Signature Verification Using Image Processing Techniques

Mr .C. Bhargav[1], B. Nasiruddin[2], S. Bharath Kumar[3], S Chandrasekhar[4], B. Parusuramudu[5]
[1]Assistant Professor, ECE Dept., St.Johns College of Engg. & Tech., Yemmiganur, Kurnool(Dist.), 518360, India
[2]Student, ECE Dept., St.Johns College of Engg. & Tech., Yemmiganur, Kurnool(Dist.), 518360, India
[3]Student, ECE Dept., St.Johns College of Engg. & Tech., Yemmiganur, Kurnool(Dist.), 518360, India
[4]Student, ECE Dept., St.Johns College of Engg. & Tech., Yemmiganur, Kurnool(Dist.), 518360, India
[5]Student, ECE Dept., St.Johns College of Engg. & Tech., Yemmiganur, Kurnool(Dist.), 518360, India
Email ID:bargauv@gmail.com

Abstract

Every person has his/her own unique signature that is used mainly for the purposes of personal identification and verification of important documents or legal transactions. There are two kinds of signature verification: static and dynamic. Static(off-line) verification is the process of verifying an electronic or document signature after it has been made, while dynamic(on-line) verification takes place as a person creates his/her signature on a digital tablet or a similar device. Offline signature verification is not efficient and slow for a large number of documents. To overcome the drawbacks of offline signature verification, we have seen a growth in online biometric personal verification such as fingerprints, eye scan etc. In this paper we created CNN model using python for offline signature and after training and validating, the accuracy of testing was 99.70%.

Keywords: Signature Verification, Pre-processing, Feature extraction, Authentication, Matching techniques, CNN, Neural Networks

1. INTRODUCTION

Signature has been a distinguishing feature for person identification through ages.

Signatures for long have been used for automatic clearing of cheques in the banking industry. When a large number of documents,

e.g., bank cheques, have to be authenticated in a limited time, the manual verification of account holders'

signatures is often unrealistic. Signature provides secure means of authentication and authorization. So, there is a need of Automatic Signature Verification and Identification system. The present dissertation work is done in the field of online signature verification system by extracting some special feature that makes a signature difficult to forge. In this dissertation work, existing signature verification system has been thoroughly studied and a model is designed to develop an offline signature verification system,

The handwritten signature is a particularly important type of biometric trait, mainly due to its ubiquitous use to verify a person's identity in legal, financial and administrative areas. One of the reasons for its widespread use is that the process to collect handwritten signatures is non- invasive, and people are familiar with the use of signatures in their daily life.

Approaches to signature verification fall into Literature Survey

There are several surveys conducted on the handwritten signature verification systems and the methodologies used. Several approaches have been recently proposed and lot of research has been carried out for both feature extraction and classification using HMM, SVM, FFT, MLP wavelets and NN [4][5]. Several matching strategies employed in signature analysis are holistic matching, regional matching and multiple regional matching. Some of the most diffuse techniques reported are Euclidean distance, Elastic matching, regional correlation, tree matching, relaxation matching, split and merge, string matching, NN, HMM, SVM

[2] [6]. Theissues and challenges faced by signature verification system are discussedin the survey reports[1] [3].

1.1 Problem Statement

Online (dynamic) signature verification uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addition to its shape. Dynamic features include the number and order of the strokes, the overall speed of the signature, the pen pressure at each point, etc. and make the signature more unique and more difficult to forger.

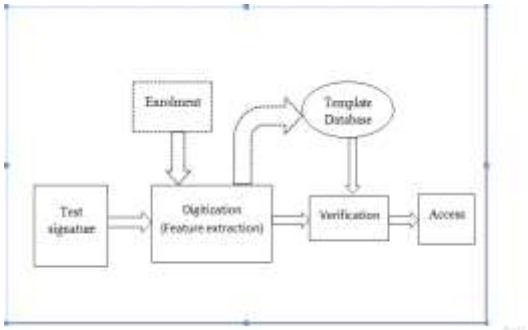


Figure 1: Typical Signature Verification System

In an online signature verification system figure 1, the users are first enrolled by providing signature samples (reference signatures). When a user presents a signature (test signature) claiming to be an individual, this test signature is compared with the reference signatures for that individual. If the dissimilarity is above a certain threshold, the user is rejected. During verification, the test signature is compared to all the signatures in the reference set, resulting in several distance values. One must choose a method to combine these distance values into a single value representingthe dissimilarity of the test signature to the reference set, and compare it to a threshold to decide. The single dissimilarity value can be obtained from the minimum, maximum or the average of all the distance values. Typically, a verification system chooses one of these and discards the others. In evaluating the performance of a signature verification system, there are two important factors: the FRR of genuine signatures and the FAR of forgery signatures. As these two errors are inversely related, the EER where FAR equals FRR is often reported .

To determine whether signature is genuine or forgery a new approach is proposed in dealing with the online signature verification a combination of two methods GMM and LCSS using publicly available signature database i.e., MCYT-100. Firstly, the signature is normalized and the parameters of the GMM are estimated by the Maximum Likelihood method. The Maximum likelihood method estimation technique finds the parameters that maximize the joint likelihood of the data which are supposed to be independent and identically distributed. In the Gaussian mixture, it captures the underlying statistical variability's of the point based features, being used for describing the online trace of the signatures. Then LCSS detection algorithm which measures the similarity of signature time series. A threshold value is set and a decision is made comparing the test signature values with the database signature values whether the signature is genuine or forgery. To evaluate LCSS performance, it is compared with the most widely used technique called DTW.

1.2 Approaches:

Signature Image Acquisition:

Signature image is acquired using digital image scanner device. In computing, an image scanner—often abbreviated to just scanner—is a device that optically scans images, printed text, handwriting, or an object, and converts it to a digital image. Common examples found in offices are variations of the desktop (or flatbed) scanner where the document is placed on a glass window for scanning. Hand-held scanners, where the device is moved by hand, have evolved from text scanning ―wands‖ to 3D scanners used for industrial design, reverse engineering, test and measurement, orthotics, gaming and other applications. Mechanically driven scanners that move the document are typically used for large-format documents, where a flatbed design would be impractical.

The acquired signature image is now brought under some image pre-processing operations in order to enhance, thinning and binarization of the image. Finally, the signature image is obtainedin true binary form with white as back ground and black as signature ink impression.

Background:

Online hand written signature verification is a process of testing whether a signature is genuine or forgery. A signature can easily be forged. Forgeries of signatures are classified into three types.

ALGORITHM Input:

signature from a database Output: verified signature classified as genuine or forged

1. Retrieval of signature image from a database.
2. Pre-processing the signatures.
3. Converting image to binary.
4. Image resizing.
5. Thinning.
6. Finding bounding box of the signature.
7. Feature extraction
8. Maximum horizontal and vertical histogram
9. Centre of mass
10. Normalized area of signature
11. Aspect ratio
12. The tri surface feature
13. The six fold surface feature
14. Transition feature
15. Creation of feature vector by combining extracted features.
16. Normalizing a feature vector.
17. Training a neural network with a normalized feature vector.
18. Steps 1 to 17 are repeated for testing signatures.
19. Applying normalized feature vector of test signature to trained neural network.
20. Using a result generated by the output neuron of the neural network declaring a signature asa genuine or forged.

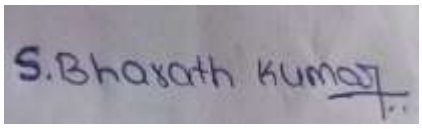
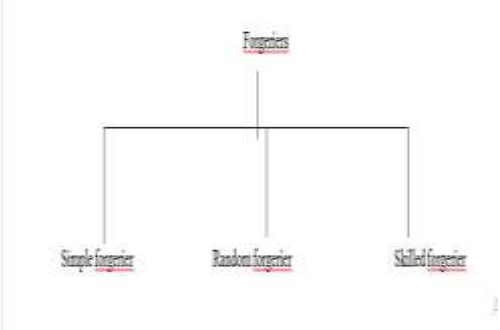


Figure : Signature Image from the database

Fig. shows one of the original signature image taken from a database and all the subsequent figures show the resultant signature image obtained after performing the steps mentioned in an algorithm.

The pre processing step is applied both in training and testing phases. Signatures are scanned in gray. The purpose in this phase is to make signature standard



and ready for feature extraction. The pre-processing stage improves quality of the image and makes it suitable for feature extraction. The prepossessing stage includes. A gray scale signature image is converted to binary to make feature extraction simpler. The signatures obtained from signatory are in different sizes so, to bring them in standard size, resizing is performed, which will bring the signatures to standard size 256*256 as shown in Fig. 3. Thinning makes the extracted features invariant to image characteristics like quality of pen and paper. Thinning means reducing binary objects or shapes to strokes that are single pixel wide. In the signature image, construct a rectangle encompassing the signature. This reduces the area of the signature to be used for further processing and saves time.

The choice of a powerful set of features is crucial in signature verification systems. The features that are extracted in this phase are used to create a feature vector. A feature vector of dimension 24 has been used to uniquely characterize a candidate signature. These features are extracted as follows:

A. Maximum horizontal and vertical histogram:

Horizontal histogram is calculated by going through each row of the signature image and counting number of black pixels. A row with maximum number of black pixels is recorded as maximum horizontal histogram. Similarly, a vertical histogram is calculated by going through each column of the signature image and finding a column with maximum number of black pixels.

B. Center of Mass:

Split the signature image in two equal parts and find center of mass for individual parts.

C. Normalized area of signature:

It is the ratio of area of signature image to the area of signature enclosed in a bounding box. Area of a signature is the number of pixels comprising it.

D. Aspect Ratio:

It is the ratio of width of signature image to the height of the image. This is done because width or height of person's signature may vary but its ratio approximately equal.

E. Tri surface feature:

Two different signatures may have same area .so; to increase the accuracy of the features three surface feature has been used.

F. The six fold surface feature:

Divide a signature in three equal parts and find bounding box for each part. Then calculate centre of mass for each part. Draw a horizontal line passing through centre of mass of each part and calculate area of signature above and below centre of mass within a bounding box. This provides sixfeatures.

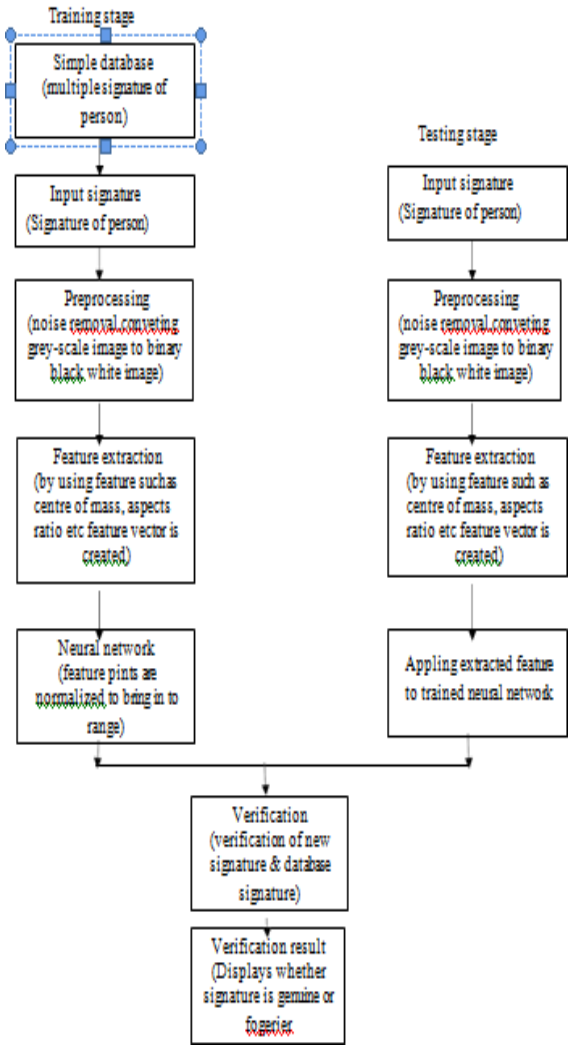
G. Transition feature: Traverse a signature image in left to right direction and each time there is a transition from 1 to 0 or 0 to 1, calculate a ratio between the position of transition and the width of image traversed and record it as a feature. Repeat a same process in right to left, top to bottom and bottom to top direction. Also calculate total number of 0 to 1 and 1 to 0 transitions. This provides ten features.

Signature Database:

The Biometric Research Laboratory, ATVS, of the Universidad Politécnica de Madrid,has promoted the plan of action and the development of the MCYT project, in which the design and acquisition of a large-scale bio-metric bi-modal database, involving fingerprint and signature traits, has been accomplished [17]. Although there are some other commercial and forensic partners within. In the case of the MCYT Signature sub corpus, 25 client signatures and 25 highly skilled forgeries (with natural dynamics) are obtained for everyone. Both on-line information (pen trajectory, pen pressure and pen azimuth=altitude) and off- line information (image of the written signature) are considered in the database.

Therefore, 330 × (25 + 25) =16500 signature samples are considered in the MCYT baseline on-line corpus. Since the acquisition of each on-line signature isaccomplished dynamically, a graphics tablet is needed: the acquisition device used is a WACOM pen tablet, model. The sampling frequency of the acquired signals is set to 100 Hz, considering the Nyquist sampling criterion, as the maximum frequencies of the underlying bio-mechanical movements arealways under 2030 Hz [17].

FLOW CHART



Preprocessing:

Preprocessing of online signatures is commonly done to remove variations that are thought to be irrelevant to the verificationperformance. Re-sampling, size, and rotation normalization are among the common preprocessing steps. In the preprocessing phase, the signature is undergone some enhancement process for extracting features. The signature images require some manipulation before the application of any recognition technique. This process prepares the image and improves its quality to eliminate irrelevant information and to enhance the selection of the important features for recognition and to improve the robustness of features to be extracted. Moreover, Preprocessing steps are performed to reduce noise in the input images, and to remove most of the variability of the handwriting [15].

For online signatures, some important preprocessing algorithms are filtering, noise reduction, and smoothing. They are also other preprocessing steps like the pen-up duration's, and drift and mean removal, time normalization and stroke concatenation before feature extraction.

To compare the spatial of a signature, time dependencies must be eliminated from the representation. Certain points in the signature such as the start points and the end points of a stroke and the points of a trajectory change, carry important information. These points are the critical points and are extracted and remained throughout the process [16].

Table : List of Common Features

List of Common Features	
S.NO	Description
1	Coordinate x(t)
2	Coordinate y(t)
3	Pressure p(t)
4	Time stamp
5	Absolute Position, $r(t)=\sqrt{p}\,x\,2\,(t)\ +\ y\,2\,(t)$
6	Velocity in x Vx(t)
7	Velocity in y Vy(t)
8	Absolute Velocity $v(t)=\sqrt{q}\,v\,2\,x\,(t)\ +\ v\,2\,y\,(t)$
9	Velocity of r(t) Vr(t)
10	Acceleration in x Ax(t)
11	Acceleration in y Ay(t)
12	Absolute Acceleration, $a(t)=\sqrt{p}\,x\,2\,(t)\ +\ y\,2\,(t)$

Feature Extraction:

Signature verification techniques employ various specifications of a signature.Selecting the features that are to be extracted has an enormous effect on the accuracy of the signature verification system. It is also the most difficult phase of signature verification system due to the different shapes of signatures and different situations of sampling. The feature extraction process represents a major tackle in any signature verification system. Even there is no guarantee that two genuine signatures of a person are accurately the same (intrapersonal variations). Its difficulty also stems from the fact that skilled forgeries follow the genuine pattern (interpersonal variations). This is unlikefingerprints or irises where fingerprints or irises from two different persons vary widely. Ideally interpersonal variationsshould be much more than the intrapersonal variations. Therefore it is very important to identify and extract those features which minimize intrapersonal variation and maximize interpersonal variations. Table 3.1 shows the list of common features. There isa lot of flexibility in the choice of features for verification of a signature extracting information from a signature is classified into two types:

1. Parameter Function based approach.
2. Function Feature based approach.

Parameter Function based approach:

Signature verification systems differ both in their feature selection and their decision methodologies. Features can be classified in

two types: global and local.

Global features are features related to the signature for instance the average signing speed, the signature bounding box, and Fourier descriptors of the signatures trajectory.

Local features correspond to a specific sample point along the trajectory of the signature. Examples of local features include distance and curvature change between successive points on the signature trajectory. Most commonly used online signature acquisition devices are pressure sensitive tablets capable of measuring forces exerted at the pen-tip, in addition to the coordinates of the pen. The pressure information at each point along the signature trajectory is another example of commonly used local feature. In some of these features are compared to find the more robust ones for signature verification purposes. Other systems have used genetic algorithms to findthe most useful features.

Function Feature based approach:

In Function feature based approach the signature is characterized in terms of a time function whose values constitute the feature set, such as position, velocity, pressure, etc.

NEURAL NETWORKS:

The main reasons for the widespread usage of neural networks (NNs) in pattern recognition are their power and ease of use. A simple approach is to firstly extract a feature set representing the signature (details like length, height, duration, etc.), with several samples from different signers. The second step is for the NN to learn the relationship between a signature and its class (either ―genuine‖ or ―forgery‖). Once this relationship has been learned, thenetwork can be presented with test signatures that can be classified as belonging to a particular signer. NNs therefore are highly suited to modeling global aspects of handwritten signatures. The proposed system in uses structure features from the signatures contour, modified direction feature and additional features like surface area, length skew and centroid feature in which a signature is divided into two halves and for each half a position of the centre of gravity is calculated in reference to the horizontal axis. For classification and verification two approaches are compared the Resilient Back propagation (RBP) neural network and Radial Basic Function(RBF) using a database of 2106 signatures containing 936 genuine and 1170 forgeries. These two classifiers register 91.21% and 88 % true verification respectively. In this paper we present a model in which neural network classifier is used for verification. Signatures from database are pre-processed prior to feature extraction. Features are extracted from preprocessed signature image. These extracted features are then used to train a neural network. In verification stage, on testsignatures pre-processing and feature extraction is performed. These extracted features are then applied as input to a trained neural network which will classify it as a genuine or forged signature.

Verification:

After applying the feature extraction process the test signature and the reference signature are compared with the minimum of the dissimilarities values,Average of all the dissimilarities and the maximum of all the dissimilarities. Choosing any of the above dissimilarity values the a decision is made whether it is a forgery signature or a genuine signature . this comparison is done using a threshold value for all the reference and test signature. if the value is approximately equal to the reference signal value then it is assumed to be a genuine signature and if the dissimilarities is above that threshold value the signature is rejected. This threshold value is can be identical to all the signature or it can also be different for each of them [15][16].

Verification:

After applying the feature extraction process the test signature and the reference signature are compared with the minimum of the dissimilarities values,Average of all the dissimilarities and the maximum of all the dissimilarities. Choosing any of the above dissimilarity values the a decision is made

whether it is a forgery signature or a genuinesignature . this comparison is done using a threshold value for all the reference and test signature. if the value is approximately equal to the reference signal value then it is assumed to be a genuine signature and if the dissimilarities is above that threshold value the signature is rejected. This threshold value is can be identical to all the signature or it can also be different for each of them [15][16].

2. BACKGROUND

Preprocessing:

The pre-processing stage improves quality of the image and makes it suitable for feature extraction. In this pre processing,we remove Noise and converting grey-scale image to binary black white image.

The Steps of Pre-Processing of the image from database is :

1. Cropping
2. Filtering
3. Conversion of Colour Image to Grayscale
4. Gray scale to binary Image
5. Resizing

1. CROPPING:

Cropping is a removal of unwanted outer area of a image. Image is a picture that has been created or copped and stored in electronic form.

2. Flitering:

Image filter is changing the appearance of an image by altering the colours of the pixels.

Once the histograms are passed through a low-pass digital filter, a filter is applied to remove unwanted areas from an image. In this case, the unwanted areas are the rows and columns with low histogram values. A low histogram value indicates that the part of image contains very little variations among neighboring pixels. Since a region with a license plate contains a plain background with alphanumeric charactersin it, the difference in the neighboring pixels, especially at the edges of characters and signature will be very high. This results in a high histogram value for such part ofan image

3. Conversion of colour image to gray scale:

The algorithm described here is independent of the type of colors in image and relies mainly on the gray level of an image for processing and extracting the required information. Color components like Red, Green and Blue value are not used throughout this algorithm. So, if the input image is a colored image represented by 3- dimensional array in MATLAB, it is converted to a 2-dimensional gray image before further processing.

5. Gray scale to binary image:

Image binarization is a process to convert an image to black and white. In this method, certain threshold is chosen to classify certain pixels as black and certain pixels as white. The main challenge is the assaigning of the threshold values for an image. Sometimes it becomes very difficult or impossible to select optimal thresholdvalue. This challenge can be overcome using the technique called Adaptive

Thresholding. A threshold can be selected by user manually or it can be selected by an algorithm automatically which is known as automatic thresholding.

6. Resizing

Image interpolation occurs when you re size or distort your image from one pixels grid to another.image resizing is necessary when you need to increase or decrease the total no of pixels.

Feature Extraction :

By using features such as centre of mass, aspect ratio etc feature vector is created. The following features are extracted from the processed image:

1. Normalised Signature Area

Total number of black signature pixels divided by total number of pixels of the image

2. Aspect Ratio

The Aspect ratio of the processed image = width/height

3. Maximum Horizontal Projection

It is the maximum number of black pixels among all horizontal rows of the image.

4. End Points

It is the number of endpoints of the signature.

1. Results and Discussions:

Final outputs of VNPR system:

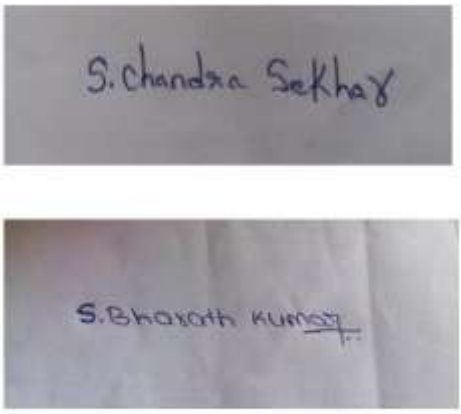
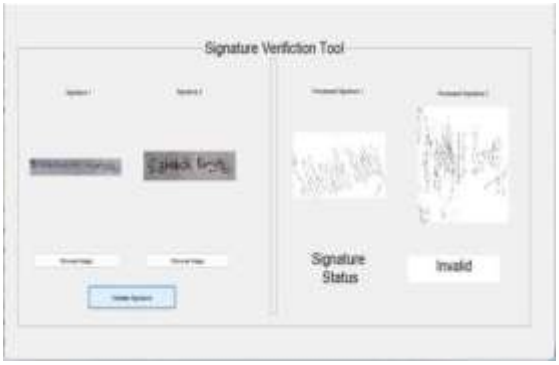


Fig: Input Images

The below images shows the input status of the signature verification usimg image processing techniques

The below figure shows one type of signature verification shows Valid signature because both signature 1 and signature 2 are same

The below figure shows third type of siggnature verification shows invaild Signature verification beacause second image is forgery bythe another person.



3. REFERENCES:

[1] D. Impedovo, G. Pirlo, and R. Plamondon, ―Handwritten signature verification: New advancements and open issues,‖ in 2012 International Conference on Frontiers in Handwriting Recognition, Sept 2012, pp. 367–372.

[2] H. Lei and V. Govindaraju, ―A comparative study on the consistency of features in on-line signature verification,‖ Pattern Recogn. Lett., vol. 26, no. 15, pp. 2483–2489, Nov. 2005.

[3] F. J. Zareen and S. Jabin, ―A comparative study of the recent trends in biometric signature verification,‖ in 2013 Sixth International Conference on Contemporary Computing (IC3), Aug 2013, pp. 354–358.

[4] G. Padmajadevi and K. S. Aprameya, ―A review of handwritten signature verification systems and methodologies,‖ in 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), March 2016, pp. 3896–3901.

[5] D. Morocho, J. Hernandez-Ortega, A. Morales, J. Fierrez, and J. OrtegaGarcia, ―On the evaluation of human ratings for signature recognition,‖ in 2016 IEEE International Carnahan Conference on Security Technology (ICCST), Oct 2016, pp. 1–5.

[6] R. Plamondon and S. N. Srihari, ―On-line and off-line handwriting recognition: A comprehensive survey,‖ IEEE Trans. Pattern Anal. Mach. Intell., vol. 22, no. 1, pp. 63–84,

Jan. 2000.

[7] M. M. Fahmy, ―Online handwritten signature verification system based on dwt features extraction and neural network classification,‖ Ain Shams Engineering Journal, vol. 1, no. 1, pp. 59 – 70, 2010.

[8] C. Gruber, T. Gruber, S. Krinninger, and B. Sick, ―Online signature verification with support vector machines based on lcss kernel functions,‖ IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), vol. 40, no. 4, pp. 1088–1100, Aug 2010.

[9] C. Gruber, T. Gruber, and B. Sick, Online Signature Verification with New Time Series Kernels for Support Vector Machines. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 500–508.

[10] A. Sharma and S. Sundaram, ―A novel online signature verification system based on gmm features in a dtw framework,‖ IEEE Transactions on Information Forensics and Security, vol. 12, no. 3, pp. 705–718, March 2017.

[11] M. Faundez-Zanuy, ―On-line signature recognition based on vq-dtw,‖ Pattern Recogn., vol. 40, no. 3, pp. 981–992, Mar.2007.

[12] B. Kar, P. K. Dutta, T. K. Basu, C. VielHauer, and J. Dittmann, ―Dtw based verification scheme of biometric signatures,‖ in 2006 IEEE International Conference on Industrial Technology, Dec 2006, pp. 381– 386.

[13] G. Zapata, J. D. Arias-Londoño, J. Vargas-Bonilla, and J. R. Orozco, ―Online signature verification using gaussian mixture models and small-sample learning strategies,‖ Revista Facultad de Ingeniería, vol. 2016, 06 2016.

[14] B. Drott and T. Hassan-Reza, ―On-line handwritten signature verification using machine learning techniques with a deep learning approach,‖ 2015, student Paper.

[15] S. Z. Li, Encyclopedia of Biometrics, 1st ed. Springer Publishing Company, Incorporated, 2009.

[16] A. K. Jain, A. Ross, and S. Prabhakar,―An introduction to biometric recognition,‖ IEEE Trans. Cir. and Sys. for Video Technol., vol. 14, no. 1, pp. 4–20, Jan. 2004.

[17] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. FaundezZanuy, V. Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero, and Q. I. Moro ―Mcyt baseline corpus: a bimodal biometric database,‖ IEE Proceedings - Vision, Image and Signal Processing, vol. 150, no. 6, pp. 395–401, Dec 2003.

[18] D. A. Reynolds and R. C. Rose, ―Robust text-independent speaker identification using gaussian mixture speaker models,‖ IEEE Transactions on Speech and Audio Processing, vol. 3, no. 1, pp. 72–83,Jan 1995.

[19] D. A. Reynolds, T. F. Quatieri, and R. B. Dunn, ―Speaker verification using adapted gaussian mixture models,‖ Digit. Signal