International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P), Volume-7, Issue-1, January 2017

Improved Security through Multimodal Biometric using Fingerprint and Iris

Mohamed Basheer. K.P, Dr. T. Abdul Razak

Abstract— **Multimodal biometric systems imitate the unification of two or more unimodal biometric systems. Such systems are predicted to be more sound due to the residence of multiple independent pieces of evidence. Hence they sign in at unparallel levels of security. This study proposes a blending of multimodal fingerprint and Iris recognition technique. The task is two section composition first is feature extraction from both the modalities and then feature level fusion of the extracted features and finally applying a encryption technique to the fused output.**

Index Terms— **multibiometric, unimodal, encryption, multimodal security.**

I. INTRODUCTION

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. A number of bio-crypto algorithms have been proposed, they have limited practical applicability due to the trade-off between recognition performance and security of the template Multimodal biometric systems that infer personal identification based on multiple physiological or behavioural characteristics are preferred. Consider, for example, a network logon application where a biometric system is used for user authentication. If a user cannot provide good fingerprint image due to a cut in the finger for example, then face and voice or other biometric identifiers can be used instead (or in conjunction). Voice identification as well cannot operate efficiently in a noisy environment or in the case where the user has some illness affecting his voice. Facial recognition is not suitable if the background is cluttered, or if the person's stored information are several years old. For these reasons among others, multimodal biometric systems found their way to emerge in the recent and advanced authentication and security applications. Fingerprint and Iris are the two modalities discuss in this paper. Fingerprint module takes fewer times, in taking the fingerprint template, as its size is smaller it will take reasonable time in taking the Fingerprint template and accepting the template. In Iris system what happens that this system is accepting everywhere, at the time of capturing the eye image no physical interaction is needed with the sensors. So you can capture the image from everywhere and used the template for recognition.

Mohamed Basheer. K.P, Assistant Professor, Department of Computer Science, Sullamussalam Sciece College,Areacode

Dr.T. Abdul Razak, Associate Professor & Research Supervisor, Jamal Mohammed College, Thiruchirappalli, Tamilnadu, India

Levels of Fusion

The information of the multimodal system can be fused at any of the four modules.

Fusion at the sensor level: In this the raw data from different sensors are fused. In it the data is fused at very early stage so it has a lot of information as compared to other fusion levels. Very less work has been done in this area.

Fusion at the Feature Extraction Level*:* The data or the feature set originating from multiple sensors or sources are fused together. Features extracted from each sensor form a feature vector. These features vectors are then concatenated to form a single new vector. In feature level fusion, can use same feature extraction algorithm or different feature extraction algorithm on different modalities whose features has to be fused. The feature level fusion is challenging because relationship between features is not known and structurally incompatible features are common and the curse of dimensionality

Matcher Score Level: Each system provides a matching score indicating the proximity of the feature vector with the template vector. The scores obtained from different matchers are not homogeneous, score normalization technique is followed to map the scores obtained from different matchers on to a same range. These scores contain the richest information about the input.

Fusion at the Decision Level*:* The final outputs of the multiple classifiers are combined. A majority vote scheme can be used to make final decision.

Biometric systems that integrate information at the early stages are more effective than those in which integration is done in later stages. So fusion at the feature level is expected to give better recognition results but it is difficult to integrate at this level because feature sets of the various systems may not be compatible. More over all commercial Biometric systems don't provide access to the feature sets, which they use in their products.

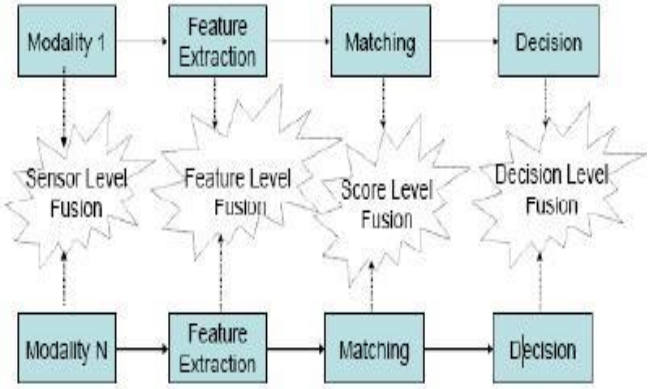


Fig1.Fussion at different levels matching of the biometric characteristic.

Types of the Multimodal Systems

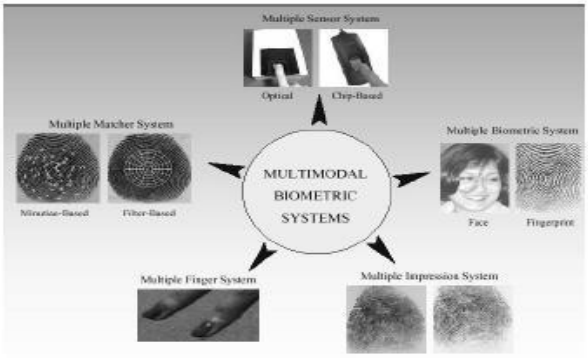


Fig 2. Types of Multimodal Systems

Single biometric trait, multiple sensors Multiple biometrics Multiple units, single biometric traits: Multiple snapshots of single biometric

Modes of Operation

A multimodal biometric system can work in three modes:

Serial mode*:* In the serial mode the output of one biometric characteristic is used to reduce the no of possible identities before the next characteristic is used.

Parallel mode: In it the information from multiple characteristics is taken together to perform recognition.

Hierarchical mode*:* In it individual classifiers are combined in a tree like structure. This mode is well suited where large no of classifiers.

II. RELATED STUDY

K.Sasidhar [1] converged on fact that multimodal biometric systems perform well than unimodal biometric systems and are popular even more complex also at the same time. His paper also epitomes the notion of accuracy and performance of multimodal biometric authentication systems using state of the art Commercial Off- The-Shelf (COTS) products.

T.Sheeba [2] laid emphasis on that multimodal biometric systems have been widely adopted to overcome the shortcomings of unimodal biometric systems . Among various multimodality options, fingerprint and finger vein multimodality ensures higher performance and spoofing resistance. This multimodal technology has reached an unparalleled level of security, accuracy and performance.

P.S.Sanjekar [3] has thrown some light on the shortcomings of unimodal biometrics such as noisy data, intra class variation, and spoofing which result in the system that possess less accuracy and low security. To overcome these problems and to rise level of security multimodal biometrics came. Multimodal biometrics makes the use of multiple source of information for personal authentication..

Vijay M. Mane[4] stated that the fusion of multiple biometrics helps to minimize the system error rates. Fusion options include processing biometric modalities sequentially until an acceptable match is obtained. Another one works in a way that combine scores from separate classifiers for every modality. He stressed on the fact that most of the biometric systems deployed in real world applications are unimodal that possess considerably high false acceptance rate (FAR) and false rejection rate (FRR). he also explained that todays unimodal system are having limited discrimination capability.

Shweta Malhotra [5] here author presents an approach to enhance the invisible watermarking technique with cryptography. The biometric trait is modified using invisible watermark information and is further secured using cryptography. The template is made more secure using encryption techniques like AES, MAES and finally stored in database.

III. PROPOSED MULTIBIOMETRIC SYSTEM

Fig. 3 shows the block diagram of the proposed multimodal biometric recognition system. First apply pre processing to extract the region of interest i.e feature extraction from each biometric image. Then the feature vectors are extracted from each biometric separately, after this encrypt the fused template in which one image comes at front another at background. Then that fused image which is output of feature extracted fingerprint and eye is encrypted to achieve security hence based on this, a final decision is made.

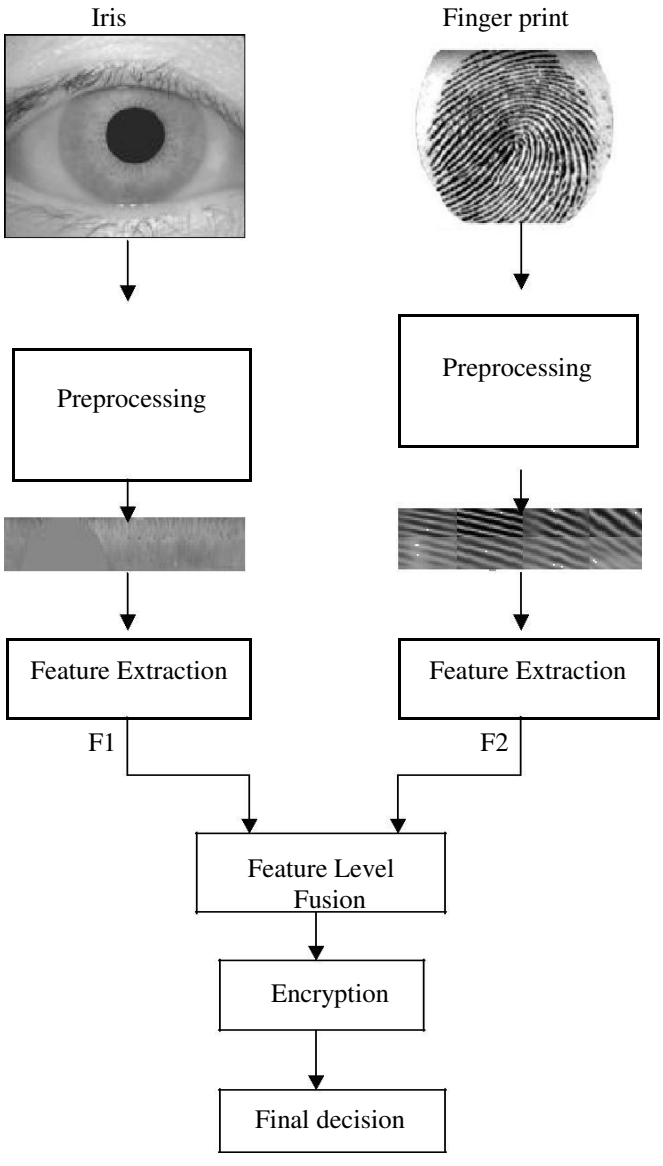


Fig 3. Proposed system

The used unimodal biometric systems

1) Iris Identification System

Iris recognition is considered to be one of the most accurate biometric technologies when compared to other technologies commercially in use today. This is because the false match and false non- match errors are very small, which implies a very high accuracy.

The Iris identification system consists of three stages, the first stage is the iris analysis which involves iris localization and iris normalization. The second stage is the feature extraction and encoding. The last stage is the recognition stage which involves identification and verification.

Only the significant features of the iris must be encoded in order to generate the iris code for the matching process. In the proposed system, binary string , segmented iris ,noise removal functions are used for extracting the features from the iris images. Finally matching is done using the calculated Hamming distance (HD) which is a measure of the number of different bits between the two iris codes.

2) Fingerprint identification System

A fingerprint is composed of many ridges and furrows. These ridges and furrows present good similarities in each small local window, like parallelism and average width. However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows. For the fingerprint image pre processing stage, used a Histogram Equalization and Fourier Transform to do image enhancement. Region of Interest extraction is done.

Fingerprint Enhancement by Fourier Transform

The image divided into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to:

$F(u,v)=\Sigma f(x,y) x \exp\{-jux((ux/M)+vy/N))\}$ --- (1)

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

In order to enhance a specific block by its dominant frequencies, multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT = abs(F(u,v)) = |F(u,v)|.

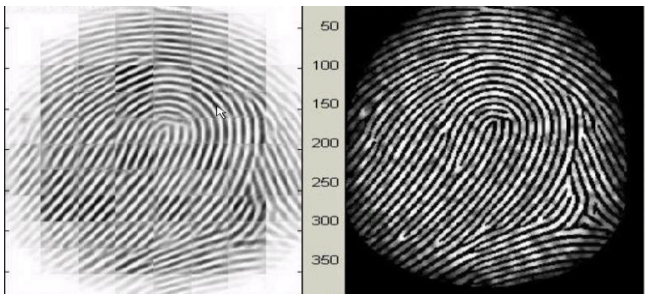
Get the enhanced block according to

$G(x,y)=F^{-1}\{F(u,v)XF(u,v)^2\}$ ---------- (2)

where $F^{-1}(F(u,v))$ is done by (3)

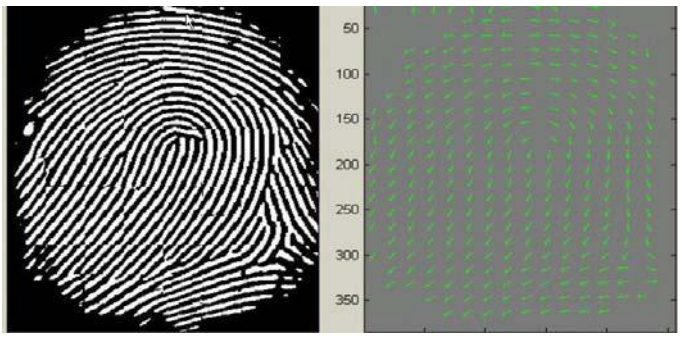
$f(x,y)=1/MN(\Sigma F(u,v)Xexp\{2xX((ux/M+vy/N)))\}$

for x = 0, 1, 2, ..., 31 and y = 0, 1, 2, ..., 31.



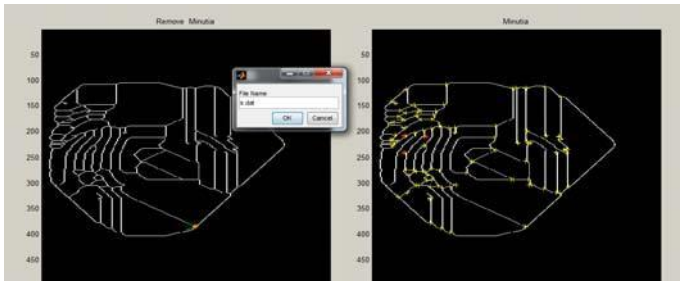
Finding Region of Interest (ROI)

In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information. Then the bound of the remaining effective area is sketched out since the minutia in the bound region are confusing with those spurious minutia that are generated when the ridges are out of the sensor.



MINUTIA MATCH

Given two set of minutia of two fingerprint images, the minutia match algorithm determines whether the two minutia sets are from the same finger or not.



IRIS:

The following assumptions are considered for human eye detection :

- Image should not be too noisy.
- Eyes should be in normal horizontal position (i.e. the head should not be tilted).
- Iris diameter shouldn't be very small in respect to the size of image.
- The two candidate circles for irises must have similar radiuses. For a normal human subject, the irises are not that different, and have a diameter of around 12 mm (the normal human pupil is around 2-3 mm in daylight and can go to 7mm during night time).

First of all input is given that is image of iris from the cassia database from where the required images of iris gathered.

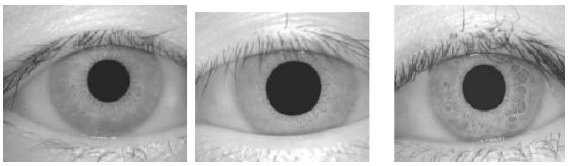


Fig. 2 Sample images for one person from CASIA iris

Then extract feature from this input image using

Step 1 Take input the image of which eye detection has to be performed.

Step 2: Convert colour image into grayscale image.
Step 3: Smoothen the image to remove noise present in the image and to avoid any feature that is not of interest using Gaussian mask.
Step 4: Detect the edges of the image using the Prewitt operator.
Step 5: Detect the iris (black circular region inside eye) using Hough transform for circle detection.
Step 6: Store the center and radii of the circles thus detected from the previous step.
Step 7: Detect the presence of the ellipses surrounding the circle again using the Hough transform.
Step 8: Geometrically match each of the detected circle enclosed in an ellipse
Step 9: Rule out the pair of eyes based on geometrical considerations from the above step.
After performing feature extraction steps we get segmented and polar output of iris

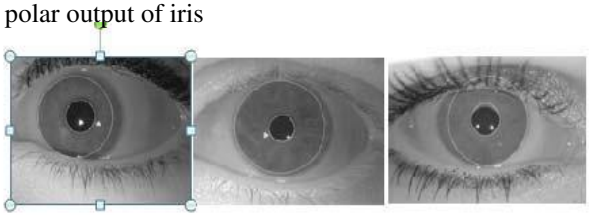


Fig 4 .Desired features are extracted from iris

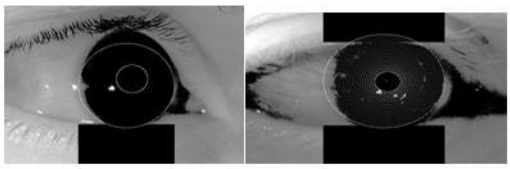


Fig 5. Noisy part of the image

IV. CONCLUSION

The scope of multimodal biometrics systems for providing a more secure environment with considerably high authentication accuracy by overcoming the shortcomings of individual biometrics. There are many multimodal biometric systems alive for authentication of a person but still opting the well suited modals, electing optimal fusion level and redundancy in the extracted features are some ultimatums in designing multimodal biometric system that needs to be fix up.

REFERENCES

[1] K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna & K.KailasaRao, "Multimodal Biometric Systems –Study To Improve Accuracy And Performance" International Journal of Computer Science & Engineering Survey (IJCSES), Vol.1, No.2, November 2010, pp. 54-61.

[2] T.Sheeba , M.Justin Bernard, " Survey on Multimodal Biometric Authentication Combining Fingerprint and Finger vein" International Journal of Computer Applications (IJCA), Vol. 51, No.5, August 2012pp.55-60

[3] P. S. Sanjekar , J. B. Patil, "An Overview Of Multimodal Biometrics" Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1, February 2013, pp. 57-64.

[4] Vijay M. Mane , Dattatray V. Jadhav , "Review of Multimodal Biometrics: Applications, challenges and Research Areas" , International Journal of Biometrics and Bioinformatics (IJBB), Volume 3, No. 5 , 2013, pp. 90-95.

[5] Sumeet kaur "Enhancing template security by a biometric key generating cryptosysytem", IJARCSSE, Vol. 3,Issue 8, pp 973-976, August 2013

[6] Debnath bhattacharya " Biometric Authentiction :A Review " Vol. 2 , Issue 3 , Sep 7 2009 , pp 13-26

[7] Parvinder S.Sandhu, Iqbldeep Kaur, Amit Verma, Samriit Jindal "Biometric Methods & Implementation of Algorithms " Vol.3 Issue 8 , 2009 , pp 492-496

[8] Harpreet Saini & Kanwal Garg "Comparitive Analysis of Various Biometric Techniques for database Security " IJSR (International journal of Science and Research) Vol. 2 Issue 4, pp150-153, April 2013Sulochana Sonkamble & Dr. Ravindra Thool "Survey Of Biometric Recognition Systems And Their Applications " Journal of Theoretical And Applied Information Technology(JATIT) , pp 45-51, 2005

[9] Nandakumar, K., 2008. "Multibiometric systems: Fusion strategies and template security". Ph.D.Thesis, Department of Computer Science and Engineering, Michigan State University.

[10] "Biometric template encryption" by A.K.Mohapatra Madhvi Sandhu IGIT,GGSIP University,Kashmere GateDelhi Published in International Journal of Advanced Engineering & Application, Jan. 2010

[11] N. Kankrale, Prof. S. D. Sapkal. Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems *Department of Information Technology SRES*