Implementation of Offline signature verification based on LBP and LDP techniques on Beagle board-xM

Chandrashekara DR, Girish M, Manjunath P, Vinay Kumar KS, H C Sateesh Kumar

***Abstract*— The signature verification is used as a popular, cost effective authentication method and preferred among various biometrics as it is the widely accepted way to identify an individual .it is used in many areas of society related to automated banking transaction, electronic fund transfer, and document analysis and access control throughout the world. There are two categories in signature verification based on the acquisition of the signature viz. online and offline verification systems. Online systems use dynamic information of a signature captured at the time the signature is made. The off-line signature verification uses a static image of the signature collected from individuals on white paper. The off-line signature verification problem is more challenging than the on-line signature verification, because the features are extracted from the static 2D image of the signature.**

In this work, an offline signature verification method was proposed which is based on two sets of features extracted from the static signature image. First set of features consists of local binary pattern, the operator labels the pixels of an image by thresholding 3x3 neighborhood of each pixel with centre value and considering the results as a binary number of which the corresponding decimal number is used for labeling. The derived binary numbers are called local binary patterns or the LBP codes. While the LBP operator uses information of intensity changes around the pixels. The second set of features is local directional patterns operator use the edge response values of the neighbor pixels and encode the image texture. The LDP assign an 8 bit binary code to each pixel of an input image. Before the features are extracted, the signature is subjected to preprocessing which include extraction of exact size of the signature by resizing. Finally Euclidean distance is used as the classifier to decide whether the signature under test is genuine or forged. Parameters like FAR, FRR, EER and TSR were calculated.

***Index Terms*— Biometrics, Off-line Signature Verification, Local Binary Patterns, Local Directional Patterns**

Manuscript received May 15, 2015

Chandrashekara DR , Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Girish M, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Manjunath P , Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

Vinay Kumar KS , Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

H C Sateesh Kumar, Dept. of Telecommunication Engineering, Dayananda Sagar College of Engineering, Bangalore, India

I. INTRODUCTION

Nowadays, identification and verification is always needed in security and resource access control. The concerning method for recognition and confirmation is biometric approach. Biometric is a very important for identification or verification that is specific for individual person. Always human physical characteristics are carried along with person and cannot be forgotten. Handwritten signature is one of the most previous biometric approaches. Biometrics can be classified into two classes one is behavioral for example signature verification and another one is physiological for example iris, face, voice characteristics and thumb impression. Different techniques of recognition are outlined in the Figure 1.1

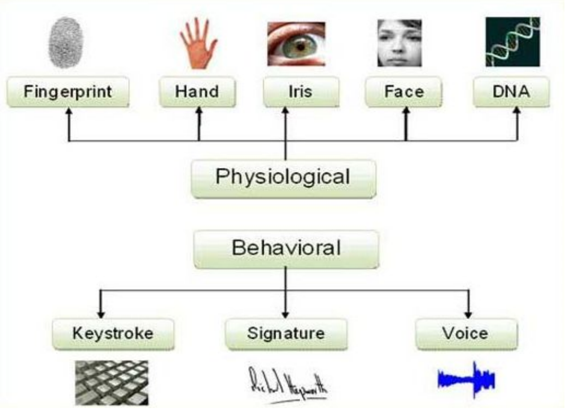


Figure 1.1 Samples of Biometric Recognition Techniques

Handwritten signatures takes a very special place in this wide set of biometric personalities. It is used for verifying the individual person. This is mainly due to the fact that handwriting signatures have long been based on the most far-flung means of personal verification. Signatures are generally recognized by administrative and financial institutions as a effectual means of verifying an individual's identity. Moreover, verification by signature analysis requires no offensive measurements and people are familiar with the use of signatures in daily life. A handwritten signature is the result of a composite process reckoning on the psychophysical state of the signer and the conditions under which the signing process occurs.

There are two major methods of signature verification. One is an off-line method that uses an optical electronic scanner to find handwriting data from a signature dropped a line on paper. The other, which is typically more fortunate, is an on-line method which, with a special device, measures the serial data, such as handwriting speed and pen pressure.

There are two main approaches for off-line signature verification: static approaches and pseudo dynamic approaches. The static one involves nonrepresentational measures of the signature while the pseudo-dynamic one tries to approximate dynamic information from the static image

Steps in Signature Recognition: Signature Recognition Systems motive to preprocess the data which includes a series of operations

Data Acquisition*:* The signatures to be refined by the system should be in the digital image format. We need to run down the signatures from the document for the verification use.

Signature Pre-processing*:* The signature pre-processing includes annealing the signature, resizing it to proper properties removing the background noise, and slimming the signature. The characteristics are extracted from the above pre-processed signature template. A typical scanned and Pre-Processed Signature is shown in Figure 1.2

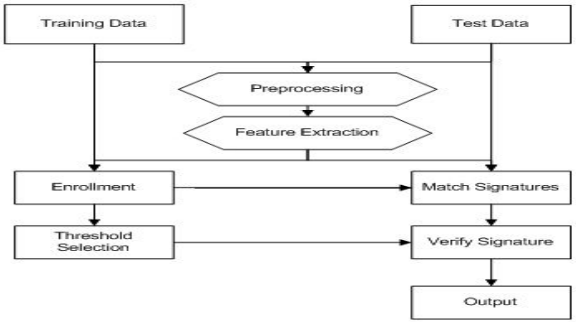


Fig 1.2. Flow chart for signature recognition algorithm

Feature Extraction*:* We are using various feature extraction algorithms. The feature set admits the conventional global features of signature as well as new features. The new features include gray level histogram, Local Binary Patterns (LBP) and Wavelet coefficients etc.

Enrollment & Training*:* The extracted features are stored in to database.. Our system should consider this version and at the same time the system should possess high degree of accuracy to detect faked signatures. We train the system using a training set of signature received from a person

Performance Evaluation: The performance of system depends on how accurately the system can classify between the genuine and fraud signatures. The forgeries involved in handwritten signatures have been categorized based on their characteristic features.

Levels of Forgeries: Various kinds of forgeries are classified into the following types:

Random Forgery: The signer makes a forgery in his own style by making use of the signature of the sign holder. This is known as random forgery. This forgery accounts for the majority of the forgery cases although they are very easy to detect even by the naked eye.

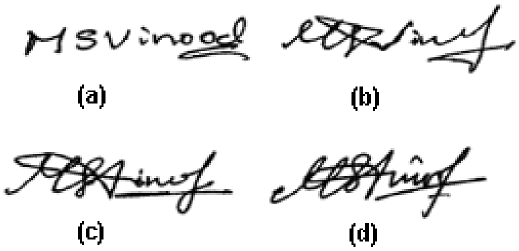


Fig 1.3Different types of forgeries (a) Original Signature (b) Random forgery (c) Unskilled forgery (d) Skilled forgery

Unskilled Forgery: The signer copies the signature in his own style without knowing the spelling. He does not have any prior experience of imitating the signature.

Skilled Forgery*:* The most difficult forgery of all forgeries is known as skilled forgery which is created by the professional impostors or persons who have experience in copying the signature. Figure 1.3 shows the different types of forgeries and how much they are varies from original signature.

Contribution: In this paper, we introduced local binary pattern and local directional pattern feature extraction techniques for the image. Which reduces FAR , FRR and increases TSR using Euclidean distances between the final feature coefficients of the test and database signatures.

Organization: The paper is organized into following section, section 2 is an overview of related work, section 3 describes the model of local binary pattern and local directional pattern feature extraction techniques, section 4 discusses the algorithm, section 5 describes the performance analysis of the model and conclusion is given in section 6.

II. Model

In this section we discussed definitions and LBP and LDP model.

A. Definitions:

i. Signature: Signature has been a distinguishing feature for person identification through ages. A signature is a handwritten depiction of someone's name, nickname or other mark that a person writes on a documents as a proof of identity and intent.

ii. Euclidean Distance: The Euclidean distance is the distance between two points in Euclidean space. The Euclidean distance is calculated via following equation 2.1

$$d(p,q) = \sqrt{(p_i - q_i)^2 + (p_j - q_j)^2} \text{ ------------------------(2.1)}$$

Where (p_i, p_j).The feature values of database image.

(q_i,q_j) - The features value of test image.

iii. False Rejection Rate: It is a measure of the biometric security system, that incorrectly reject an access attempt by an authorized user. A FRR is the Ratio of the number of false rejections to the total number of identification attempts is given by equation 2.2.

$$FRR = \frac{\text{Number of Persons falsely rejected}}{\text{Total Number of Persons in database}} \text{ --------------------(2.2)}$$

iv. False Acceptance Rate: It is the measure of the biometric security system that incorrectly accept an access attempt by unauthorized user. A FAR is the ratio of the number of false acceptance to the total number of identification attempts is given by the equation 2.3.

$$FAR = \frac{\text{Number of Persons falsely accepted}}{\text{Total Number of Persons outside database}} \text{-------(2.3)}$$

v. Total Success Rate: The number of test faces matched with the appropriate person accurately. A TSR is the ratio of correctly matched persons to the total number of persons in the database, and is given by equation 2.4.

$$TSR = \frac{\text{Number of Persons matched correctly}}{\text{Total Number of Persons in the database}} \text{---------(2.4)}$$

vi. Threshold/Decision Threshold: The acceptance or rejection of a data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the system can be made more or less strict; depending on the requirement of any given application.

B. Block diagram of LBP and LDP

The Figure 2.1 gives the block diagram of LBP and LDP

I. Signature Database: The GPDS300 signature database is considered. Signatures are obtained from persons on blank white paper at dissimilar timings depending upon the mood and stress levels and are scanned to get images of 96 dpi resolution in png format to create the database. The genuine signature is faked after ample training. The database consists of an appeal of twenty four genuine signature samples for three hundred persons. Each person consists of twenty four genuine signature samples and twenty seven forged signature samples

II. Preprocessing: For any signature verification technique before extracting the features some set of procedures should be performed in order to improve the character of the image. In the current process the considered operations were considering the exact signature field, Resizing manually earlier loading in to database..

Re-sizing : In order to standardize the inputs to the system all the pictures in the database are resized to a consistent size of 128 x 128. This operation is utilized on the image after extracting the demand size of image. The same size is also applied on the trial image

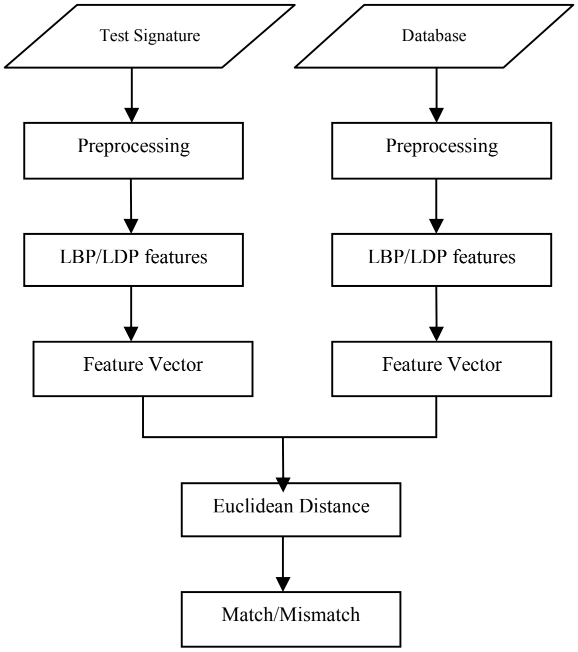


Fig 2.1: Block diagram of LBP/LDP

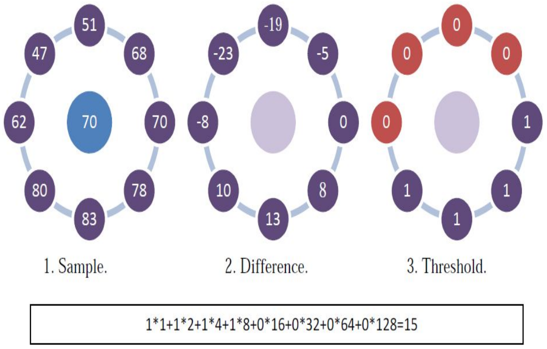
Feature Extraction: In the proposed work the feature extraction was done in two different phases. In the first phase the LBP coefficients were extracted. In the second phase the LDP coefficients were extracted. The process involved in extracting the two different features is explained as follows.

LOCAL BINARY PATTERN:

In the LBP, we compare the gray-scale value between the centre pixel and one of its neighbor pixels (interpolated pixels for more accurate result) to get the binary coding zero or one for the bit. We adjust the radius of this coding scheme as 1 and the number of neighbors as eight as non-remittal shape. We can get the local binary pattern (LBP) for the centre pixel after comparing all the 8 neighbors, which is 8-bit binary number shown as 01011110 or 11110000. Here, we can consider that the range of this form of LBP is from 0 to 255 if we convert the binary number to decimal number.

The value of the LBP code of a pixel (x_c, y_c) is given by

$$LBP_{P,R} = \sum_{p=0}^{P-1} s(g_p - g_c) * 2^P, \quad s(x) = \begin{cases} 1, if\ x \geq 0; \\ 0, otherwise. \end{cases} \text{---(2.5)}$$



1. Sample. 2. Difference. 3. Threshold.

4. Multiply by powers of two and sum

Local Directional Pattern features

LDP is a gray-scale texture pattern which qualifies the spacial structure of a local image grain. A LDP operator computes the edge reaction values in all eight directions at each picture element position and generates a code from the relative strength magnitude. Since the edge responses are more clarification and noise insensitive than chroma values, the resultant LDP feature describes the local primitives including different type of curves, corners, junctions; more stably and retains more information. Given a key pixel in the image, the eight directional edge response value $sm_i\{0,1,,\ldots.7\ \}$ are computed by Kirsch masks in eight different predilections centered on its attitude. The masks are shown in fig.2.2

$$\begin{bmatrix} -3 & -3 & 5 \\ -3 & 0 & 5 \\ -3 & -3 & 5 \end{bmatrix} \begin{bmatrix} -3 & 5 & 5 \\ -3 & 0 & 5 \\ -3 & -3 & -3 \end{bmatrix} \begin{bmatrix} 5 & 5 & 5 \\ -3 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix} \begin{bmatrix} 5 & 5 & -3 \\ 5 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix} \quad \textbf{East}$$

M_0 **North East** M_1 **North** M_2 **North West** M_3

$$\begin{bmatrix} 5 & -3 & -3 \\ 5 & 0 & 3 \\ 5 & -3 & -3 \end{bmatrix} \begin{bmatrix} -3 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & 5 & -3 \end{bmatrix} \begin{bmatrix} -3 & -3 & -3 \\ -3 & 0 & -3 \\ 5 & 5 & 5 \end{bmatrix} \begin{bmatrix} -3 & -3 & -3 \\ -3 & 0 & 5 \\ -3 & 5 & 5 \end{bmatrix}$$

West M_4 **South West** M_5 **South** M_6 **South East** M_7

Fig 2.2 Kirsch edge masks in all eight directions.

These eight edge replies magnitude are used to generate an eight bit binary number which can describe the local edge pattern of a special pixel. Different edge responses and the corresponding bit perspective is shown with the following figure 2.3

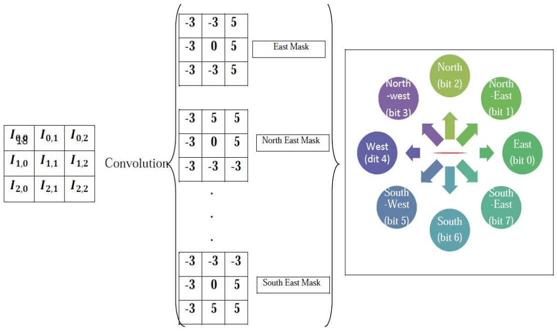


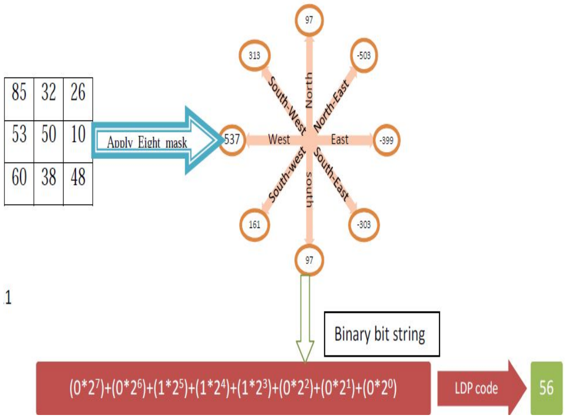
Fig 2.3 LDP binary bit positions

The response values are not equally important in all directions. The presence of corner or edge show high response values in some particular directions. Therefore, we are interested to know the k most prominent directions in order to generate the LDP.

Here, the top k directional bit responses are set to 1. The remaining (8-k) bits of 8-bit LDP pattern is set to 0. Finally, the LDP code is derived which is shown by an exemplary figure with k=3. After computing all the LDP code, the input image of size is represented by a LDP histogram which is LDP descriptor of that image.

$$LDP_k = \sum_{i=0}^{7} b_i(m_i - m_k) * 2^i, \quad b_i(x) = \begin{cases} 1, if\ x \geq 0; \\ 0, otherwise. \end{cases} \text{---(2.6)}$$

Where m_k is the kth most significant directional response.



IV. Matching/ Mismatching: Matching is biometric security system is the process of comparing biometric sample with a stored reference template and subsequently assigning a score based on level of similarity. Matching allows us to verify whether the person is in the database or not. For this, we make use of Euclidean distance. Test image is taken from the database and Euclidean distance is calculated by comparing the feature vector of one test image and feature vector all images in the database. Euclidean distance value and position of the image in the database for which Euclidean distance is minimum, is noted and used to calculate person number.

Euclidean distance value is compared with the threshold value. If the Euclidean distance value is less than the threshold, we have to check whether the person from the database and test image of a person is same. If it is same, then the match count is incremented. If it is not same, then the mismatch count is incremented. If the Euclidean distance value is greater than threshold then false rejection rate count is incremented indicating the image in database is falsely rejected. Likewise, The biometric system then issues are accept or reject decision based on the results of the matching.

Euclidean distance is used to verify whether the person is in database or not, by comparing final features vector set of database image with final feature vector set of test images.

The Euclidean distance is calculated via equation

$$d(p, q) = \sqrt{(p_i - q_i)^2 + (p_j - q_j)^2} \text{----------(2.7)}$$

Where (p_i, p_j) – The feature values of database image. (q_i, q_j) – The feature values of test image.

The range of Euclidean distances for all the comparisons of test signatures verses the database signatures were considered as threshold. Varying the threshold from minimum to maximum the performance parameters of the system were calculated.

The signature under test is considered to be matching when the Euclidean distance of that particular test image and the database image is less than the considered threshold value. If it is greater than the threshold value then the test signature is considered to be mismatched.

III. Algorithm

Problem definition: The method considered for offline signature verification in our work is explained in the Model. The GPDS 300 database is considered and preprocessed by extracting exact signature area, resizing, later the Local binary pattern and Local Directional patters features extracted.

The objectives:

1. Reduce FAR, FRR
2. Reduce EER
3. Increase TSR

The algorithm for signature verification in this work is shown in Table 3.1

```
INPUT:  Database signature images and Test signature images
OUTPUT: Match/Mismatch
STEPS:
    1. An arbitrary sized signature image from GPDS 300
       Database is taken as input.
    2. Image is resized manually to 128x128.
    3. The size of the image is extracted and converted into a
       matrix.
    4. LBP/LDP features are extracted from the matrix
    5. Steps 2 to 4 are repeated for the test image.
    6. The test image features are compared with database
       image features using Euclidean distance.
    7. Based on Euclidean distance Match or Mismatch count
       is evaluated by fixing a threshold.
    8. Varying threshold from minimum to maximum FAR,
       FRR, EER and TSR are calculated.
```

Table 3.1: Proposed Algorithm for LBP/LDP

IV. PERFORMANCE ANALYSIS

The performance parameters like FAR, FRR, EER, TSR are calculated using the Euclidean distances between the final feature coefficients of the test and database signatures.

The database is created by considering 10 persons from GPDS 300 with five genuine signatures per person, i.e., fifty signatures are available in the database. In the test section genuine signatures are considered to compute FRR and TSR. The forged signatures are considered in the test section to compute FAR. The values of FAR, FRR and TSR for ten persons are tabulated in table. As threshold value increases FAR and TSR increases, whereas FRR decreases.

Table 4.1 FAR, FRR, TSR for different thresholds calculated for 10 persons using LBP technique

Threshold	FRR	FAR	TSR
0.520000	1.000000	0.000000	0.000000
0.530000	0.800000	0.000000	20.000000
0.690000	0.700000	0.200000	30.000000
0.710000	0.400000	0.200000	50.000000
0.810000	0.200000	0.600000	60.000000
0.830000	0.000000	0.600000	60.000000

The value of EER is 0.3.The TSR at the optimum threshold of 0.71 is obtained as 0.5 or 50% and maximum TRS with 0.6 or 60%

Table 4.2 FAR, FRR, TSR for different thresholds calculated for 10 persons using LDP technique.

Threshold	FRR	FAR	TSR
0.440000	1.000000	0.000000	0.0000000
0.460000	0.800000	0.000000	20.000000
0.600000	0.700000	0.000000	30.000000
0.640000	0.600000	0.200000	40.000000
0.660000	0.400000	0.200000	50.000000
0.700000	0.300000	0.300000	60.000000
0.720000	0.200000	0.400000	70.000000
0.770000	0.100000	0.400000	80.000000
0.810000	0.000000	0.900000	80.000000

The value of EER is 0.3 .The TSR at the optimum threshold of .72 is obtained as 0.70 or 70% and the maximum TRS obtained is 0.80 or 80%.

Comparison with LBP and LDP results:

Method	TSR
LBP	60%
LBP	80%

Table 4.3 Comparison with LBP and LDP result

From the table 4.3 it can be observed that in the proposed models of LDP yields better EER and TSR when compared with the LBP technique previous methods.

CONCLUSION AND FUTURE WORK

An Off-line Signature Verification System (OSVS) has been described is developed using a feature set comprising the Local Binary Patters and Local Directional Patterns features of the image. The Local Binary Patter will differentiate the genuine and forged signatures of different persons using intensity values whereas the Local Directional Patterns features will differentiate the genuine and forged signature of the person using directional response (edge detection). The results have been tabulated and have been shown that LDP gives better EER and TSR when compared to LBP technique. In future the results are expected to be further improved with the use of neural networks or SVM (Support Vector Machines), PCA (Principal Component Analysis) in the place of Euclidean distance classifier.

REFERENCES

[1] VahidMalekian, AlirezaAghaei, MahdieRezaeian and Mahmood Alian “Rapid Off-line Signature Verification Based on Signature Envelope and Adaptive Density Partitioning”, *First Iranian Conference onPattern Recognition and Image Analysis (PRIA)*, pp. 1 – 6 : 2013.

[2] Vaibhav Shah, UmangSanghavi and Udit Shah “Off-line Signature Verification UsingCurve Fitting Algorithm with Neural Networks” *International Conference onAdvances in Technology and Engineering (ICATE)*, pp. 1 – 5 : 2013.

[3] Suhail M. Odeh and Manal Khalil “Off-line signature verification and recognition: NeuralNetwork Approach” *International Symposium on Innovations in Intelligent Systems and Applications (INISTA)*, pp. 34 – 38 : 2011.

[4] EfstathiosHadjidemetriou, Michael D. Grossberg andShree K. Nayar “Multiresolution Histograms and Their Use for Recognition” *IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE,* VOL. 26, NO. 7, pp. 831-847 : July 2004

[5] Mohamad HoseynSigari, Muhammad Reza Pourshahabi and Hamid Reza Pourreza “Offline Handwritten Signature Identification and Verification Using Multi-Resolution Gabor Wavelet”, *International Journal of Biometrics and Bioinformatics (IJBB)*, pp. 234-248, Volume (5): Issue (4) : 2011

[6] Kekre, H.B. and Bharadi, V.A “Signature Recognition using Cluster Based Global Features”, *Advance Computing Conference,.IACC 2009. IEEE International* , pp. 1323 – 1329 : 2009.

[7] H N Prakash and D S Guru, “Relative Orientations of Geometric Centroid for Off-line Signature Verification,” *International Conference on Advances in Pattern Recognition*, pp. 201-204, 2009.

[8] HaiRongLv, Wen Jun Yin, and Jin Dong, “Off-line Signature Verification Based on Deformable Grid Partition and Hidden Markov Models,” *IEEE International Conference on Multimedia and Expo*, pp. 374-377, 2009.

[9] Prashanth C R and K B Raja “Off-line Signature Verification based on Angular Features” International Conference on Computer Modeling and Simulation (ICCMS 2011) pp. 362-366: 2011