International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075, Volume-1, Issue-2, July 2012

Intra-modal Score level Fusion for Off-line Signature Verification

Prashanth C R, K B Raja, Venugopal K R, L M Patnaik

Abstract*— Signature is widely used as a means of personal verification which emphasizes the need for a signature verification system. Often the single signature feature may produce unacceptable error rates. In this paper, Intra-modal Score level Fusion for Off-line Signature Verification (ISFOSV) is proposed. The scanned signature image is skeletonized and exact signature area is obtained by preprocessing. In the first stage 60 centers of signature are extracted by horizontal and vertical splitting. In the second stage the 168 features are extracted in two phases. The phase one consists of dividing the signature into 128 blocks using the center of signature by counting the number of black pixels and the angular feature in each block is determined to generate 128 angular features. In the second phase the signature is divided into 40 blocks from each of the four corners of the signature to generate 40 angular features. Totally 168 angular features are extracted from phase one and two to verify the signature. The centers of signature are compared using correlation and the distance between the angular features of the genuine and test signatures is computed. The correlation matching score and distance matching score of the signature are fused to verify the authenticity. A mathematical model is proposed to further optimize the results. It is observed that the proposed model has better FAR, FRR and EER values compared to the existing algorithms.

***Index Terms*—Biometrics, Off-line Signature Verification, Image Splitting, Center of Signature, Angular Features, Correlation.**

I. INTRODUCTION

A wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services and to ensure that the services are accessed only by a legitimate user. Biometric recognition refers to the automatic authenticity verification of individuals based on their physiological and/or behavioral characteristics. The term Biometrics is derived from a Greek word and means *life measure*. Biometric measures based on physiological or behavioral characteristics are unique to an individual and have the ability to reliably distinguish between a genuine person and an imposter. Biometric traits increase the security by eliminating the traditional way of identifying a person using PIN, passwords and smart cards, which can be forgotten, stolen or lost [1].

Manuscript received on July, 2012.

Prashanth C R, Department of Electronics and Communication Engineering, Vemana Institute of Technology, Visvesvaraya Technological University, Bangalore, India

K B Raja, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India

Venugopal K R, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore, India.

L M Patnaik, Honorary Professor, Indian Institute of Science, Bangalore, India.

The biometric authentication of a person is based on physiological characteristics such as fingerprints, iris, face, palm print, DNA, retina or/and behavioral characteristics such as signatures, voice, body odor and gait [2]. Physiological characteristics are stable over life time of a person. Behavioral characteristics vary with time, mood and stress level of a person. The behavioral traits are acquired with cost effective equipments and are less threatening to users.

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 transfers, and document analysis and access control through out the world. The advantage of signature verification for identity authentication purpose is that most of the modern portable computers and personal digital assistants use handwritten inputs.

There are two categories in signature verification based on the acquisition of the signature viz., on-line and off-line verification systems [3]. The on-line signature verification uses pen and an E-pad to generate information about velocity, stroke order, acceleration, pen pressure etc. 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 [4], because the features are extracted from the static 2D image of the signature.

The difficulties in processing off-line signature are (i) the highly stylish and unconventional writing, (ii) the nature and variety of the writing pen (iii) the non-repetitive nature of variation of the signatures, because of age, illness, mood, stress levels, geographic location and perhaps to some extent the emotional state of the person. Considering these factors and to detect forgeries effectively, an efficient signature verification system has to be designed. The system should have an acceptable trade-off between a low False Acceptance Rate (FAR) and a low False Rejection Rate (FRR).

The generalized signature verification consists of four stages: signature acquisition, preprocessing, feature extraction and matching. The signature acquisition step captures the images of signatures. Preprocessing step involves removal of noise and skeletonization for making the acquired signature suitable for feature extraction. Then the preprocessed image is used to extract relevant features that can distinguish signatures of different persons.

The accuracy, efficiency, robustness, applicability and universality can be improved by biometric fusion. Researchers have shown that the use of biometric fusion provides better authentication performance. The different

levels of fusion are: (1) fusion at the feature extraction level, (2) fusion at the matching score level, (3) fusion at decision level [5].

Fusion at the feature extraction level: Two or more biometric features are used to get a feature vector. The features extracted are independent of each other and are concatenated into a single new vector. The redundant and irrelevant features are removed. From the reported a few researches on feature fusion, it is observed that feature fusion leads to dimensionality problems.

Fusion at matching score level: The matching score obtained from the system indicated the proximity of the feature vector with the template vector. The matching scores obtained from the systems are combined to authenticate the claimed identity.

Fusion at the decision level: The multiple biometric traits and the resulting features are used for classification. A majority vote scheme is used to make final decision.

Contribution: In this paper, we propose a technique for Intra-modal Score level Fusion for Signature Verification. The Discrete Wavelet Transform is used for enhancing the spatial domain features and to reduce noise. The features from skeleton of the signature are extracted in two stages. First stage is vertical and horizontal splitting to extract the center of signature. The second stage is extraction of angular features. Matching between the test image and the database image is done using correlation of center of signatures and distance matching of angular features. The correlation matching score and distance matching score are fused to verify the authenticity of the signature.

Organization of the paper: The rest of the paper is organized as follows. In section II, we discuss about related work. In section III we discuss about signature verification model. In section IV we present the ISFOSV algorithm. The performance analysis is presented in section V and concluded in section VI.

Motivation: The motivation behind the work is the growing need for a signature verification system which can guarantee the maximum possible security from forged signatures. The idea behind the work is also to ensure that the proposed ISFOSV system can provide comparable and better performance than existing off-line signature verification systems.

II. LITERATURE SURVEY

Manuel R. Freire et al., [6] proposed a model, which us auxiliary data that allows the matching with secure templates but do not provide information to a potential attacker. The performance of the proposed system is evaluated using the MCYT signature database comprising 330 users, within 25 genuine signatures and 25 skilled forgeries per user. The result shows similar performance compared to the baseline unprotected system. However the security of the proposed system against attacks to the template database is significantly higher.

Alonso-Fernandez et al., [7] proposed an effective method for off-line signature verification based on signature legibility and types. The process of initiation of signature depends on knowledge of letters, syllabus and name instances. Two machine experts were used one based on global image analysis and statistical distance measure and other one based on local image analysis and hidden markov model. The experimental results are obtained in terms of FAR, FRR, and EER.

Lucas Ballard et al., [8] proposed the steps towards developing the evaluation methodology for behavioral biometrics that take into account threat models that have been largely ignored. To overcome the current labor intensive hurdles in performing more accurate assessments of security system, the authors present a generative attack model based on contaminative synthesis that can provide a rapid indication of the security offered by the system.

Alessandro Zimmer and Lee L. Ling [9] proposed a method for hybrid handwritten signature verification. In this method, segmentation of the signature is done using vectorial delta-lognormal kinematic handwritten reproduction model. The data samples obtained from a digitizer are used to create prototype signature, which is saved in database. The distance between a pair of reference signatures is calculated as the total difference of direction of each individual stroke of the signature.

Banshider Majhi et al., [9] used geometric centre for feature extraction and Euclidean distance for classification. The threshold for comparison is selected based on stastical parameters like average and standard deviation. Nidal et al., [10] proposed dynamic signature verification system based on Singular Value Decomposition (SVD) to find singular vectors sensing the maximal energy of glove data matrix. These limited set of vectors are used to model the signature. The principal subspace of the reference signature is extracted and stored in database for verification. The angle between the different principal subspaces is used for signature verification.

Hannon Coetzer and Robert Sabourin [11] proposed a human centric off-line signature verification system in which they have investigated the feasibility of utilizing both human and machine classifiers for the purpose of signature verification in a banking environment. They proposed combined classifiers that perform better than human classifier and hidden markov model based classifiers. Hannon Coetzer and Robert Sabourin [12] proposed a human centric offline signature verification system in which they have investigated the feasibility of utilizing both human and machine classifiers for the purpose of signature verification in a banking environment. They proposed combined classifiers that perform better than human classifier and hidden markov model based classifiers.

Ramachandra et al., [13] proposed Robust Off-line Signature Verification based on Global Features for skilled and random forgeries. The model extracts the features which are preprocessed by normalization, binarization and thinning. The feature extraction technique consists of global features such as aspect ration, maximum horizontal histogram and maximum vertical histogram, horizontal and vertical centre of signature and signature area. Luiz S Oliveira et al., [14] proposed a writer independent model which reduces the pattern recognition problem to a 2-class problem. Receiver Operating Characteristic curves are used to improve the

performance of the system. The impacts of fusion strategies to combine the partial decisions are classified by SVM.

Taylan Das and Canan Dulger [15] proposed a technique based on Neural Network approach trained with particle swarm optimization algorithm using grid segmentation model. The image is scanned and noise is removed by normalization, area cutting, resampling, erode dialate and thinning. The algorithm verifies three types of forgeries i.e., random, skilled and unskilled.

Azzopardi and Camilleri [16] proposed Radial Basis Function Neural Networks for off-line Signature Verification. The signature database was collected using intrapersonal variations for evaluation. Global, grid and texture features are used as feature sets. The system is extensively tested with random forgeries and high recognition rates obtained demonstrate the effectiveness of the architecture.

Ghandali and Moghaddam [17] proposed a model based on Image Registration, Discrete Wavelet Transform and Image Fusion. Training signatures of each person are registered to overcome shift and scale problems. The several registered instances of each signature are fused together to generate reference pattern of signatures. In the classification phase Euclidean Distance is used.

Debasish Jena et al., [18] proposed an off-line signature verification system which is based on selecting 60 feature points. The classification of the feature points uses statistical parameters like mean and variance to identify skilled and unskilled forgeries. Prakash and Guru [19] proposed Relative Orientations of Geometric Centroids Off-line Signature Verification (ROGCOSV). The signature image is split into blocks to determine the centroids to form an interval valued symbolic features. The set of slopes representing the test signature are compared with corresponding slopes of the symbolic features stored in the database. Wan-Suck Lee et al., [20] described an off-line signature verification technique based on dynamic time warping. The signature verification is evaluated using neural network.

Prashanth et al., [21] presented a Standard Scores Correlation based Off-line Signature Verification (SSCOSV) System in which pixel density and geometric features points are extracted from a signature and compared using the concept of correlation. Bharadi and Kekre [22] explained off-line Signature Recognition Systems using normalization, noise removal and thinning of the signature. The features extracted include global features, Walsh coefficient of pixel distribution, codeword Histogram based on clustering technique, Grid features and Successive Geometric centers.

Prashanth et al., [23] proposed Off-line Signature Verification based on Angular Features. Angular features are obtained from the preprocessed image in two stages. The difference between angular features of genuine and test signatures is compared with threshold. Tirtharaj et al., [24] discussed neural network based associative memory net for off-line signature verification. The network is trained by testing samples and extracted features are compared against threshold for making decisions.

III. MODEL

In this section, definitions and block diagram of the Intra-modal Score level Fusion for Off-line Signature Verification (ISFOSV) are discussed.

A. Definitions

1) Signature: It is the handwritten depiction of a person's identity.

2) Random Forgery: The signature of an imposter having no knowledge about shape and structure of genuine signature [26].

3) Casual Forgery: It is a forgery signature produced with the knowledge about the genuine writer's name only.

4) Unskilled forgery: Signatures produced by inexperienced forgers without the knowledge of the spelling and shape of the genuine signature.

5) Skilled forgery: Forgeries which are produced by a professional imposter, who has experience in copying [26].

6) False Accept Rate (FAR): It is the total number of forgery signatures accepted by the system with respect to the total number of comparisons made.

$$FAR = \frac{NumberofForgerySignaturesaccepted}{TotalNumberofcomparisons}$$

7) False Rejection Rate (FRR): It is the total number of genuine signatures rejected by the system with respect to the total number of comparisons made.

$$FRR = \frac{NumberofGenuineSignaturesrejected}{TotalNumberofcomparisons}$$

8) Equal Error Rate (EER): It is the threshold value for which the FAR and FRR values are equal. A smaller EER indicates a better performance.

B. ISFOSV System

Figure 1 gives the block diagram of ISFOSV System, which verifies the authenticity of given signature of a person. The signature images for study are collected from the different subjects to create the database. The Discrete Wavelet Transform (DWT) is used for improving the spatial domain features of the signatures and to reduce the noise. Two types of features are extracted in two stages. The center of signature is obtained by vertical and horizontal splitting of signature to get 60 features. The 168 angular features are extracted by splitting the signature into 168 blocks in two phases. The center of signature is compared using correlation matching score and the distance in angular features is compared with threshold for verification.

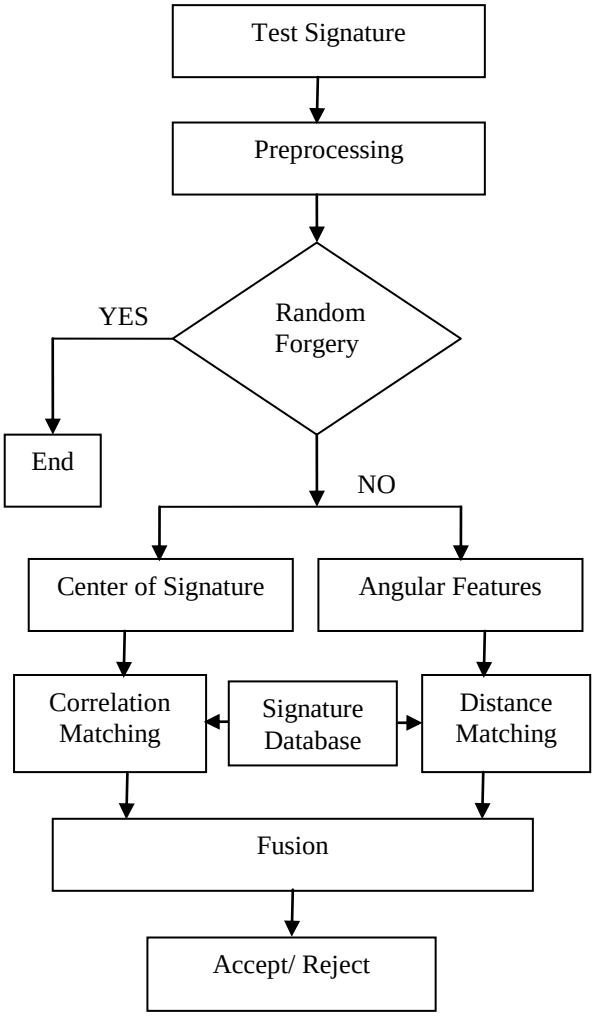


Figure 1. Block diagram of ISFOSV System

i) Signature Database

Signatures are obtained from persons on a blank white paper at different time instances depending upon the mood and stress levels and are scanned to get images of 96 dpi resolution in bmp format to create the database. The genuine signature is forged after sufficient training. A sample of genuine signature image is as shown in Figure 2.

Figure 2. Genuine signature

ii) Preprocessing

The signature is transformed to enhance image quality. It includes Discrete Wavelet transformation (DWT), Resizing, Skeletonization by morphological operations and considering the exact signature area.

a) Discrete Wavelet Transform

Dirt on camera or scanner lens, imperfections in the camera or scanner lens, imperfections in the scanner lighting, etc introduces noise in the scanned signature images. A filtering function is used for removal of the noise in the image. The DWT applied on signature images to preserve the pixel density in the signature image as compared to size normalization. Haar wavelet filter is used since its hardware implementation is cheaper than that of other filters. The Figure 3 shows the signature image after applying the DWT.

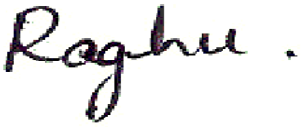


Figure 3. Signature after applying DWT

b) Resize

The images are resized to 150*450 instead of having signatures of different dimensions. Algorithm needs all the signatures to be of same size so that fair comparison is made among the signatures to produce better results.

c) Skeletonization

Reducing image to its single pixel width is skeletonization. A binary 2D object can be represented by its skeleton, which consists of the spines of the object parts. A 2D skeleton may consist of curves (spines), isolated 2D points and 2D surfaces. The generation of a skeleton is realized by applying an iterative process which erodes the object layer by layer until only the object spines remain, which form the skeleton of the 2D object. The skeletonization is done by removing the pixels on the boundary of the signature image without allowing the signature image to break apart. The process is achieved by morphological operations on signature image. The Figure 4 shows the signature after skeletonization.

Figure 4. Signature after skeletonization

d) Exact signature area

The signature image might not be present on the entire frame. So, the exact signature area is considered in the skeletonized image for further analysis. This reduces verification time and is cost effective. The signature image is scanned horizontally from top to get the first black pixel row *a1* of the image and is the value of the row variable i corresponding to first black pixel. The signature image is scanned from the bottom to get he last black pixel row *a2* of signature and is the value of the row variable i corresponding to last black pixel. The horizontal scanning for finding the top row and bottom row of the exact signature area is given by the Equations 1 and 2.

$$\sum_{i=1}^{M}\sum_{j=1}^{N} I_s(i,j) = 0 \quad \text{---- (1)}$$

$$\sum_{i=1}^{N}\sum_{j=1}^{M} I_s(N+(1-i),j) = 0 \quad \text{--- (2)}$$

The signature image is scanned vertically from left to get the first black pixel column *a3* of the image and is the value of the column variable j corresponding to first black pixel. The

signature image is scanned vertically from right to get the last black pixel column *a4* of the signature and is the value of the column variable j corresponding to last black pixel. The vertical scanning for finding exact signature area is given by the Equations 3 and 4. The Figure 5 shows the image with exact signature area.

$$\sum_{j=1}^{M}\sum_{i=1}^{N} I_s(i,j) = 0 \quad \text{--- (3)}$$

$$\sum_{j=1}^{M}\sum_{i=1}^{N} I_s(i, M+(1-j)) = 0 \text{ --- (4),}$$

where $I_s(x.y)$ is the skeletonized signature image.

Figure 5. Exact signature area

iii) Random Forgery Detection

To detect Random Forgery at the early stage, the number of rows r_i and columns c_i are obtained for all the ten genuine signatures using the equations 5 and 6. The average number of rows R_{avg} and columns C_{avg} are obtained using the equations 7 and 8.

$$r_i = a_{1i} - a_{2i} \quad \text{--- (5)}$$

$$c_i = a_{3i} - a_{4i} \quad \text{--- (6)}$$

$$R_{avg} = \frac{\sum_{i=1}^{N_{GS}} r_i}{N_{GS}} \quad \text{--- (7)}$$

where r_i is the number of rows representing the i^{th} signature and N_{GS} is the total number of genuine signatures.

$$C_{avg} = \frac{\sum_{j=1}^{N_{GS}} c_j}{N_{GS}} \quad \text{--- (8)}$$

where C_R is the number of columns representing the j^{th} signature and N_{GS} is the total number of genuine signatures.

The number of rows and columns of test signature are calculated and compared with R_{avg} and C_{avg} respectively. If the absolute value of the difference between R_{avg} and number of rows R_{Ti} representing the test signature is less than or equal to predefined threshold value and if the absolute value of the difference between C_{avg} and number of columns C_{Ti} representing the test signature is less than or equal to predefined threshold, then the angular feature extraction and verification are carried out on the test signature else random forgery is detected and verification process is aborted.

iv) Feature Extraction

The two sets of features are extracted in two stages. In stage one, the signature image is split vertically and horizontally get total 60 centers of signature. In the second stage, the signature is divided into 168 blocks in two phases to obtain 168 angular features.

1) *Center of Signature*

The two sets of feature points are extracted in two-dimensional plane from the signature image obtained by skeletonization. Vertical Splitting and Horizontal Splitting are two main steps to retrieve these feature points. Each set has thirty feature points which represent the stroke distribution of signature pixels in image. These sixty feature points are found using geometric center. The vertical splitting of the image results thirty feature points (*v1, v2, v3... v30*) and the horizontal splitting results thirty feature points (*h1, h2, h3… h30*). These feature points are obtained with relative to a central geometric point of the image.

The skeleton of the signature image is scanned from left to right for calculating the total number of black pixels. Again it is scanned from top to bottom to calculate the total number of black pixels. Then the image is divided into two halves with respect to the number of black pixels by two lines vertically and horizontally which intersects at a point called the geometric centre. With reference to this point, we extracted 60 feature points: 30 vertical and 30 horizontal feature points of each signature image.

a. Feature Points based on Vertical Splitting

Thirty feature points are extracted based on vertical splitting. The feature points are nothing but the geometric centers. The procedure for finding feature points by vertical splitting is explained as follows.

The signature image is split with vertical line passing through geometric center of image to get left and right parts of image. This geometric centre is obtained by locating a point where number of black pixels is half of the total number of black pixels in the signature. Geometric centers *v*1 and *v*2 are found for left and right parts respectively. The left part is split with a horizontal line at *v*1 to find the geometric centers *v*3 and *v*4 for top and bottom parts of left part correspondingly. Similarly, the right part is split with a horizontal line at *v*2 to find the geometric centers *v*5 and *v*6 for top and bottom parts of right part correspondingly. Each part of the image is again split through their geometric centers to obtain feature points *v7, v8, v9… v13, v14*. Then, each part is again split through their geometric centers to obtain thirty vertical feature points as shown in Figure 6.

b. Feature Points based on Horizontal Splitting

Thirty feature points are extracted based on horizontal splitting. The procedure for finding the feature points by horizontal splitting is explained below.

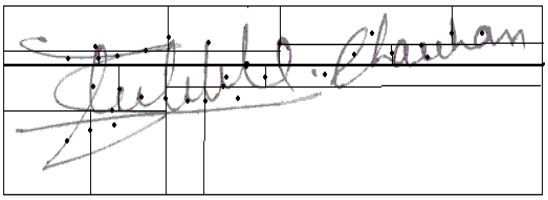


Figure 6. Vertical splitting of the signature

As explained for vertical splitting, the signature image is split with horizontal line passing through the geometric centre

to get top and bottom parts of image. The geometric centre is obtained by locating a point where number of black pixels is half of the total number of black pixels in the signature. Geometric centers *h*1 and *h*2 are found for top and bottom parts correspondingly. The top part is split with a vertical line passing through *h*1 to find the geometric centers *h*3 and *h*4 for left and right parts of top part correspondingly. Similarly, the bottom part is split with a vertical line passing through *h*2 to find the geometric centers *h*5 and *h*6 for left and right parts of bottom part correspondingly. Each part of the image is again split through their geometric centers to obtain feature points *h7, h8, h9… h13, h14*. Then, each part is again split through their geometric centers to obtain all thirty horizontal feature points as shown in Figure 7.

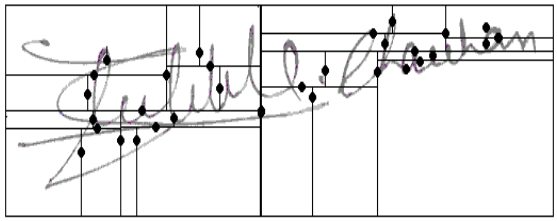


Figure 7. Horizontal splitting of the signature

Now total sixty feature points (*v*1…v30 and *h*1…*h30*) are obtained by vertical and horizontal splitting. Next we will see how each feature point can be compared. The features extracted from the reference signature are stored in the database. For verification of test signature, its features are extracted and are correlated with the corresponding features present in the database.

2) *Angular Features*

The angular features are extracted in two phases. In first phase, the preprocessed signature image is made to undergo vertical splitting and horizontal splitting. The skeleton of the signature image is scanned from left to right and top to bottom to calculate the total number of black pixels. The image is divided into two halves with respect to the number of black pixels by two lines, vertically and horizontally which intersects at a point called the centre of signature or geometric centre.

The signature image is split with horizontal line passing through geometric centre of image to get top and bottom parts of image. The coordinates of the boundary of each part or block is stored. The geometric centre for each block is obtained by locating a point where number of black pixels is half of the total number of black pixels in the block. Geometric centre is found for top and bottom blocks respectively. The top block is split with a vertical line to find the geometric centre for left and right parts of top block. Again the coordinates of the boundary of each block is obtained. Similarly, the bottom block is split with a vertical line to find the geometric centre for left and right parts of bottom block. Then, each part is again split through their geometric centre to obtain angular feature points as shown in Figure 8.

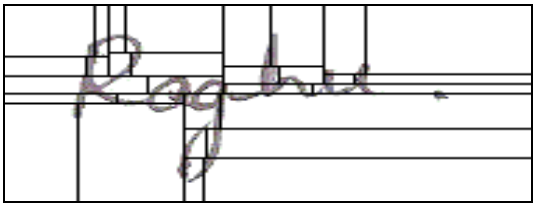


Figure 8. Horizontal and Vertical splitting of the signature

The process of vertical and horizontal splitting of signature leads to 128 blocks. The distance between top left corner of the original image is considered as the reference point and the centre of signature is obtained by the Equation 9.

$$\text{Distance} = \sqrt{(i_2 - i_1)^2 + (j_2 - j_1)^2} \quad \text{---- (9)}$$

where, (i_2, j_2) and (i_1, j_1) are the coordinates of two points.

Consider the reference point, $A(1,1)$ and the centre $C(i, j)$ of signature as shown in the Figure 9. The angle θ is computed using the Equation 10.

$$\theta_i = \cos^{-1}\left(\frac{AB}{AC}\right) \quad \text{--- (10)}$$

where $i = 1,2,3,4.....128$, adjacent side AB and hypotenuse AC are given by Equations 11 and 12 respectively.

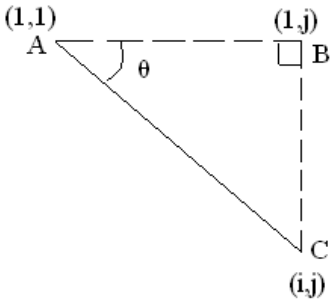


Figure 9. Right angled triangle

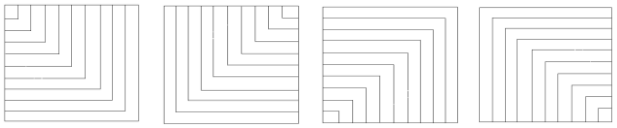
$$AC = \sqrt{(i-1)^2 + (j-1)^2} \quad \text{---- (11)}$$

$$AB = j - 1 \quad \text{---- (12)}$$

The procedure is carried out for all the 128 blocks and the corresponding angular features are obtained. The number of blocks can be increased further but there may be the case where the angle computed would be infinity. As the pixel appears on the top left corner of the block, hypotenuse becomes zero. So the numbers of blocks are limited to 128.

The second phase consists of division of an image into dimensions which are predefined. The image is divided into ten square blocks containing 1, 4, 9, 16, 25, 36, 49, 64, 81 and 100 pixels as shown in the Figure 8. The Figures 10a, 10b, 10c and 10d correspond to division of the signature image from top left, top right, bottom left and bottom right respectively. Each division produces 10 blocks. The procedure is repeated for the remaining 3 parts to get 30 more blocks. This leads to totally 40 blocks. The angular features for these 40 blocks are determined. The 168 angular features obtained from first and second phase are used to verify the

signatures.



a b c d

Figure 10. Division of signature image

v) Matching

a) Correlation matching of center of signature

The matching between the genuine signature and test signature is done based on correlation between the x and y components of vertical and horizontal features for genuine and test signatures.

The x and y components of the vertical and horizontal features for N training Signatures (genuine) are found. The correlation coefficient $R(x, y)$ is calculated using the formula given by Equation 13.

$$R(x,y) = \frac{\Sigma XY - \Sigma X \Sigma Y}{\left(\left[N\Sigma X^2 - (\Sigma X)^2\right]\left[N\Sigma Y^2 - (\Sigma Y)^2\right]\right)^{1/2}} \quad \text{--- (13)}$$

The threshold correlation coefficient of 0.94 is considered for verification purpose. The x and y components of test signature for vertical and horizontal features are obtained. The correlation between x and y components of vertical and horizontal features of genuine and test signatures are calculated. If correlation coefficients of x and y components of vertical and horizontal features are greater than the threshold correlation 0.94, then test the signature is genuine else forged.

b) Distance matching of Angular features

The comparison between the genuine signature and test signature is made by computing the difference between the angles in radians obtained for both the signatures. A threshold is set which decides the authenticity of the signature.

The threshold value of 0.26 radians is considered for verification purpose. The absolute difference between i^{th} angle θ_{Gi} of the genuine signature and i^{th} angle θ_{Ti} of the test signature is compared with the threshold as given in the Equation 14.

$$\left|(\theta_{Gi} - \theta_{Ti})\right| \le 0.26 \quad \text{---- (14),}$$

where $i = 1,2,3,4.....168$.

If the number of angles having difference less than or equal to 0.26 radians, is greater than or equal to 133 then it is considered genuine otherwise forged signature.

vi) Fusion

The fusion of correlation matching score and distance matching score is carried out by considering the equation 15.

$$a + b = 1 \quad \text{--- (15)}$$

The effective value of FAR and FRR using fusion are found using the equations 16 and 17.

$$FRR_{fusion} = a^2 FRR_1 + b^2 FRR_2 \text{ --- (16)}$$

$$FAR_{fusion} = a^2 FAR_1 + b^2 FAR_2 \text{ --- (17)}$$

where FRR_1 and FRR_2 are False Rejection Rate using center of signature and angular features respectively. And FAR_1 and FAR_2 are False Acceptance Rate using center of signature and angular features respectively.

IV. ISFOSV ALGORITHM

Problem definition:

Consider a signature image of a subject whose identity has to be verified. The objective is to

i. Preprocess the acquired signature image

ii Extract the features by splitting operation

iii.Verify the authenticity of the test signature against random and skilled forgery by correlation of center of signature and angular feature

iv Obtain low FAR and FRR

***Assumptions*:**

i. The signature image is captured using scanner

ii.The input signature image should be a 8 bit gray scale image of bitmap image (bmp) format, having vertical and horizontal resolution of 96 dpi.

iii.The minimum size of signature image for second phase feature extraction is 100*100

Table 1 shows the ISFOSV algorithm in which the authenticity of the test signature image is verified. Firstly, the signature is acquired using a scanner and is preprocessed to remove the noise contents and to bring it to the form suitable for feature extraction. Then, the features are extracted from these preprocessed images in two stages by vertical and horizontal splitting. In first stage, totally 60 feature points are extracted by vertical and horizontal splitting. In second stage, 168 angular features are extracted. These features of various signatures are compared with threshold and decision is made whether the signature is genuine or forged.

TABLE 1. ISFOSV ALGORITHM

- Input: Database and Test signatures
- Output: Verified signature
  1. Signature Acquisition
  2. Preprocessing the signature image
  3. Test Signature for Forgery
  4. Compare Signature intersection feature of test Signature with database by correlation matching
  5. Extract Angular Features of Signature
  6. Compare Angular Features of test Signature with database by distance matching
  7. Fuse correlation matching score with distance matching score
  8. Verify the result of Accept/ Reject

V. PERFORMANCE ANALYSIS

The performance analysis is made by using the database consisting of 198 signature samples of 9 subjects. Among them, 90 samples are genuine and 108 samples are forged. Ten genuine signatures are obtained from

each person at different time instances to produce intra-signature variations. Twelve skilled forgeries are obtained for each person's signature. The Matlab version 7.0.1 is used for implementation of the proposed algorithm.

Samples of genuine and skilled forgery signatures used for experimentation are as shown in Figures 11 and 12 respectively.

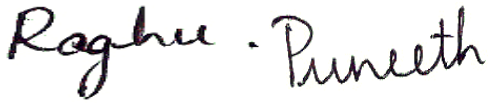


Figure 11. Sample Genuine signatures

Figure 12. Sample skilled Forgery signatures

For each subject, 1 out of 10 genuine signature samples is taken as reference and it is compared with 9 other genuine samples. This process is continued until all signature samples are compared. The same process is repeated for the signature samples of other 3 subjects also to calculate False Reject Rate (FRR).

One sample of each subject is considered as the reference signature and is compared with the 12 forged samples for the same subject. This process is repeated for all the genuine signature samples to calculate False Accept Rate (FAR).

Figure 13 shows the graph of FAR and FRR obtained for different values of angular threshold to compare the performance of signature verification system. The value of Equal Error Rate (EER) obtained is 7.2 corresponding to optimal threshold of 0.256 at a point where FAR equals to FRR. This value of ERR is better compared to many of the existing off-line signature verification systems.

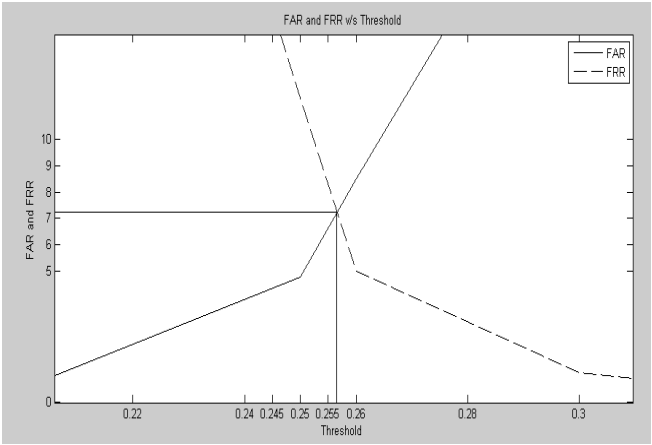


Figure 13. FAR and FRR with Threshold for Angular distance score matching

Figure 14 shows the graph of FAR and FRR obtained for different values of threshold correlation to compare the performance of signature verification system using DWT for de-noising, vertical and horizontal splitting for feature extraction and correlation for feature comparison. As threshold correlation increases, the value of FRR decreases whereas FAR increases. The value of EER obtained is 8 corresponding to optimal correlation threshold of 0.935 at a point where FAR equals to FRR. This value of ERR is better compared to many of the existing off-line signature verification systems.

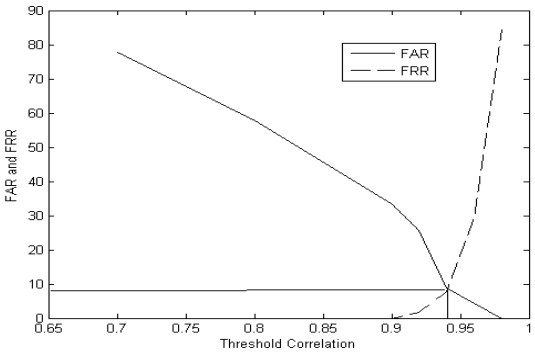


Figure 14. FAR and FRR with Threshold for Correlation matching score

The value of FAR, FRR and EER of Feature Extraction by Signature intersection method, Angular Feature Method and proposed fusion method tabulated as shown in table 2. It is observed that the proposed fusion method has comparatively less error rates. The value of ERR is better compared to many of the existing off-line signature verification systems as well as other methods considered in the paper.

TABLE 2. FAR, FRR AND ERR VALUES FOR EXISTING AND PROPOSED METHODS

Techniques	FAR	FRR	**EER**
Feature Extraction by Signature intersection[21]	8.880	4.995	**4.393**
Angular features method [23]	7.760	8.500	**5.143**
Proposed Fusion method	8.000	7.200	**4.283**

VI. CONCLUSION

The proposed ISFOSV algorithm which is based on fusion of correlation matching score of center of signature and distance matching score angular features is more efficient, accurate, robust and gives better results than the existing techniques against the skilled forgeries. Two sets of features are extracted in two stages. In the first stage, 60 centers of signature and in the second stage 168 angular features are extracted. The comparison is made using correlation and difference in angular features against pre-defined threshold. The algorithm is made efficient by two stage feature extraction and eliminating the random forgeries after the preprocessing. The error rates are further improved by score level fusion of the two feature sets. It is important for a user to put his signature with utmost care so that there are no large variations in the signatures. Otherwise there is a probability of rejection of a genuine signature.

In future, the results can be improved by fusion at feature extraction level and decision level. Neural network and Support Vector Machine techniques can be used for match score fusion. Hence there is scope for algorithms which give still better error rates.

REFERENCES

[1] Jesus F Vargas, Miguel A Ferrer, Carlos M Travieso, and Jesus B Alonso, "Off-line Signature Verification Based on Psuedo-Cepstral Coefficients," *International Conference on Document Analysis and Recognition*, pp. 126-130, 2009.

[2] Ramachandra A C, Pavithra K, Yashasvini K, K B Raja, Venugopal K R and L M Patnaik, "Off-line Signature Verification based on Cross-Validation for Graph Matching," *IEEE International Conference on Electrical and Electronics (INDICON-2008)*, pp. 17-22, 2008.

[3] Milena R P Souza, Leandro R Almeida, and George D C Cavalcanti, "Combining Distances Through an Auto-encoder Network to Verify Signatures," *tenth Brazilian Symposium on Neural Networks*, pp.63-72, October 2008.

[4] Stephane Armand, Michael Blumenstein and Vallipuram Muthukkumarasamy, "Off-line Signature Verification using the Enhanced Modified Direction Feature and Neural-based Classification," *IEEE International Joint Conference on Neural Networks*, pp. 684 -689, July 2006.

[5] Arun Ross and Anil Jain, "Information Fusion in Biometrics," Pattern recognition Letters, Vol. 24, pp. 2115-2125, 2003.

[6] Manuel R. Freire, Julian Fierrez and Javier Ortega-Garcia, "Dynamic Signature Verification with Template Protection using Helper Data," *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 1713-1716, 2008.

[7] Alonso-Fernandez, MC Fairhurst, J. Fierrez and J. Ortega-Garcia, "Impact of Signature Legibility and Signature Type in Off-line Signature Verification," *IEEE International Biometrics Symposium*, pp.1-6, September, 2007.

[8] Lucas Ballard, Daniel Lopresti and Fabian Monrose, "Forgery Quality and its Implications for Behavioral Biometric Security," *IEEE Transactions on System, Man and Cybernetics*, Vol. 37, No. 5, pp.1107-1118, October 2007.

[9] Alessendro Zimmer and Lee L Ling, "A Model Based Signature Verification System," *IEEE International Conference on Biometrics: Theory, Applications, and Systems*, pp.1-6, September. 2007.

[10] Banshider Majhi, Y Santhosh Reddy and D Prasanna Babu, "Novel Feature for Off-line Signature Verification," *International Journal of Computers, Communication and Control*, Vol. 1, No. 1, pp. 17-24, 2006.

[11] Nidal S Kamel, Shohel Sayee and Grant A Ellis, "Glove-based Approach to On-line Signature Verification, "*IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 30, No. 6, pp. 1109-1113, June 2008.

[12] Hanno Coetzer and Robert Scbourin, "A Human-Centric Off-line Signature Verification System," *Ninth International Conference on Document Analysis and Recognition*, pp. 1-6, August 2007.

[13] Ramachandra A C, Jyothi Srinivasa Rao, K B Raja, K R Venugopal and L M Patnaik, "Robust Off-line Signature Verification Based On Global Features," *IEEE International Advance Computing Conference*, pp. 1173-1178, March 2009.

[14] Luiz S Oliveira, Edson Justino, and Robert Sabourin, "Off-line Signature Verification using Writer-Independent Approach," *International Joint Conference on Neural Networks*, pp. 2539-2544, August 2007.

[15] M Taylan Das and L Canan Dulger, "Off-line Signature Verification with PSO-NN Algorithm," *Seventh International Conference on Intelligent Systems Design and Applications*, pp. 843 – 848, 2007.

[16] George Azzopardi and Kenneth P Camilleri, "Off-line Handwritten Signature Verification using Radial Basis Function Neural Networks," *IEEE International Conference on Electrical and Electronics (INDICON-2008)*, pp. 17-22, 2008.

[17] Samaneh Ghandali and Mohsen Ebrahimi Moghaddam, "Off-line Persian Signature Identification and Verification Based on Image Registration and Fusion," *Journal of Multimedia*, Vol. 4, No. 3, pp.137-144, June 2009.

[18] Debasish Jena, Banshidahar Majhi, and Sanjay Kumar Jena, "Improved Off-line Signature Verification Scheme using Feature Point Extraction Method," *Journal of Computer Science*, pp. 111-116, 2008.

[19] 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.

[20] Wan-Suck Lee, N Mohankrishnan, and Mark J Paulik, "Improved Segmentation through Dynamic Time Warping for signature Verification using a Neural Network Classifier," *International Conference on Image Processing*, Vol. 2, pp. 929-933, 1998.

[21] Prashanth C R, K B Raja, K R Venugopal, and L M Patnaik, "Standard Scores Correlation based Off-line Signature Verification System," *International Conference on Advances in Computing, Control, and Telecommunication Technologies*, pp. 49- 53, 2009.

[22] V A Bharadi and H B Kekre, "Off-line Signature Recognition Systems," *International Journal of Computer Applications*, Vol. 1, No. 27, pp. 61-70, 2010.

[23] Prashanth C R and K B Raja, "Off-line Signature Verification based Angular Features," *International Conference on Computer Modeling and Simulation*, pp. 362- 366, 2011.

[24] Tirtharaj Dash, Tanishta Nayak and Subaghata Chattopadhyay, "Offline Handwritten Signature Verification using Associative Memory Net," *International Journal of Advanced Research in Computer Engineering and Technology*, Vol. 1, No. 4, pp. 370-374, 2012.

Prashanth C R received the BE degree in Electronics and the ME degree in Digital Communication from Bangalore University, Bangalore. He is pursuing his Ph.D. in Computer Science and Engineering of Bangalore University under the guidance of Dr. K. B. Raja, Assistant Professor, Department of Electronics and Communication Engineering, University Visvesvaraya College of Engineering. He is currently an Assistant Professor, Dept. of Electronics and Communication Engineering, Vemana Institute of Technology, Bangalore. His research interests include Computer Vision, Pattern Recognition, Biometrics, and Communication Engineering. He is a life member of Indian Society for Technical Education, New Delhi.

K B Raja is an Assistant Professor, Dept. of Electronics and Communication Engineering, University Visvesvaraya college of Engineering, Bangalore University, Bangalore. He obtained his BE and ME in Electronics and Communication Engineering from University Visvesvaraya College of Engineering, Bangalore. He was awarded Ph.D. in Computer Science and Engineering from Bangalore University. He has over 85 research publications in refereed International Journals and Conference Proceedings. His research interests include Image Processing, Biometrics, VLSI Signal Processing, computer networks.

K R Venugopal is currently the Principal and Dean, Faculty of Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. He obtained his Bachelor of Engineering from University Visvesvaraya College of Engineering. He received his Masters degree in Computer Science and Automation from Indian Institute of Science, Bangalore. He was awarded Ph.D. in Economics from Bangalore University and Ph.D. in Computer Science from Indian Institute of Technology, Madras. He has a distinguished academic career and has degrees in Electronics, Economics, Law, Business Finance, Public Relations, Communications, Industrial Relations, Computer Science and Journalism. He has authored 27 books on Computer Science and Economics, which include Petrodollar and the World Economy, C Aptitude, Mastering C, Microprocessor Programming, Mastering C++ etc. He has been serving as the Professor and Chairman, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, Bangalore. During his three decades of service at UVCE he has over 275 research papers to his credit. His research interests include computer networks, parallel and distributed systems, digital signal processing and data mining.

L M Patnaik is the Honorary Professor, Indian Institute of Science, Bangalore, India. During the past 35 years of his service at the Indian Institute of Science, Bangalore, He has over 550 research publications in refereed International Journals and Conference Proceedings. He is a Fellow of all the four leading Science and Engineering Academies in India; Fellow of the IEEE and the Academy of Science for the Developing World. He has received twenty national and international awards; notable among them is the IEEE Technical Achievement Award for his significant contributions to high performance computing and soft computing. His areas of research interest have been parallel and distributed computing, mobile computing, CAD for VLSI circuits, soft computing, and computational neuroscience.