification using surroundedness feature. Pattern recognition letters, 33(3), 301-308.
- [13] Bertolini, D., Oliveira, L. S., Justino, E., &Sabourin, R. (2010). Reducing forgeries in writer-independent off-line signature verification through ensemble of classifiers. Pattern Recognition, 43(1), 387-396.
- [14] Kruthi, C., &Shet, D. C. (2014, January). Offline signature verification using support vector machine. In 2014 Fifth International Conference on Signal and Image Processing (pp. 3-8). IEEE.
- [15] Yilmaz, M. B., Yanikoglu, B., Tirkaz, C., &Kholmatov, A. (2011, October). Offline signature verification using classifier combination of HOG and LBP features. In 2011 international joint conference on Biometrics (IJCB) (pp. 1-7). IEEE.
- [16] Hu, J., & Chen, Y. (2013). Offline Signature Verification Using Real Adaboost Classifier Combination of Pseudo-dynamic Features. 2013 12th International Conference on Document Analysis and Recognition, 1345-1349.

- [17] Haque, M.A., Ali, T., & Ali, R. (2012). Offline signature verification method using weighted block analysis. IEEE-International Conference On Advances In Engineering, Science And Management (ICAESM -2012), 134-139.
- [18] Ganapathi, G., &Rethinaswamy, N. (2014). A fuzzy framework for offline signature verification. 2014 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), 1-6.
- [19] Foroozandeh, A., Hemmat, A.A., & Rabbani, H. (2020). Offline Handwritten Signature Verification Based on Circlet Transform and Statistical Features. 2020 International Conference on Machine Vision and Image Processing (MVIP), 1-5.
- [20] Guerbai, Y., Chibani, Y., &Hadjadji, B. (2015). The effective use of the one-class SVM classifier for handwritten signature verification based on writer-independent parameters. Pattern Recognition, 48(1), 103-113.
- [21] Gumusbas, D., &Yıldırım, T. (2019). Offline Signature Identification and Verification Using Capsule Network. 2019 IEEE International Symposium on INnovations in Intelligent SysTems and Applications (INISTA), 1-5.
- [22] Hanmandlu, M., Sronothara, A. B., &Vasikarla, S. (2018, November). Deep learning based offline signature verification. In 2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 732-737). IEEE.
- [23] Jagtap, A. B., Hegadi, R. S., & Santosh, K. C. (2019). Feature learning for offline handwritten signature verification using convolutional neural network. International Journal of Technology and Human Interaction (IJTHI), 15(4), 54-62.
- [24] Jagtap, A. B., Sawat, D. D., Hegadi, R. S., &Hegadi, R. S. (2020). Verification of genuine and forged offline signatures using Siamese Neural Network (SNN). Multimedia Tools and Applications, 79, 35109-35123.