Multi-Modal Biometric Template Protection Using Image Processing

Balamurugan. G[1], Dr. K. B. Jayarraman[2], Arulalan. V[3]
[1,3]MTECH Student,
Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology,
Pondicherry University, Pondicherry, INDIA.

[2]HEAD OF THE DEPARTMENT,
Department of Computer Science & Engineering, Manakula Vinayagar Institute of Technology,
Pondicherry University, Pondicherry, INDIA

***Abstract*: Biometric template protection is the essential progressive approach for the identification of personal verification, because it provides best result of recognition and also improves the security impact. In the single modality the progressive steps of recognition is complicated and weak in security because, it determine only the features of a single mode function (i.e.) face biometrics, hand geometry biometrics; from these, the features of those modal is obtained for the recognition; if there is any misbehaviour or any other misconception, we cannot get the progress relatively; In this paper we propose a multimodal biometric process, to perform the authentication report and high security level, when it is compared to the single modality. We use a fusion technique for the multimodal approach and nearest neighbour classifier has employed to reach for the final decision.**

Keywords— Biometrics, single modality, authentication, multi-modal, nearest neighbour

I. INTRODUCTION

In recent decade, authentication and identity has become important; people are identified as an authorized progress to validate the genuine actions to access the process like ATM access, file transfer access; Before Biometrics, the authentication is based on the knowledge like password or personal identification etc. However accessing of these, traditional methods are potentially critical because password can be hacked or forgotten. Biometrics enables an authentication based method that can provide efficient security for the various applications. Biometrics recognition provides the automatic authentication of an individual based on their characteristics of behavioural and physiological. It is practically impossible to forging biometric process.

Various biometric techniques namely

- Face recognition,
- Finger recognition,
- Palm recognition,
- Hand geometry,
- Iris recognition,
- The Retina images.

Identification system operates either in authentication mode or in verification mode. In authentication mode a large database is potentially used for searching the corresponding individual to the match score. In verification mode, the match should be sufficiently high; the test is matched with the input which has been claimed for identity.

Although biometric system has the recent advance, but still there is a problem for implementation of their recognition system, because due to the real world entity. For example, in face biometric system, there is a problem under in voice process, the noisy environment the recognition gets crashed over there. A potential solution to overcome these problems and to perform the robust security for the authentication using biometrics. And a desired approach is known as the MULTIMODAL BIOMETRICS of various or multiple source of established information for the identification.

Various information at different levels are integrated in the multi-model biometrics and a fusion technique is performed in it. This fusion technique is carried out by a score matching level. It is an achieved by a three fields.

1. SIMPLE SUM;
2. WEIGHTED SUM;
3. MIN/MAX RULES;

Facial and Fingerprint recognition techniques are widely focused system for the recognition studies and also used in the commercial applications. Because due to two reasons on

1. Data acquisition
2. Relatively low costs

In this, we provide an efficient approach to multimodal biometric system using facial recognition and fingerprint recognition. Facial image recognition is performed using texture analysis based on local mapping binary pattern (LMBP). In fingerprint recognition technique is based on the minutiae extraction.

II FACE RECOGNITION TECHNIQUES:

TEXTURE ANALYSIS:

Texture descriptors, have a noticeable attention at the face analysis and also at the face authentication. Two important characteristics of texture analysis is

1. Computational efficiency and
2. Robustness in analysing images at challenging real-time settings.

FINGERPRINT RECOGNITION TECHNIQUES:

Each person has unique fingerprint to achieve this minutiae is obtained. The minutiae extraction is well- defined for the automatic fingerprint recognition

III FUSION TECHNIQUE

Fusion technique which has been employed modalities and it is performed by the product rules. Product rule is achieved by using score matching level fusion and then a nearest neighbour classifier has been employed to reach a final decision. This fusion technique is highly simple and accurate.

IV BIOMETRIC MODALITIES

FACE TEXTURES:

Texture analysis plays a vital role in many real world applications like computer vision, image retrieval, and motion analysis

Application areas:

1. Image retrievals
2. Motion analyst

MAIN APPROACH

Local mapping binary pattern approach, significant advance in the texture analysis which has the property of Tolerance against illuminations changes which is termed as "face histograms"

WORKING:

Step1: Facial images separated into small regions

Step2: a texture description for sub images is then intended using LMBP

Step3: then texture descriptions are combined into histograms

Steps4: Finally this histogram encodes the exterior and the spatial relations of facial regions.

LMBP is known as an ordered set of uniform patterns at a given pixel position. To extract the LMBP texture descriptor of a region, the operation begins by assigning a label to each pixel of a region by the 5x5 neighbourhood of a pixel with the pixel representation.

The decimal form of 8-bit (LMBP) is given by

$$\text{LMBP}(X_C, Y_C) = \sum_{n=0}^{i} s(in - ic)2^n$$

$I_C \rightarrow$ centre pixel

$I_n \rightarrow$ value of the 8 surrounding pixels

$$S(x) = \begin{cases} 1 \; if \; x \geq 0 \\ 0 \; if \; x < 0 \end{cases}$$

The local neighbourhood is defined as the set of evenly spaced sampling points on a circle cantered at the pixel; a sampling point which does not fall at the centre of a pixel is calculated through bilinear interpolation; to compare histograms, we employ the chi-squared distance defined as

$$X^2(u, v) = \sum_{i=1}^{n} \frac{(ui - vi)^2}{(ui - vi)}$$

Were u &v are normalized histograms, n-is the number of elements in the histogram. This pair of histograms was measured by the chi-squared distance.

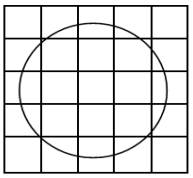

Figure1: Circular neighbourhood with 8 sampled points radius of 2

FINGERPRINT MINUTIA:

Fingerprints has several ridges and furrous Frequently used minutia types are terminated and bifurcation.termination is refers to the ending point of a ridge.

Bifurcation is the branches derived from points on a ridge which describes,We proceed 3 stages for the minutiae extraction .

1.pre-processing stage

2.minutiaextraction stage

3.post processing stage

1.PRE PROCESSING STAGE :

It uses the hstogram equalisation and FFT.FFT is known as the fast fourier transformation .these process are known for the enhancement of image.histogram equalisation is carried out for the expansion of the pixel value of an image.FFT employed to connect the false broken points of ridges and increase the contrast between ridges and furrows.Binarisation is performed to transform the 8-bit grayscale fingerprint image into a binary image where 0s indicate ridges and 1s furrows.

Image segmentation is achieved through a three steps approach

1. Estiamtion of block direction
2. Intensity direction by segmentation

3. Regions of interest by morphological open and close operations to extract

2.MINUTIA EXTRACTION STAGE:

Algorithm of thinning marks down redundant pixels of ridges; these pixels removed till that the ridges are one pixel wide in each small image window(3x3).

3.POST PROCESSING STAGE :

It is carried out to remove false minutia to reduce the complexity of computation;In this ,terminations and bifurcations are unified (x,y,Θ).In this elastic match algorithm is used for counting the minutia pairs matched.

V SCORE MATCHING FUSION :

Combining scores by the different modalities in fusion at score amtching level is easy to acess. Feature vector are stored separately and created independent level. Based on the proxmity of feature vector and template ,the score matching is computed by each subsystem. Finally , the decision is based on the scores of individual;for Final decision ,we obtain by the classification technique. We utilize the simple product rule is given by

$$fi= \prod_{m=1}^{M} ni\, m\, , \forall i$$

were ni^m is the normalised matcher scorer m (m=1,2,……..,M)
M- number of matchers
I-number of individuals in the database
Fi-fused score for user i

K-NN (Nearnest Neighbour) Classfier:

It is used for classifying the context according to their high accuracy and execution time . This classifier is a simple and the training phsae is not a requierment to be specific.

1.Human image in the test set , we compute the distance involving the feature for each input attribute and the features of the claimed identity in the training database.

2.We choose the least distances of the feature vectors for both face and fingerprint separately.

3.Since a test session has the score matching of each biometric is performed; for this we normalise the distance by means of the product

4.We obtain ,the score of the nearest fused distance for face and fingerprint in the training database using nearest neighbour classifier to turn up at a final decision.

5.If the inputs is close sufficient to one of the users in the database ,we authenticate the user.

DESCRIPTION:

In this block diagram (FIGURE2), we compose of two subparts namely creation of database and another is processing of system in it. From the sample image using the both LMBP and the MINUTIAE EXTRACTION we extract the features and then store it in the database. Then by checking process we obtain the input for the both patterns and then the simple product rule is applied to the input sample and then the final matcher is acquired by the classifier named nearest neighbour and then the final output is obtained. In this if the match is validate the authentication output will be provided. If it is not so, then the fine tuning extraction process is carried out with the simple product to revalidate the process.

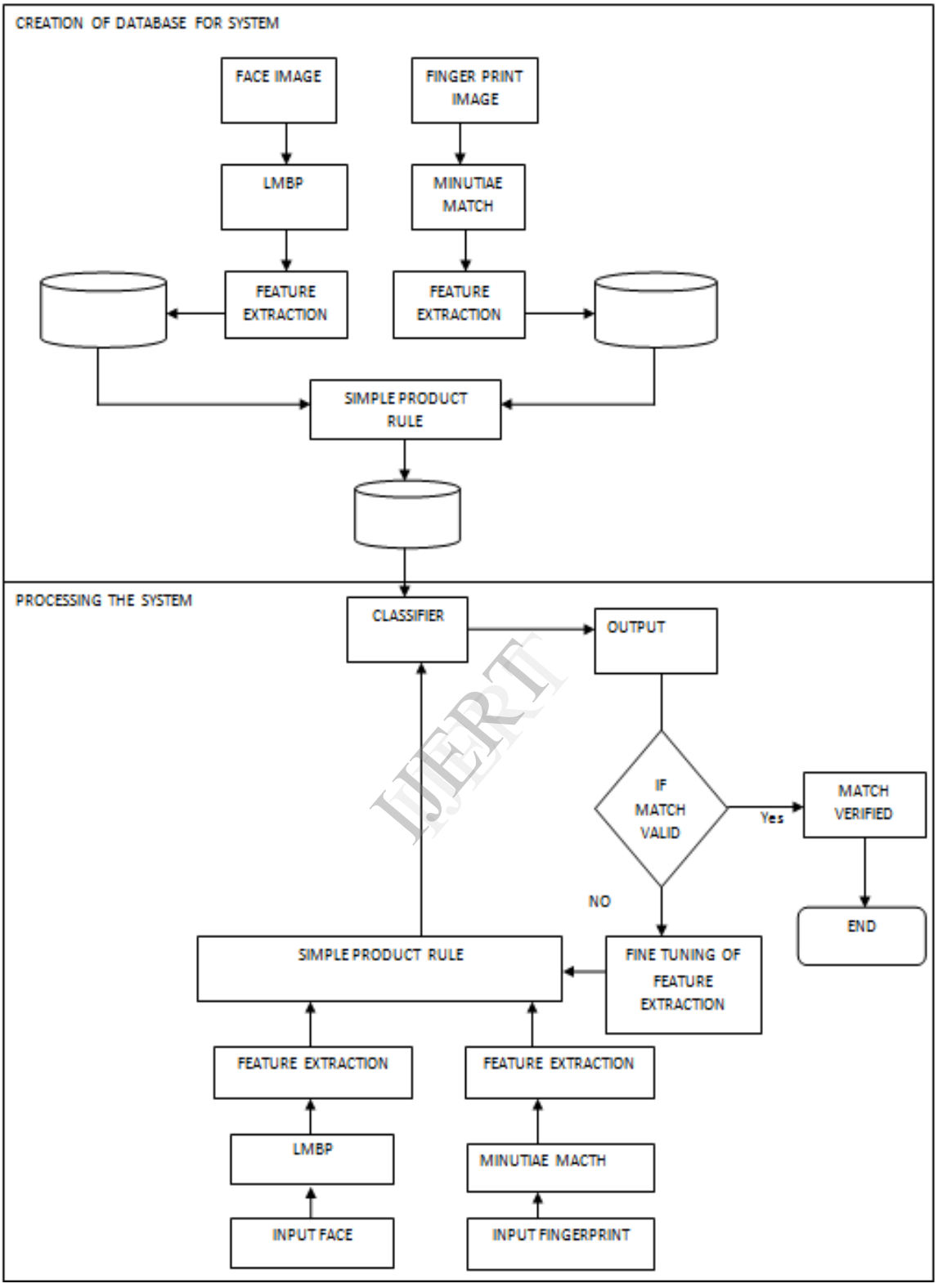

Figure2: Block Diagram

VI CONCULSION:

In this modal, we presented a multi modal biometrics which integrating the two modalities of face and fingerprint which provide better and robust performance. We use local mapping binary pattern features from face sub image and extracted minutia information from fingerprints. Fusion technique is carried by the product rule and their final decision is obtained by the classifier named nearest neighbour classifier. From this, we obtain high robust and accuracy for the authentication.

REFERENCE:

1. Jain, R. Bole, Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers.
2. D. Milton, et al., Handbook of Fingerprint Recognition, Springer, (2003).
3. A Survey on Biometric Recognition Techniques Arulalan.V, Balamurugan.G, Premanand. V International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 2, February 2014
4. R. Bolle, J. Connell, and N. Rather, Biometric Perils and Patches, Pattern Recognition, Vol. 35, (2002) 2727-2738.
5. W. Stallings, Cryptography and Network Security, Pearson Ed. Inc., (2003).
6. H. Lee, et al: An Audio Watermarking Modifying Tonal Maskers, ETRI Journal, Vol.27, No.5, (2005).
7. S. Jung, et al.: An Improved Detection Technique for Spread Spectrum Audio Watermarking with a Spectral Envelope Filter, ETRI Journal,
8. Jain, U. Uludag, and R. Hsu: Hiding a Face in a Fingerprint Image, Proc. of Int. Conf. on Pattern Recognition, (2002) 52-54.
9. M. Yeung and S. Penchant: Verification Watermarks on Fingerprint Recognition and Retrieval.
10. S. Pan, et al.: A Memory-Efficient Fingerprint Verification Algorithm using A MultiResolution Accumulator Array for Match-on-Card ETRI Journal, Vol. 25, No. 3 (2003) 179-186.
11. M. Turk and A. Petland: Face Recognition using Eigen face, Proc. of IEEE Conf. on Computer Vision and Pattern Recognition, (1991).
12. R. Dugad, K. Ratakonda, and N. Ahuja: A New Wavelet-based Scheme for Watermarking Images, Proc. of the ICIP, (1998)