IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 73-79
www.iosrjournals.org

Design of Multimodal Biometrics Authentication using Feature Extraction and Fusion

[1]Ms.D. Indra Devi, [2]M. Karthiga, ME CSE
Department of Computer Science and Engineering Indra Ganesan College of Engineering Trichy, Tamilnadu, India
clifi2001@gmail.com
Department of Computer Science and Engineering Indra Ganesan College of Engineering Trichy, Tamilnadu, India
karthimuthu11@yahoo.com

ABSTRACT–*Multimodal biometric can overcome the limitation possessed by single biometric trait and give better classification accuracy. The present work proposes an authentication system with the fingerprint, face and iris multimodal biometric system based on fusion at the feature level. The performances of fingerprint, face and iris recognition can be enhanced using a proposed feature selection method to take an optimal subset of features. Fingerprints are the most popular and studied biometric features. Their stability and uniqueness makes the fingerprint identification system extremely reliable and useful for security applications. An optimized fingering print algorithm is used to extract the ridge count, ridge length, and ridge curvature direction features from a fingerprint. Iris is also a unique biometric feature, advanced iris and sclera algorithm is used to extract the iris and sclera features of the eye and Eigen face feature extraction algorithm is used to extract the face feature extraction. The results indicate that the proposed feature selection method is able to improve the classification accuracy in terms of total error rate.*

Index Terms - *Biometrics, Multimodal, Face, Fingerprint, Iris and Fusion.*

I. INTRODUCTION

"Biometrics" means "life measurement", however the term sometimes relates to the utilization of distinctive physiological characteristics to identify an individual. One in every of the applications which the majority goes with life science is secure. However, life science identification has eventually a way broader relevancy as a computer interface becomes a lot of natural. It's an automatic methodology of recognizing someone supported a physiological or activity characteristic. Among the options measured are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, voice, etc. Biometric technologies have become the muse of an intensive array of extremely secure identification and private verification solutions. Because the level of security breaches and dealings fraud will increase, the necessity for extremely secure identification and private verification technologies is changing into apparent. In recent years, biometrics authentication has seen extended enhancements in responsibility and accuracy, with a number of the traits providing sensible performance. However, even the simplest biometric traits until date face varied problems; a number of them are inherent to the technology itself. Especially, identity verification systems typically suffer from enrollment issues because of non-universal biometric traits, status to biometric spoofing or lean accuracy caused by the noisy knowledge acquisition in certain environments.

One way to beat these issues is that the use of multi-biometrics. Driven by lower hardware prices, a multi biometric system uses multiple sensors for data acquisition. This enables capturing multiple samples of one biometric trait (called multi-sample biometrics) and/or samples of multiple biometric traits (called multi supply or multimodal biometrics). This approach additionally allows a user who doesn't possess a selected biometric identifier to still inscribe and evidence victimization different traits, therefore eliminating the enrolment issues and creating it universal. A unimodal biometric system consists of 3 major modules: device module, feature extraction module and matching module. The performance of a biometric system is basically laid low with the dependability of the device used and also the degrees of freedom offered by the options extracted from the detected signal. Further, if the biometric attribute being detected or measured is noisy (a fingerprint with a scar or a voice altered by a cold, for example), the resultant matching score computed by the matching module might not be reliable. This drawback may be solved by putting in multiple sensors that capture completely different biometric traits. Such systems, called multimodal biometric systems, are expected to be additional reliable as a result of the presence of multiple items of proof. These systems also are able to meet the

rigorous performance needs obligatory by varying applications. However, multimodal systems address the matter of non-universality: its potential for a set of users who don't possess a specific biometric. As an example, the feature extraction module of a fingerprint authentication system is also unable to extract options from fingerprints related to specific people, as a result of the poor quality of the ridges. In such instances, it's helpful to accumulate multiple biometric traits for collateral the identity. Multimodal systems additionally offer associate anti-spoofing measures by creating it tough for a trespasser to spoof multiple biometric traits at the same time. By asking the user to gift a random set of biometric traits, the system ensures that a live user is so gifted at the purpose of acquisition. However, the associate degree integration theme is needed to fuse the knowledge conferred by the individual modalities.

II. RELATED WORK

A template-level fusion algorithm working on a unified biometric description. The aforementioned result leads to a matching algorithm that is able to process fingerprint codified templates, iris-codified templates, and iris and fingerprint fused templates. In contrast to the classical minutiae-based approaches, the nominated system performs fingerprint matching using the segmented regions (ROIs) surrounding (pseudo) singularity points [1].Multibiometric systems are being increasingly deployed in many large-scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to unibiometric systems. However, multibiometric systems require storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user, which results in increased risk to user privacy and system security. One method to protect individual templates is to store only the secure sketch generated from the corresponding template using a biometric cryptosystem [2].In this it is intended to investigate the performance of multimodal biometrics using palm print and fingerprint. Features are extracted using Discrete Cosine Transform (DCT) and attributes selected using Information Gain (IG). Their implemented technique shows an average improvement of 8.52% compared to using the palm print technique alone. The processing time does not increase for verification compared to palm print techniques [3].In this a multimodal sparse representation method, which represents the test data by a sparse linear combination of training data, while constraining the observations from different modalities of the test subject to share their sparse representations. Thus, simultaneously take into account correlations as well as coupling information among biometric modalities. A multimodal quality measure is also implemented to weigh each modality as it gets fused. Furthermore, they also kernelize the algorithm to handle non-linearwith data. The optimization problem is solved using an efficient alternative direction method. Various experiments show that the projected method compares favorably with competing fusion-based methods [4].Fusion at feature level is considered here for the purpose of recognition. The biometrics considered for fusion is face and iris. Here, new face images along with iris images are generated, and they are included in the training set. Feature-level fusion is incorporated. The recognition rates of the classification algorithm thus obtained are statistically found to be significantly better than the existing feature level fusion and classification techniques [5].This system uses Local Binary Patterns local feature extractor and subspace Linear Discriminant Analysis global feature extractor ofthe face and iris images, respectively. Face and iris scores are normalized using tanh normalization, and then, Weighted Sum Rule is applied to the fusion of these two modalities. Improved recognition accuracies are achieved compared to the individual systems and multimodal systems using other local or global feature extractors for both modalities [6].

III. SYSTEM OVERVIEW

Literatures in Section II have some potential difficulties such as they are fusion is performed only for the same identifiers with different features.The system architecture design in Fig 1 for enrollment phase and Fig 2 for verification phase shows the overall architecture of the process that is carried out.

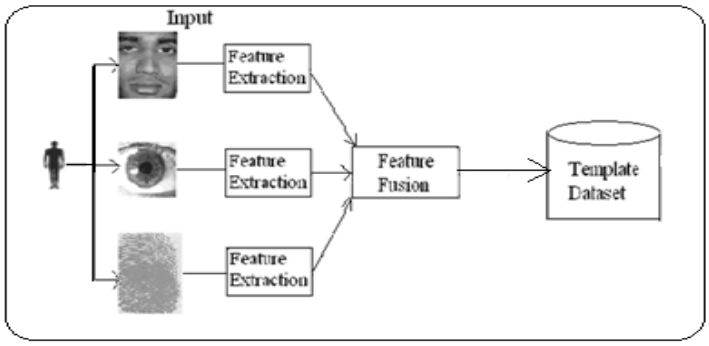

Fig 1 Architecture design for enrollment phase

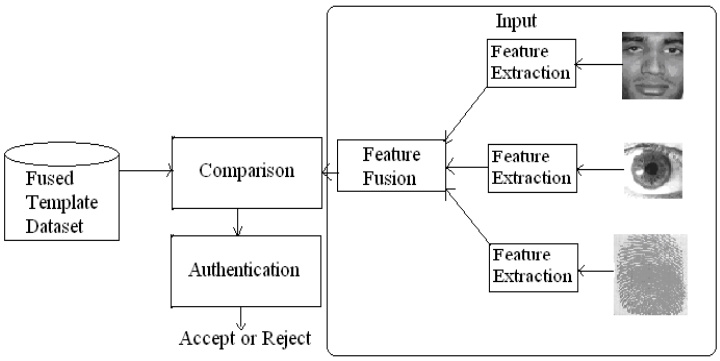

Fig 2 Architecture design for verification phase

Theblock diagram of a multi-modal biometric authentication System, Showing three modalities (i.e., the fingerprint, the iris and the face). The system consists of four modules (i.e., feature extraction, fusion, matching and decision.

A. Iris Feature Extraction

The important steps involved in iris recognition are:

1. Pupil Detection
2. Iris Detection
3. Normalization
4. Feature Extraction

Prior to implementation of the steps mentioned above iris image has to be acquired which should be rich in texture because all subsequent stages depend upon the image quality.

The pupil is the darkest portion of the eye and is detected and removed from the rest of the eye image so that the only iris pattern can be used for matching. To find the outer iris boundary intensity variation approach is used. In this approach concentric circles of different radii are drawn from the detected center. The circle, havinga maximum change in intensity with respect to previous drawn circle is iris circle. The approach works fine for iris images having sharp variation between iris boundary and the sclera. The radius of the iris and pupil boundary is used to transform the annular portion of a rectangular block, known as the strip. The localized iris image is transformed into strip. The mapping is done after transforming the Cartesian coordinates into its polar equivalent using

$$\begin{cases} I(x(\rho,\theta),y(\rho,\theta)) \rightarrow I(\rho,\theta) \\ with \\ x_p(\rho,\theta) = x_{\rho 0}(\theta) + r_p * \cos(\theta) \\ y_p(\rho,\theta) = y_{\rho 0}(\theta) + r_p * \sin(\theta) \end{cases} \quad (1)$$
$$x_i(\rho,\theta) = x_{i0}(\theta) + r_i * \cos(\theta)$$
$$y_i(\rho,\theta) = x_{i0}(\theta) + r_i * \sin(\theta)$$

where r_p and r_i are respectively the radius of the pupil and the iris in equation (1), while (x_p (θ), y_p(θ)) and (x_i(θ), y_i(θ)) are the coordinates of the pupillary and limbic boundaries in the direction θ. The value of θ belongs to [0; 2π], ρ belongs to [0; 1]. The transformed iris image consists of points taken from the pupil boundary to the outer iris boundary. Thus the same set of points is taken for every image. The iris image is normalized so that the size of the strip does not vary for different images. The size of the same iris image may vary due to expansion and dilation of the pupil. Thus the size of iris strip is fixed for every iris image. In this experiment the size of strip is 80×360 pixels.

IRIS Effective Region Extraction and Pattern Generation

1. Take the 8-Bit BMP Image produced from previous Algorithm as Input and open this BMP file in binary Read Mode.
2. Read the raster Data and Store the raster Data into a Matrix of vector size. Where vs = fsize - (54+(4*256)).
3. Then a 8*12 Iris Pattern is extracted from the Edge Detected BMP using the following logic-

```
for (x=0;x<=oi.rows-1;x++)
 {
     for (y=0;y<=oi.cols-1;y++)
     {
     if ( y<30 && x=((oi.rows/2)+4) && GrayValue == 255)
      {
           for (i=0;i<8;i++)
           {
                for (j=0;j<12;j++)
                     {
*(ei.data + (i *ei.cols) + j) = *(oi.data + (x * oi.cols) - (i * oi.cols) + (y + j));
 Write to new BMP Image file
                     }
            }
      }
      }
}
```

Where vs-vector size,fsize-file size,oi-original image and ei-edge image

B. Fingerprint Feature Extraction

The fingerprint is one of the most widely used biometric modality. The main reason behind the use of fingerprint biometric is that it is the most proven technique to identify the individual. The fingerprint is basically the combination of ridges and valleys on the surface of the finger. The major steps involved in fingerprint recognition using minutiae matching approach after image acquisitions are:

1. Image Enhancement
2. Minutiae Extraction

A fingerprint image is corrupted due to various kinds of noises such as creases, smudges and holes. It is almost impossible to recover the true ridge/valley structures from the unrecoverable regions; any effort to improve the quality of the fingerprint image in these regions may be futile. Therefore, any well-known enhancement algorithm may be used to improve the clarity of ridges/valley structures of fingerprint images in recoverable regions and to mask out the unrecoverable regions. The enhancement starts with normalization of input fingerprint image so that it has pre-specified mean and variance. The orientation image is estimated from the normalized input fingerprint image. Further, frequency image is computed from the normalized input

fingerprint image and the estimated orientation image. After computation of frequency image the region mask is obtained by classifying each block in the normalized input fingerprint image into a recoverable or unrecoverable block. Lastly, a bank of Gabor filters which is tuned to local ridge orientation and ridge frequency is applied to the ridge and valley pixels in the normalized input fingerprint image to obtain an enhanced fingerprint image.

The enhanced fingerprint image is binarized and submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide. The skeleton image is used to extract the minutiae points which are the points of ridge endings and bifurcations. The location of minutiae points along with the orientation is extracted and stored to form feature set using the following algorithm.

An algorithm for extracting ridge features. (FPFE)

1. Perform preprocessing steps and extract a ridge image from a fingerprint.
2. Traverse the ridge-valley structures along the vertical axis from each minutia origin.
3. If the vertical axis intersects with the ridges attached to a minutia, extract ridge features (ridge count, ridge length, ridge curvature direction, and ridge type) from the ridges.
4. The origin to the minutia and form a ridge feature vector between the origin and the minutiae.
5. Keep traversing all the ridges until one of three terminating conditions is satisfied.
6. If all minutiae are used as the origin minutiae, terminate the procedure. Otherwise, return to step 2).
7. The termination conditions include the following three cases:
    1. The vertical axis reach a background region in the fingerprint image.
    2. The vertical axis reach a poor quality region in the fingerprint image.
    3. The vertical axis reach a high circular variance region in the fingerprint image.

C. FACE FEATURE EXTRACTION

In face recognition's core problem is to extract information from photographs. This feature extraction process can be defined as the procedure of extracting relevant information from a face image. The extracted feature information must be valuable to the later step of identifying the subject with an acceptable error rate. The feature extraction process must be efficient in terms of computing time and memory usage. The feature should also be optimized for the classification step.

Facial recognition systems usually consist of four steps,

1. Face detection (localization),
2. Face pre-processing (face alignment/normalization)
3. Feature extraction.

Algorithm for extracting face feature. (FFE)

1. Get the input image and template directory.
2. Also get the number of Eigen faces and threshold value.
3. The image size compatibility is tested. If the image size is compatible not, then returnedan error, otherwise continue to the next step.
4. The faces constituting the training set should be prepared for processing.
5. The average matrix has to be calculated, then subtracted from the original faces and the result stored in a variable.
6. The covariance matrix C is calculated according to the variable.
7. The eigenvectors ui and the corresponding eigenvalues should be calculated. The eigenvectors (Eigen faces) must be normalized so that they are unit vectors, i.e. of length 1. The description of the exact algorithm for determination of eigenvectors and eigenvalues, is omitted here, as it belongs to the standard collection of most math programming libraries.
8. The higher the eigenvalue, most characteristic features of a face does the particular eigenvector describe. Eigen faces with low eigenvalues can be omitted, as they explain only a small part of the characteristic features of the faces.

After M' Eigen faces ui are determined.

IV. RESULT AND ANALYSIS

The performance of the proposed algorithms is evaluated using the real time images and the results are shown in the below figures. Fig 3 shows the iris feature extraction. The figure 4 shows the finger print extraction and Fig 5 shows the face feature extraction results of multimodal biometric authentication using fusion at the feature level.

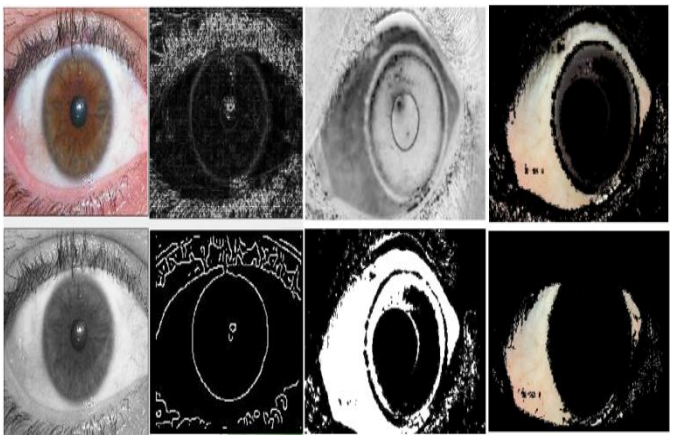

Fig 3 IRIS FEATURE EXTRACTION

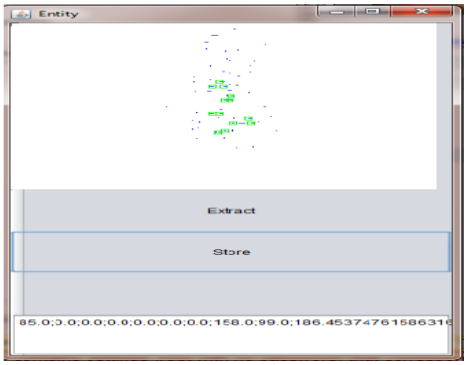

Fig 4 Fingerprint Feature Extraction

Fig 5 Face Feature Extraction

V. CONCLUSION AND FUTURE SCOPE

In this paper the individual scores for each trait are combined at classifier level and trait level to develop a multimodal biometric system are proposed.This system proposes a fingerprint, face and iris multimodal biometric system based on fusion at the feature level for authentication. The optimized algorithms are used to extract the fingerprint, face and iris features. The proposed work of feature selection method to improve the performance of individual fingerprint, face and iris recognition by removing the redundant and irrelevant information. The results show that the proposed method is can find an optimal subset of the feature that sufficiently describes fingerprint, iris and face images by removing unwanted and redundant features and at

the same time improving the classification accuracy. In future the extracted features are fused into one object. The fused data are compared with the template data, and to provide whether the user is authenticated or not.

REFERENCES

[1] Vincenzo Conti, Carmelo Militello, Filippo Sorbello," A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", JULY 2010.
[2] Abhishek Nagar, Karthik Nandakumar, and AnilK. Jain "Multibiometric Cryptosystems Based on Feature-Level Fusion", FEBRUARY 2012.
[3] Krishneswari, K. and S. Arumugam," Multimodal Biometrics using Feature Fusion", Journal of Computer Science, 2012.
[4] Sumit Shekhar, Vishal M. Patel, Nasser M. Nasrabadi and Rama Chellappa" Joint Sparse Representation for Robust Multimodal Biometrics Recognition", 2013.
[5] Dhiman Karmakar • C. A. Murthy, "Generation of new points for training set and feature-level fusion in multimodal biometric identification".Springer, 2013.
[6] Maryam Eskandari and Onsen Toygar" Fusion of face and iris biometrics using local and global feature extraction methods", Springer, Nov 2012.