

# An Efficient Offline Handwritten Signature Verification Method Based on ODBTC Features

A.Mary Jerin <sup>#1</sup>, S. Palanikumar<sup>\*2</sup>, Resmi H B<sup>#3</sup>

<sup>#1</sup> M.Phil Computer Science & Software Engineering

Noorul Islam Centre for Higher Education

Thuckalay, Kumaracoil-629180

## Abstract

The most widely recognized secure personal biometric authentication is handwritten signature. Most organizations, primarily concentrate on the visual appearance of the handwritten signature for confirmation purposes. Many archives, for example, forms, contracts, bank cheques, and credit card transactions require the handwritten signature. Main challenging issues in the system is features are used for recognizing forged and genuine signatures. This article presents a technique for offline handwritten signature verification by exploiting the advantage of low-complexity ordered-dither block truncation coding (ODBTC) for the generation of image content descriptor and Local binary patterns (LBP). LBP was widely used as a robust illumination invariant feature descriptor. The system consists of pre-processing, feature vector extraction, training and classification or verification stage. In the pre-processing stage ODBTC compresses a signature image into corresponding quantizers and bitmap image. The Bit Pattern Features (BPF) is generated from ODBTC encoded data streams and LBP feature is extracted from input image. In the training stage a set of reference, signature images for each person is used. The mean vector of the set of feature vector is used for the verification purpose. The relative distance measure was used for classification. The proposed system is executed and tested utilizing GPDS database. The performance of the system is measured and experimental result shows convenience and viability of the proposed system.

**Keywords** - Signature Verification, Matching processes, ODBTC features LBP, BPF, and relative distance.

## I. INTRODUCTION

Signature is a feature to recognizing the identity of a person. Signatures are most common secure personal authentication in biometrics [1]. In the present society, signatures are utilized as a formal and an essential step in a document, In spite of an expanding number of electronics, other options for paper checks, fraud executed at financial institutions

in the United States has turned into a national epidemic. Since business financial institutions give cautious thought to confirm signatures on cheques essentially because of the number of cheques that are processed daily on a system which is equipped for screening easy going forgeries will prove useful. Most manufactured checks contain cheats of this compose.

Researches about in this field have been begun since 1970s and until now it is still quickly developing field to investigate and different strategies for different kinds of classification have been researched for this issue [2]. In any case, the majority of them are not extendable to various languages [3], because every language has their own particular qualities and different writing styles. One of the most serious issues that they experience to discover an autonomous -independent strategy is the features dissimilarity for various languages.

Signature is specific characteristics of biometric that is generally similar to handwriting and beneficial for individual verification [4], however, there are a few attributes that make it not quite the same as handwriting. For example the greater part of the signature styles are independent to the language of individual who sign, in some scenarios it just like an art comprise of curved shape lines even if it is blended with somehow name composing. This could be advantage and furthermore detriment for beginning an examination on new strategies for signature verification, and advantages it will help us to concentrate our research on algorithms which are in autonomous to language classification. It implies that we won't have any issue for various language signatures and can build the similarity of applications on this problem with no particular circumstance like different techniques. In any case, because of this trademark people don't take after correct guidelines in their signatures make it hard to find another strategy for extracting features from the signature that could be expandable to different languages.

In our project, we had tried to develop an efficient language independent signature verification framework that consequently verifies documents based on the owner's written by hand signature.

#### **A. Objectives**

The objectives of this study are:

1. To build an improved extracted features based on ordered-dither block truncation coding (ODBTC) and Symbolic Aggregate approXimation (SAX)
2. The feature extraction algorithm focus on the feature extracted from the different types signatures in the following situations
  - Noise in the image
  - Different orientation
  - Various writing
3. To verify and implement a whole accurate language independent offline signature verification system for skilled and random forgery detection.

This section will discuss the differences between the related work and the project presented in this report. Signatures are usually detected as a lawful means for confirming an individual recognizable proof by management and financial sectors. During the most recent couple of years, scientists have made great endeavours on signature verification. Signature verification consist of two type online and offline signature verification

## **II. RELATED WORK**

In [5] authentication of signature that is written by hand online with the help of a classifier that is neural subjected to the PCA (Principal Component Analysis) is developed. In this method, online signature authentication by the way of using multilayer perceptron (MLP) on the section of the features of PCA. PCA is used to analyse the signature time series signals to decrease the feature space dimensionality and extract new prominent features. The basic concept of PCA involves mapping multi-dimensional data distribution into a lower dimension with reduced loss of important information. It is achieved by projecting the raw data with high correlation between variables to a new space with uncorrelated variables. Then it performed a strategic feature by selecting some other elements in PCA computation such as latent and score. Finally, the obtained result from the feature extraction and selection stages is combined to represent the signature at the classification stage.

Engrafted system for verifying the signatures online in a biometric method is developed in [6]. This study depicts its usage on the Field-Programmable Gate Arrays (FPGAs) of an installed system used for verifying signs online. The pattern for recognizing includes three levels. First, an initial pre-processing is then applied to the input signature image, the input data contain noise in the preprocessing stage which is eliminated and also the information that is in the horizontal positions and vertical positions is normalized. Then, a pattern which is an active time wrapping is utilized to adjust this prepared sign with

its default type that is already been secured in a database. Finally, feature vector is then mined and proceed with the help of a Gaussian Mixture Model, which identify the similarity score between two signatures. The pattern was tried by utilizing an open database of 100 users, acquiring high detection rates for both genuine and forgery signatures. The developed system comprises of a Vector Floating-Point Unit (VFPU), particularly intended for accelerating the floating-point calculations engaged with this biometric methodology. Moreover, the architecture incorporates a microprocessor that communicates with the VFPU, and executes by using a application for the rest of the online process for confirming the signs. The designed framework is able completing the verification process with in 68ms at 40MHz clock rate authenticating the signatures online on mobile devices is introduced in [7]. This paper describes the system for verifying the signatures online for touch mobile devices. In this framework the set of features is extracted from a number of histogram that can be executed in a linear time. The histogram features are mined for the important attributes of the signature also the correlation between these features. During the enrolment process a user temple is generated. The feature set is extracted from the multiple signature from the user then the average of feature set is consumed for the process of authentication. The process is experimented on the MCYT-100 and SUSIG data sets. The structure for finger drawn signs on touch gadgets, a dataset were gathered from an unchecked domain and beyond various counsels. In the system the input data is converted to time series representation Cartesian coordinate vectors attributes and their derivatives. Afterwards the polar coordinate vectors are generated from the Cartesian coordinate vectors. At last histogram bins generated from the polar vector sequences.

In [8] authentication of signs online related to a represented feature is introduced. In online verification system facing difficulty in feature extraction step because of various shapes the signature and the input accessing from different environmental conditions. The features are varied in different situations. This paper develops strategy based on the feature learning process. The sparse auto encoder used for learn the signature features. The system is beginning with feature learning then classification. In classification stage, database of system has been developed utilizing classified represented data from reference signatures. These learning and database construction stage dine in section for system training. Eventually, at the authentication stage, which is the area for employing Framework, anonymous sign have been compared with that of in the system database to be checked. In the evaluating process, test signatures will be held back by comparing its properties with the signatures

taken as reference. SVC2004 Database has been exploited for this stage. SVS2004 database has two classifications named Task1 and Task2.

Authentication of online signatures subjected to neural network is developed in [9]. Online signature system combines two techniques which are the characteristic parameter technique and the characteristic function technique. The first one takes the major part of the signature data such as acceleration, speed, and pressure, and it depicts time function, and involves the functions characteristic value. The strategy is hard for analysing the stage, for the uneven continuous-time as well as the presence of lateral distortions, analysing is becoming a lot of difficult tasks, in this way they can enhance the cost, and also decreases the merits of low-cost sign authentication. Therefore the characteristic parameter technique can be made useful in this system. Despite the fact that the pressure sequence, the coordinate sequence, and other wave signal attributes were evaluated with a valuable process, yet just as in the exact notes for identifying these attributes were insufficient in generating a template for feature and adapt the recognition accuracy. The algorithm is developed using matlab software, the following characteristics is needed for implementation such as writing time, time of signature, with maximum speed for writing, average writing speed, time taken for the positive level of writing, time taken for the negative level of writing, time of positive vertical writing, time taken for negative vertical writing, the time taken for lifting a pen, first direction of normalization, the aggregate number of components of disruption, total Points, the time taken for the writing of all points and the time taken for writing, the ultimate vertical point that matches to the time taken for writing. The training and classification based on neural network.

A Comparison of Artificial Neural Network and K-Nearest Neighbour Classifiers in the Off-Line Sign authentication are proposed in [10]. For generating the feature, two totally variant descriptors are introduced to get property of the sign. The primary is that the Gaussian pyramid used for texture synthesis that is very redundant, coarse scales offer a lot of the data within the finer scales and Laplacian pyramid seamlessly stitch along images into an image plaid (i.e., register the photographs and blurring the boundary), by smoothing the boundary in a very scale-dependent style to avoid boundary artifacts. The second descriptor is that the canny edge detector accustomed detects wide selection of edges in image. Performance analysis is administrated on GPDS-100 dataset.

Online Signature Verification and Authentication using Smart Phones is developed in [11]. The system is designed to determine whether the person signing on any touch screen device is authenticated user or

not. This can be done by verifying his/her sign written by hand which is a socially agreed biometric feature for verifying a person. In this paper, a client (mobile) application which captures the user's signature and extracts various features like pressure, time and x-y co-ordinates and the server application verifies these features to find whether the signature has been done by an authenticated user or a forger is developed. The implementation is done using Python and the GUI is coded using X-code. The system consists of 3 phases. In Phase 1, User registration process user credentials is recorded, and along with the signature performed by the user in multiple conditions it is stored in the database. For signature storage, first the user is made to perform signature in multiple different conditions. Then, normalization is performed on the signatures, and this data is then stored in the database. In Phase 2, it consists of forgery prevention process in which we show user's signature to 5 professional forgers, each of which performs 5 forged signatures of the user's real signature. This data is then stored in the database. In Phase 3, it involves verification of signature in the login process. In this, user enters credentials and signature to verify. This signature is then compared with the real and forged signatures as secured in the collection. If the signature is verified as real, the user is logged in. The system is majorly implemented by using 2 algorithms, Relative Slope Algorithm and Hidden Markov Model.

In [12] Online Signature Verification by the help of Recurrent Neural Network and Length-normalized Path Signature is proposed. In this system, introduce a novel RNN system to develop the performance of online signature authentication. The training objective is to directly minimize intra-class variations and to push the distances between skilled forgeries and genuine samples above a given threshold. By back-propagating the training signals, our RNN network produced discriminative features with desired metrics. Additionally, the length-normalized path signature (LNPS) is introduced. LNPS has interesting properties, such as scale invariance and rotation invariance after linear combination, and shows promising results in online signature verification and SVC-2004 dataset is used.

In [13] Stable features are dynamically extracted in this method. In this model stability of information of spectral is evaluated. To mine more efficient spectral data, properties are downsized by using wavelet packet with the maximum mother wavelet. To boost the security range of online sign authentication, distinctive powers of fixed spectral properties are evaluated by factorial test style. The ideal property subspace is chosen in proportion to donation rate. Furthermore, a simple and efficient and modified dynamic time warping (DTW) with signature curves limited to solve the issue of high computation of DTW is introduced. So many tests are done on open

access collection of MCYT\_DB1 and SVC2004 task2 which includes 6600 signs from 140 people in total.

This section introduces the inspiration in utilizing the Ordered Dithered Block Truncation Coding (ODBTC) [14, 15], and its usability in creating representative image features. In this model, the bit pattern features (BPF) used. The primary merit in the use of the ODBTC image compression is on its low difficulty in creating a bitmap image by combining the Look-Up Table (LUT), and free of arithmetical operations on the decision of the two ultimate quantizers. ODBTC yields better reconstructed image quality by enjoying the extreme-value with doubling result that is compared to that of the typical BTC technique as reported in [1,27]. In the proposed technique is explained by establishing to create an image property descriptor from the ODBTC collection.

While numerous symbolic representations of time are presented in last years, they all experience from two fatal flaws. At first, the dimensionality of the symbolic representation is as same as the real data, and virtually all data mining algorithms scale poorly with dimensionality. In [16] unique representations in it allows dimensionality deduction, and it additionally allows to measure the length that has to be defined on the symbolic approach that lower the comparable length measures defined on the real series

Two of the image features that are combined for the proposed technique to specialize the contents of the image, i.e., Symbolic Aggregate approximation (SAX) and Bit Pattern Feature (BPF).

### **III. PROPOSED METHODOLOGY**

Signatures that are handwritten are considered as one of the most common medium for authenticating the identity of a person. Manual authentication of signs of a large number of documents is a time consuming work. Human signature provides a safe means for legal documents to get authorized and confirmed.

The most widely used identification method of an individual is the signatures that are written by that person. To verify and authenticate any official document, signatures that are handwritten are the most acceptable way. They are unique to each person which are easy to collect as it came as a result of spontaneous gesture.

- The chief purpose of this system is to verify the identity of individual related to his or her sign, through a process that differentiates a real signature from a fake one.
- The second goal of this system of verification is to classify the signs as skilled forgery signatures.

Nowadays in the field of pattern identification, verification of signs with the help of computers is getting more interest. Even though verifying the signs

is not a popular topic in image processing and in recognizing patterns, it plays an important role in other processes such as a security access control and contractual matters.

The proposed method includes two phases; they are Training and Testing. In the training level a set of reference signs are passed through the pre-processing, feature extraction, feature dataset creation, Classifier training. The testing phase includes four main steps of pre-processing, feature extraction, comparison of similarity values and the final decision. A brief detail about our proposed system is shown in Fig.1

For improving the accuracy of the feature extraction and also the verification, some of the essential procedures have to carry out to the sign image, before starting the extraction. For both the phases of training and testing, the step of pre-processing is found to be necessary. Smoothing is a process used to reduce the noise inside an image or to generate an image that is less pixelated. Here unsharp mask filtering used. The unsharp filter is a simple sharpening tool which enhances edges through a process which reduces an unsharp version of an image from the original image.

#### **A. Feature Extraction Techniques**

This step reduces the dimension of original sign images while retaining and mining the important details within the image. Carefully selected set of features will transform the images so that it becomes easier to differentiate between real and fake classes.

Our project will be on a feature mining algorithm which should not only be considered as challenging factors but also in recognize various types of forgeries. In the algorithm low-complexity, ODBTC and SAX are made use of. In this section small description about proposed optimized feature extraction algorithm.

In ODBTC it compresses an image block into bitmap image. The ODBTC scheme is a suitable way to list images in authentication process [1]. Time series is symbolically represented by SAX by transforming it into strings where a PAA based pattern is utilized for efficient dimensionality reduction. Since it require less space, it is utilized for resolving many challenging issues in the data gathering technique's [2]. In the proposed system BPF and SAX feature combined for efficient authentication method.

#### **B. Feature Extraction using ODBTC Method**

This features the contents of the image such as edges, shape. Fig. 2 shows the diagram for attaining the BPF. ODBTC is encoded using a codebook, which is generated with a set of training images. Let  $Q = \{Q1, Q2, \dots, Nb\}$  be the bit pattern codebook containing  $Nb$  binary code words. The bitmap is generated with the following criterion.



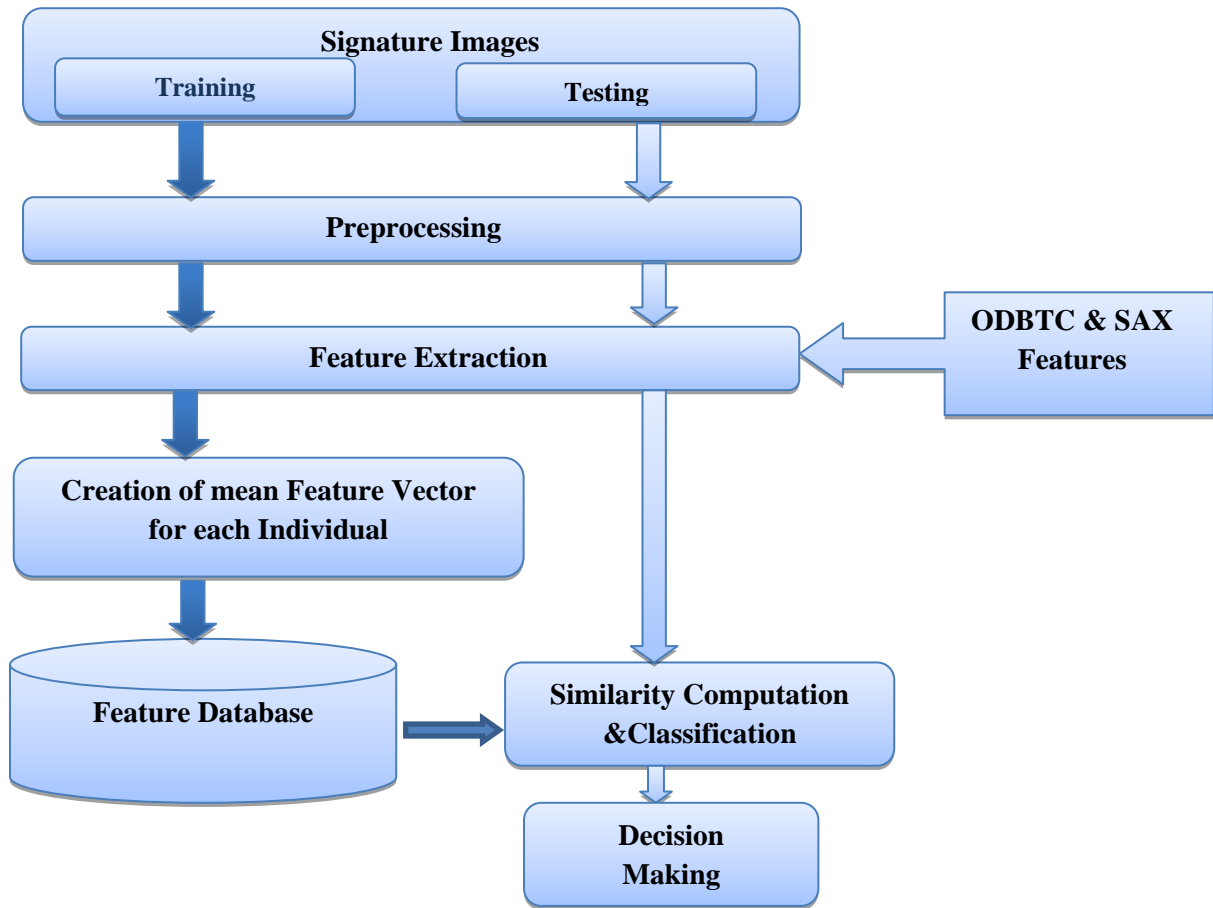


Fig. 1. Block Diagram Proposed System

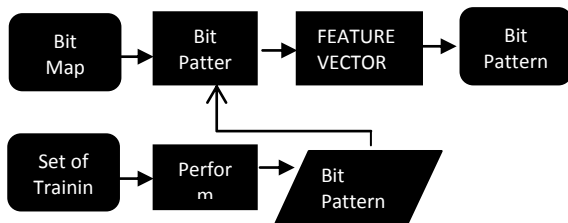


Fig.2. Schematic diagram for deriving the BPF

$$\tilde{b}(x, y) = \underset{q=1,2,\dots,N_b}{\operatorname{argmin}} \delta H\{bm(x, y), Qq\} \quad (1)$$

for all  $x = 1, 2, \dots, Mm$  and  $y = 1, 2, \dots, Nn$ .  
Thus, BPF is formally defined as

$$BP(t) = \Pr \{ \tilde{b}(x, y) = t | x = 1, 2, \dots, Mm ; y = 1, 2, \dots, Nn \}, \quad (2)$$

for all  $t = 1, 2, \dots, Nb$ .

The feature dimensionality of the BPF is similar to the codebook size. Fig. 3 explains the calculation of BPF on ODBTC image and a bit codebook. As same as that of CCF, BPF is made use for getting it adequate for the applications for which fast outcomes is needed.

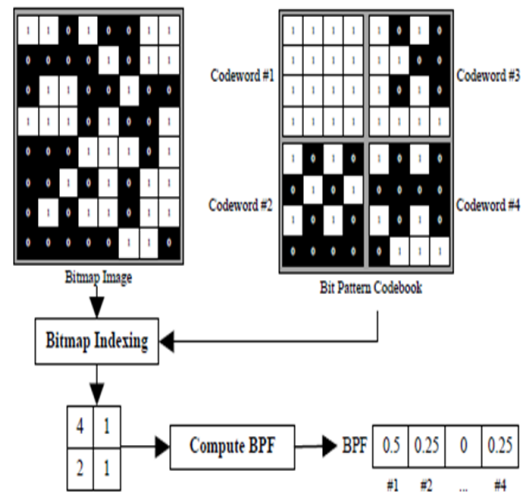


Fig. 3. Example of BPF computation.

### C. SAX Representation

It represents time series symbolically by converting the input data into strings where an algorithm based on PAA is utilized. This symbolic representation helps the researchers to go further to collect more data structures and algorithms for altering string in computer science.

The pattern includes two levels. Firstly, it converts time-series into a PAA algorithm ( $\bar{C}$ ) and then into alphabetic string ( $\hat{C}$ ) in the second step.

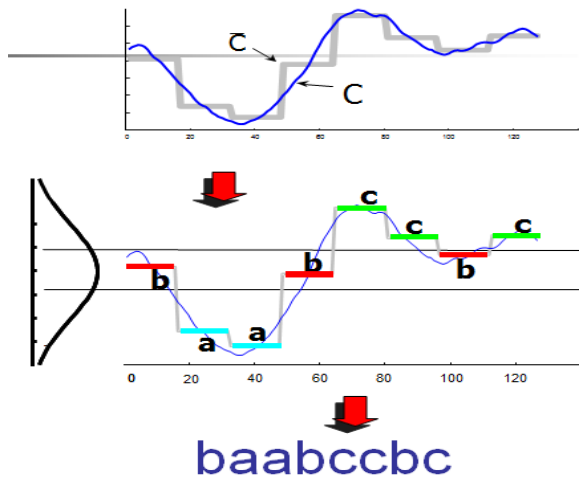


Fig.4.SAX representation (a) Time series, (b) PAA representation, (c) SAX string representation

Creating SAX from PAA illustration is executed by producing icons that related to the various magnitude of the same data. Fig. 4. (a) is the data that is real (b) shows the related PAA illustration and (c) depicts the SAX string illustration.

#### D. Similarity Score Calculation

The commonly used tools for calculating the distance between two vectors are City-block, Mahalanobis and Euclidean. As our proposed representation models is consisted of values and each of the signs have a feature that is a numerical value. In this system regarding similarity measure following formula is used

$$S(query, target) = \alpha_1 \sum_{t=1}^{N_c} \frac{|BPF^{query}(t) - BPF^{target}|}{|BPF^{query}(t) + BPF^{target}|} + \alpha_2 \sum_{t=1}^{N_c} \frac{|SAX^{query}(t) - SAX^{target}|}{|SAX^{query}(t) + SAX^{target}|} \quad (3)$$

Where  $\alpha_1$  and  $\alpha_2$  denote similarity weighting constants

#### E. Classification

In the proposed study, we classify the forgeries into skilled and random. When the feature vector of an image is submitted to the classifier, the feature vectors are partitioned into decision boundaries whose separating planes or hyper planes are determined by the sample patterns used for training. Each region of separation will be dominated by a particular signature. This work compares the performance and efficiency of LDA, Ensemble Ada boost (EAD) classifiers and Decision tree for the three handwritten signature classification.

A decision tree is a tool that uses a graph or model like tree of decisions and their possible consequences, including chances, events, and outcomes for making a proper decision.

EAD classifier is a particular method of training a classifier. It gives those features to improve the predictive power of the sample, reducing dimensionality and potentially enhancing execution time. Ensemble classifiers are multiple classifier algorithms and the outcome of the classification is the combined result of all the classification algorithms. Ensemble Ada boost classifier combines weak classifier algorithms into strong classifier. The algorithm is repeatedly trained by choosing the training set based on the accuracy of previous training. The weightage of each trained classifier at any iteration depends on the accuracy achieved. Each weak classifier is trained using random subset of the overall data set.

$$H(x) = \text{sign} \left( \sum_{t=1}^T \alpha_t h_t(x) \right) \quad (4)$$

$h_t(x)$ - Is the output of weak classifier  $t$  for input  $x$

$\alpha_t$  - Is the weight assigned to classifier

A weak classifier is trained and updated the weight for each training sample is updated as:

$$D_{t+1}(x) = \frac{D_t(i) \exp(-\alpha_t y_i h_t(x_i))}{z_t} \quad (5)$$

$D_t$  Is the weight at previous level,  $y_i$  is the parameter used for specifying coordinate.

The weights are normalised by dividing each of them by the sum of all the weights

LDA is made use of when the measurements made on independent variables for each observation are continuous quantities. For those applications in which there is no just to assume that the variables that are independent are usually scattered, this method is preferred. LDA uses Bayes approach for classification where the data set has been modelled as a set of multivariate normal distributions with a covariance matrix  $\Sigma$  but with different mean vectors  $\mu_k$  for  $k$  classes. In this work  $k$  has been assigned the value 9, there by assigning each input into any one of the 9 appropriate label. The estimates of  $\Sigma$  and  $\mu_k$  are used to compute the log ratios of the density of one class against another class.

## IV. IMPLEMENTATION

The software developed to offline handwritten signature verification and classification of proposed feature extraction algorithm BPF SAX representation. Intel(R) 2.10 GHz Core(TM) i3-2310M CPU, 4 GB RAM, and MATLAB software platform is used for implementation

#### A. Database Details and Evaluation Metrics

A bench mark offline sign dataset called GPDS300 [17, 18] is used for evaluating the proposed

verification model. The GPDS-140 was used for levelling the parameters of the introduced method for verifying the signs and GPDS-160 and BHSig260 were taken for testing. The GPDS-300 signature collection consists of 16200 offline sign images [18]. About 300 people were selected randomly for creating the collection. For every real signs, 30 faked signs from 10 various skilled forgers are collected. The sign images saved as binary images in bmp format with a resolution of 300DPI [18]. As we cannot acquire datasets for the study, we generated some real time forgery classification; random forged signatures datasets such as GPDS and ICDAR are used. Some test images based on different class is shown in Table I.

For evaluating the types of the rate, the errors are classified into two as metrics. These are False Rejection Rate (FRR) or False Non-Match Rate (FNMR), which means a real sign is treated as faked one and being aborted by the system, and second type of error is False Acceptance Rate (FAR) or False Match Rate (FMR), when a faked sign is treated as the real one and therefore accepted by the system. In Table II & Table III, both FAR and FRR are mathematically defined for further with the help of confusion matrix.

$$FRR = \left( \frac{FG}{GG+FG} \right) \quad (6)$$

$$FAR = \left( \frac{GF}{FF+GF} \right) \quad (7)$$

$$AER = \left( \frac{FAR+FRR}{2} \right) \quad (8)$$

In Table II and III, represents forged and *G* represent genuine signatures and *R* represent the random forged signatures, respectively. *GG* is used to represent the real signs. *FG* is the number of real signs that is treated as faked ones. *GF* is the number of faked signs, that considered as real ones and *FF* is the faked signs. *RR* is the randomly faked signs that are treated as random forged. *RF* is the random forged signs that is treated as forgeries. *RG* is the number of random forged signatures.

The *EER* and the *AER* have also been used for the evaluation of the system for authenticating signs. The *EER* indicates where the *FRR* and *FAR* are equal and *AER* is the average of *FAR* and *FRR* it calculated using equation (6) - (8). It may be noted that the *FAR*, *FRR*, *AER* and *EER* were evaluated considering that these classes are not balanced.

TABLE I : Dataset of Signature image



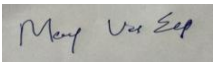





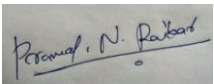





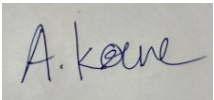


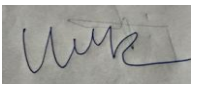








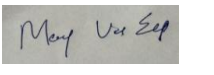


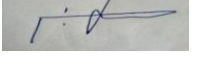
no	Genuine	Skilled Forgery	Random Forgery
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Table III: Confusion Matrix of Classification

True Label		Predicted Label	
		G	F
	G	GG	FG
	F	GF	FF

Table III: Confusion Matrix of Classification

True Label		Predicted Label		
		G	F	R
	G	GG	FG	RG
	F	GF	FF	RF
	R	GR	FR	RR

V. EXPERIMENTAL RESULTS

The figure 5 shows the intermediate results of genuine query image.

A. Performance Analysis of Signature Verification

Out of the 88 images tested, images turned out to be genuine, and the rest 33 images were forged ones. The feature vectors based on  $\alpha_1$  and  $\alpha_2$  are used for this. When  $\alpha_1 == 1$  and  $\alpha_2 == 0$ , then the feature vector is BPF, and when  $\alpha_2 == 1$  and  $\alpha_1 == 0$ , then the feature vector is SAX. And if both gives the value

of 1, then the feature vector that is used is the combination of both SAX and BPF. And it gives, the value for ACC as 96.59091 and AER as 6.666667 and FAR as 3.030303 and FRR as 3.636364. Table IV shows the FRR, FAR, AER, ACC values of different feature combination using result.

Table V shows the AER (%) Obtained By the Proposed Model Compared To Other Systems Using the GPDS-160 Dataset. From this table we can obtained that very less average error rate in the proposed method that is 06.6687% and also directional features vector has highest AER i.e.; 17.2553 %. Figure 6 show the pictorial representation the average error rate proposed system compared with existing features.

Performance analysis is different Feature Vector based on  $\alpha_1$  and  $\alpha_2$

- Total number of test images = 88
- Number of genuine images = 55
- Number of Forged images = 33

Performance analysis is different Feature Vector based on  $\alpha_1$  and  $\alpha_2$

If  $\alpha_1 == 1$ , feature vector is BPF

If  $\alpha_2 == 1$ , feature vector is SAX

If  $\alpha_1 == 1$  &&  $\alpha_2 == 1$ , feature vector is BPF\_SAX

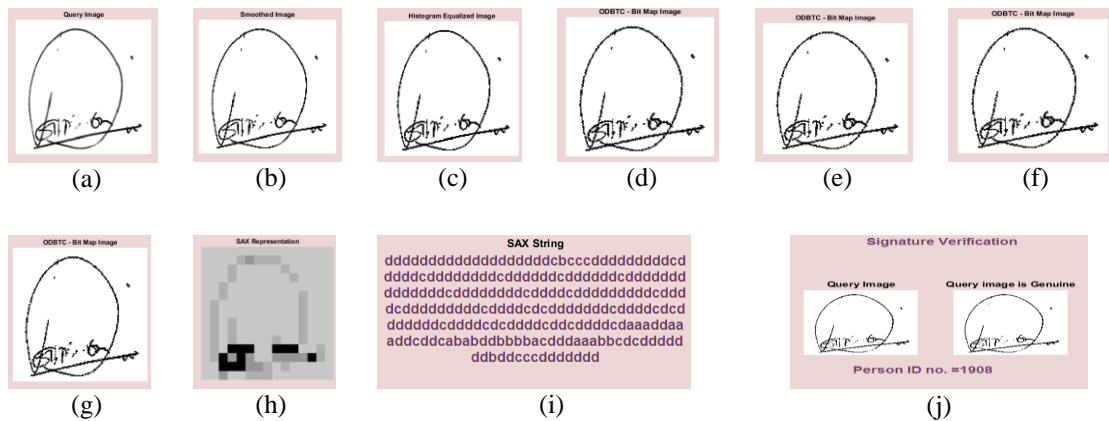


Fig. 5. Intermediate results of forgery query image.

Table IV: Performance analysis basis of different feature combination

Features	Predicted Label		Performance				
	G	F	FRR	FAR	AER	ACC	
SAX	G	52	3	5.454545	6.060606	11.51515	94.31818



	F	2	31				
BPF	G	50	3	5.660377	18.18182	23.8422	89.53488
	F	6	27				
BPF_SAX	G	53	2	3.636364	3.030303	6.666667	96.59091
	F	1	32				

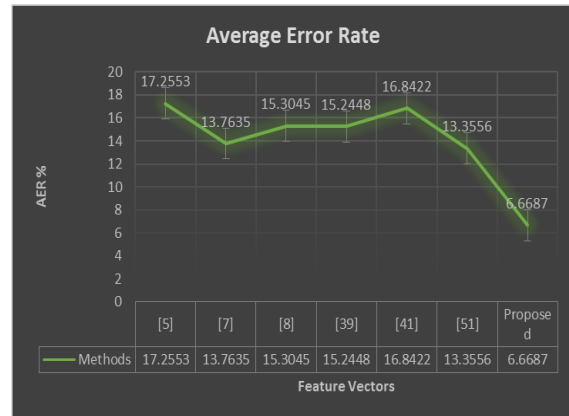
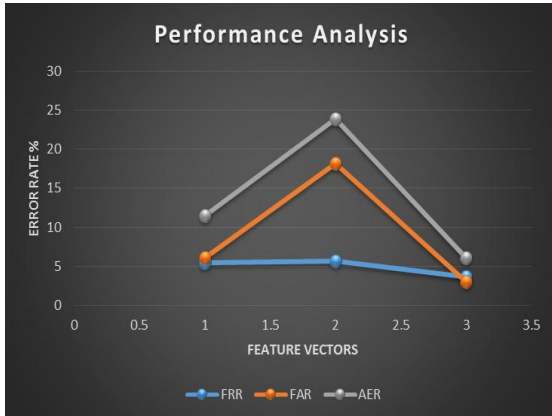


Fig. 6 (a) Graphical representation of performance analysis based on different feature combination (b) Comparison of proposed method with existing techniques based on AER

Table 4.5 Comparison of AER

	Feature Vector	AER %
[5]	Directional features	17.2553
[7]	Surroundedness	13.7635
[8]	Local descriptors	15.3045
[39]	Boosting Features	15.2448
[41]	Curvelet Transform	16.8422
[51]	Grid Segmentation	13.3556
<b>Proposed</b>	<b>BPF_SAX</b>	<b>06.6687</b>

**B. Performance Classification**

Table VI gives the amount of random forgeries detected in respect to the Genuine and forged signatures with the help of directional features. And that of in the table VII gives the value of RR as 32 when the system used the method of the feature surroundings. And as far the Table VIII is taken into consideration as it gives the value of 32 for RR and 0 for RG, RF, and GR.

On the other hand Table X shows the result of using all the three classifiers that are adaboost, LDA and decision tree. Accuracy of the classification system is calculated using equation (2). As per the result obtained, adaboost gives the values as 96.72131 and LDA gives the result as 90.16393 and the result obtained by decision tree is 83.60656. The ROC curve of the BPF SAX feature with different classifiers is shown in Figure 6 (d). Figure 6 (a) shows the roc curve of the decision tree classifier based on different class. Figure 6 (b) shows the roc curve of the linear discriminant analysis classifier

based on different class. . Figure 6 (c) shows the roc curve of the adaboost classifier based on different class.

$$Acc\% = \frac{GG+FF+RR}{GG+GF+GR+FF+FR+FG+RF+RG+RR} \times 100$$

Table VI: Decision Classifier

Dec	G	F	R
G	50	5	0
F	9	24	0
R	0	6	28

Table VII: Decision Classifier

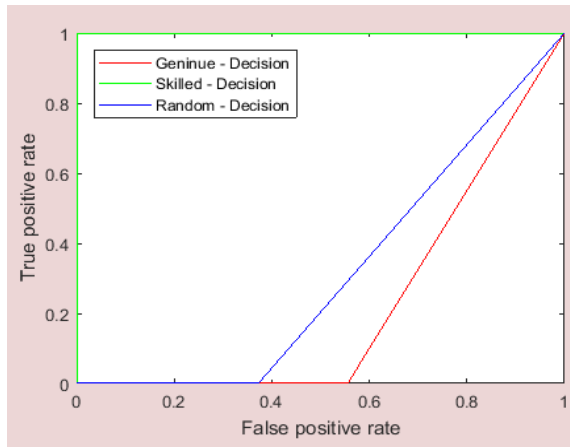
LDA	G	F	R
G	52	3	0
F	4	29	0
R	0	2	32

Table VIII: AdaBoost Classifier

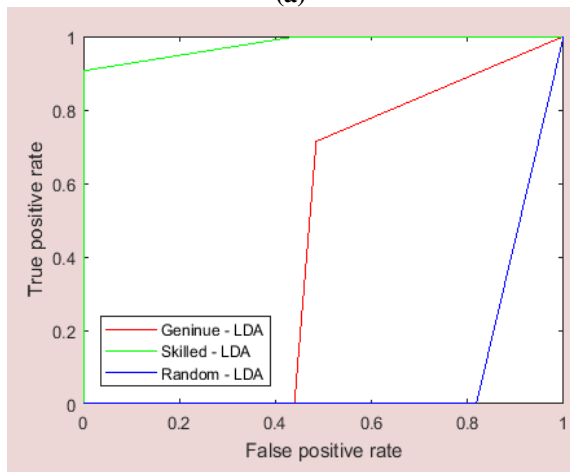
Ada	G	F	R
G	54	1	0
F	1	32	0
R	0	2	32

Table X: classifier Comparison

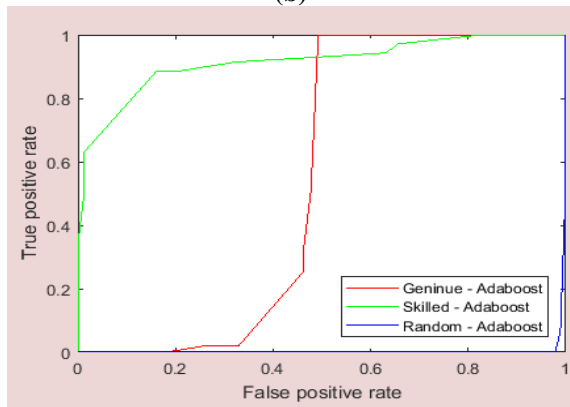
Classifiers	T	TP	FP	ACC
Adaboost	122	118	4	96.72131
LDA	122	110	12	90.16393
Decision	122	102	20	83.60656



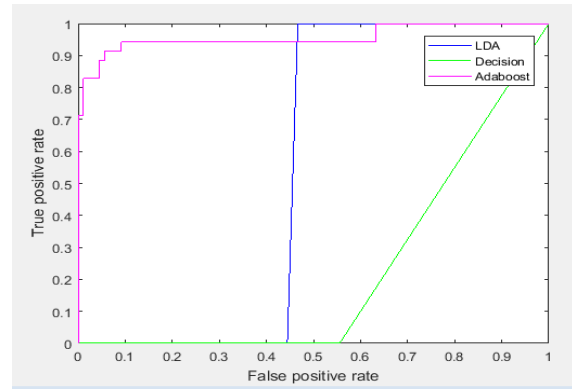
(a)



(b)



(c)



(d)

Fig. 6.(a) Roc curve of Decision tree classifier (b) Roc curve of Linear discriminant analysis classifier (c) Roc curve of Adaboost classifier (d) Roc Curve of comparison of different classifiers

### VI. CONCLUSION

In this study, automatic offline signature authentication and classification system related on BPF SAX representation model is presented. The feature vector in every signature class is created then stored in a database is used for classification verification method. A best similarity measure is later introduced to evaluate between a trained and the related BPX SAX model. Various types of three classifiers are practised, to perform classification. Ensemble adaboost classifier get better result for classification compare to other methods.

As quoted in the beginning, outcomes depends upon the collection of (GPDS-160), existence of skilled and random forgeries in training and testing. For an overall performance comparison, BPF SAX feature report the better result for comparison and adaboost classifier report the better result for classification. Even though the processes which utilize random skilled forgeries in practicing gives improved outcomes, they are not usable in real-life situations. The combination of both SAX and BPF. And it gives, the value for ACC as 96.59091 and AER as 6.666667 and FAR as 3.030303 and FRR as 3.636364 tested 55 genuine images and 33 skilled forged images. The performance of this method is evaluated with the help of the conducting a test for requested sign image with both skilled and random skilled forgeries on the GPDS-160 sign collection. A comparison is made between the attained outcomes with that of mentioned in the literature for the collection of GPDS.

The importance in authenticating the signs offline attains about 6.6 % EER, the achievement of these models are thought to be worse than the signs gathered in real situations. In the future, the further studies about this system need to aim on adding the robustness of the model regarding greater differences happened in real life and also generate language independent system. For example, sign

which are made in space that has been small, or in a hustle, or on papers with lines that are interfering. Some other issue is in working with few numbers as references as in many banking procedures, three references is used. For the future use, both simple and best method of normalization is preferred. Many problems like enforcement of security and score normalization, can be rectified with the help of evaluating the level of complexity in a sign.

## REFERENCES

- [1] Liu, Simon, and Mark Silverman. "A practical guide to biometric security technology." *IT Professional* 3.1 pp: 27-32, 2001
- [2] Yilmaz, M.B., Yanikoglu, B., Tirkaz, C. and Kholmatov, A., October. Offline signature verification using classifier combination of HOG and LBP features. In *Biometrics (IJCBI), International Joint Conference on IEEE*. (pp. 1-7). 2011
- [3] Zheng, Rong, et al. "A framework for authorship identification of online messages: Writing-style features and classification techniques." *Journal of the American society for information science and technology* 57.3, pp: 378-393, 2006.
- [4] Monrose, Fabian, and Aviel D. Rubin. "Keystroke dynamics as a biometric for authentication." *Future Generation computer systems* 16.4, pp: 351-359, 2000
- [5] Iranmanesh, V., Ahmad, S.M.S., Adnan, W.A.W., Yussof, S., Arigbabu, O.A. and Malallah, F.L., "Online handwritten signature verification using neural network classifier based on principal component analysis". *The Scientific World Journal*, 2014.
- [6] López-García, M., Ramos-Lara, R., Miguel-Hurtado, O. and Cantó-Navarro, E., "Embedded system for biometric online signature verification". *IEEE Transactions on industrial informatics*, 10(1), pp.491-501. 2014.
- [7] Sae-Bae, N. and Memon, N., "Online signature verification on mobile devices." *IEEE Transactions on Information Forensics and Security*, 9(6), pp.933-947, 2014.
- [8] Fayyaz, M., Saffar, M.H., Sabokrou, M., Hoseini, M. and Fathy, M., March. "Online signature verification based on feature representation". In *Artificial Intelligence and Signal Processing (AISP)*, 2015 International Symposium on IEEE. 2663-2676. pp. 211-216. 2015.
- [9] Xu, N., Guo, Y., Cheng, L., Wu, X. and Zhao, J., 2011, May. "A method for online signature verification based on neural network". In *Communication Software and Networks (ICCSN)*, IEEE 3rd International Conference on IEEE. pp. 357-360. 2011
- [10] Kaur, J. and Sharma, R., "A COMPARISON OF ARTIFICIAL NEURAL NETWORK AND K-NEAREST NEIGHBOR CLASSIFIERS IN THE OFF-LINESIGNATURE VERIFICATION". *International Journal*, 8(7). 2017.
- [11] Shah, H., Pawar, P., Khachane, M.S., Sharma, S. and Pithava, S., "Online Signature Verification and Authentication using Smart Phones". 2016
- [12] Lai, S., Jin, L. and Yang, W., "Online Signature Verification using Recurrent Neural Network and Length-normalized Path Signature". *arXiv preprint arXiv:1705.06849*. 2017.
- [13] Song, X., Xia, X. and Luan, F., "Online signature verification based on stable features extracted dynamically" *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 47(10), pp.2663-2676. 2017.
- [14] Guo, J.M. and Prasetyo, H., "Content-based image retrieval using features extracted from halftoning-based block truncation coding". *IEEE Transactions on image processing*, 24(3), pp.1010-1024. 2015.
- [15] Guo, J.M., "High efficiency ordered dither block truncation coding with dither array LUT and its scalable coding application". *Digital Signal Processing*, 20(1), pp.97-110. 2010.
- [16] Lin, J., Keogh, E., Wei, L. and Lonardi, S., "Experiencing SAX: a novel symbolic representation of time series". *Data Mining and knowledge discovery*, 15(2), pp.107-144. 2007.
- [17] Maini, R. and Aggarwal, H., "Study and comparison of various image edge detection techniques". *International journal of image processing (IJIP)*, 3(1), pp.1-11. 2009.
- [18] Vargas, J.F., Ferrer, M.A., Travieso, C.M. and Alonso, J.B. "Off-line signature verification based on grey level information using texture features". *Pattern Recognition*, 44(2), pp.375-385. 2011
- [19] Pal, S., Alireza, A., Pal, U. and Blumenstein, M., December. "Multi-script off-line signature identification. In *Hybrid Intelligent Systems (HIS)*", 2012 12th International Conference on . IEEE. pp. 236-240 2012.