International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 11 6308 - 6312

Use of Multimodal Biometric System for the Authentication and Security

Deep Kumar Sharma
M.Tech (SE)
SRSMSCET Bareilly
UP, India
shsharma814@gmail.com

Mukesh Azad
Department of CS/IT
SRMSCET Bareilly
UP, India
Mukeshazad1985@gmail.com

***Abstract*—** We know that security is the main challenge of the modern era, there may be many techniques and methods used for providing the security of any system or data. The biometric system is the widely used method for security. The biometric security is more secure method then others like passwords, card etc. In biometric the part of the body with some uniqueness use as the input image. But now a day the use of single biometric is not more secure, so the alternative or solution of this problem is to use the Multimodal biometric system. In a multimodal system more than one biometric trait used for providing security and authentication to a system. The images are stored in the database by using different operations on the images for compare it by input images. There are some steps used in processing of multimodal biometric system like as ROI, feature extraction and matching.

***Keywords*—** *Biometric, Multimodal system, ROI (Region of Interest) Extraction.*

*****

I. INTRODUCTION

Biometrics refers to the use of physical biometric or behavioral biometric characteristics to measure the uniqueness of an individual. The features that are extracted are unique of each individual and remain unchanged during the person's whole life. The biometrics is making by using these features to providing a solution to the world. The access to the safe area can be prepared by the use of ID or password which amounts to memory based security. But this type of information can be accessed easily by intruders and they can infringe the doors of security. The difficulty arises in case of economic transactions and extremely restricted information zone. Thus to prevail over the above given issue biometric security system are used. A biometric system is fundamentally a pattern recognition system that makes personal identification by determining the accuracy of a specific physical or behavioral biometric characteristic infatuated by the user. The biometric techniques are defined as the automated method of identify or authenticate the identity of a person based on a physical or behavioral biometric characteristic.

Biometric is the science and technology of evaluating and analyzing biological data. The technologies that used to measure and analyze human body characteristics, such as DNA, fingerprints, retinas and iris, voice patterns, facial patterns and hand measurements, for authentication purposes is known as the biometric system. Human iris is rich in features that can be used to authentication and positively distinguish one eye from another.

With the increasing importance of the security, there is need to guaranty that only authenticated users have authorized to use the system. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits present good performance. However, even the best biometric traits now a day facing numerous problems some of them are intrinsic to the technology itself. Biometric authentication systems generally suffer from enrolment problems because of non-universal biometric traits, insufficient accuracy caused by noisy image.

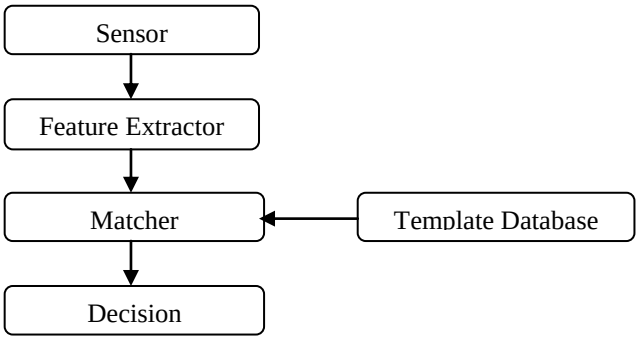

Figure1. Biometric authentication system

The fig1 shows the process of the biometric system which are used to identify or authentication. To use the biometric system first we need to take the biometric trait as input so we need sensor. After this process we extract the feature of the input image than perform matching with the image which is stored in the template database. The matching process decides that the user is authorized or not for granting the access.

II. BIOMETRIC CHARACTERISTIC

The biometric characteristic is mainly of two types one is physical biometric characteristic and other one is behavioral biometric characteristic. In the physical biometric characteristic fingerprint, face, hand geometry, iris, retina, vain, palm print, ear, DNA etc comes. On the other hand the behavioral biometric characteristic includes the signature dynamics, gait pattern, keystroke dynamics etc.

Figure2. Physical biometric characteristic

The figure1 shows the physical biometric characterictic. This biometric characteristic is the part of the human body that are different each other's by features and characteristic, and can be used for authentication and providing security of a system.

Figure3. Behavioral biometric characteristic

Figure2 shows the behavioral biometric characteristic. In the behavioral biometric characteristic the behavioral characteristic of any person measured for authentication like as voice of a person, gait pattern of any person, signature dynamics of a person and keystroke dynamics etc.

III. TYPES OF BIOMETRIC

A. Unimodal biometric system

The management of identity goes through the challenge of providing authorized users with secure and easy access of information over the variety of the networks. There are some traditional methods are used but they are not sufficient because of increasing the challenges of fake users. To overcome these problems biometric system takes place because of the way of providing security and accuracy [4]. The unimodal biometric system is a recognition system that uses the biometric trait to provide the security and personal recognition for any system. In the unimodal system only one biometric trait use like fingerprint, iris, retina, face, etc. for recognition. In the biometric system we use sensor to scan images for processing.

a. Limitation of Unimodal system

We know that the bometric unimodal system is more secure system than other security system but it has some limitations that's why we need to use the Multimodal biometric system. In the unimodal system only one biometric trait used so it can be eaisy to crack the security of unimodal system as compaired to the multimodal biometric system.

B. Multimodal biometric system

As the requirement of the security is increases the use of the biometric is also increases for more secure and accurate system. The multimodal biometric system is a new approach for identification and authentication [2]. In the multimodal biometric system we use multiple sensors that capture different biometric traits. There are different-different biometric features are used by these systems. Biometric systems that utilize more than one physical or behavioral characteristic for identification are known as multimodal biometric system. The multimodal biometric systems are proposed to be more reliable due to the use of multiple sensors

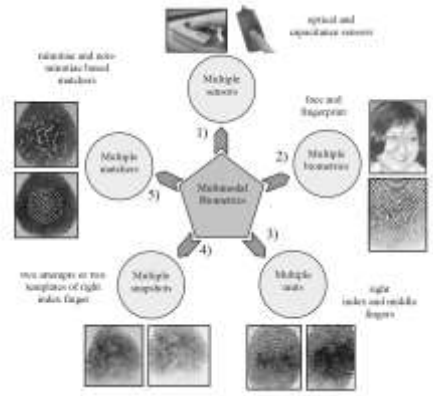

Figure4. Sensors used in a multimodal biometric system

Figure4 shows the multiple sensors that are used to take the image as input for authentication.

IV. PROPOSED MULTIMODAL BIOMETRIC SYSTEM

Here we proposed the multimodal biometric system that includes the iris, fingerprint and face images for processing.

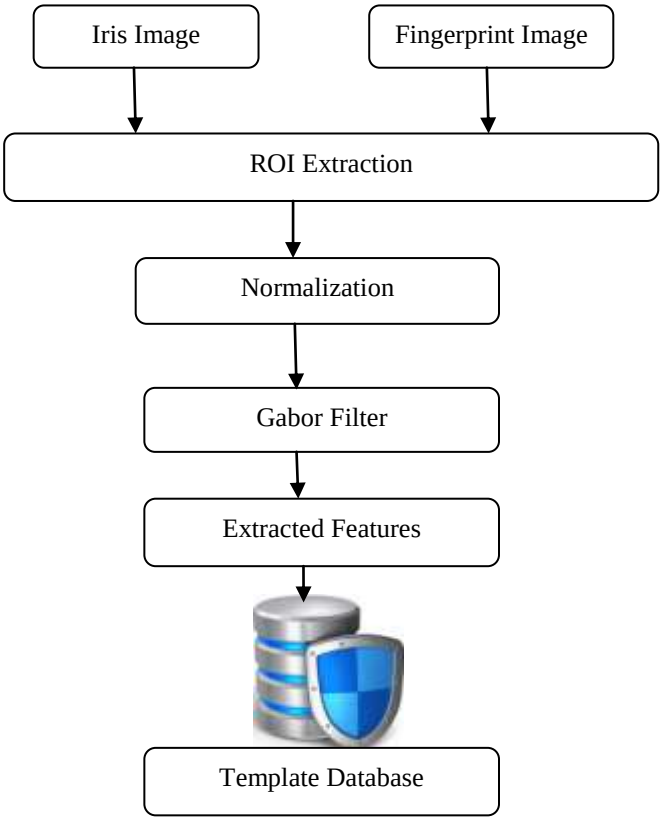

Figure5. Enrollment Module

Our proposed multimodal biometric system includes two types of modules Enrollment module and Matching or Identification module. The enrollment module includes the preprocessing stage and matching module includes matching stage.

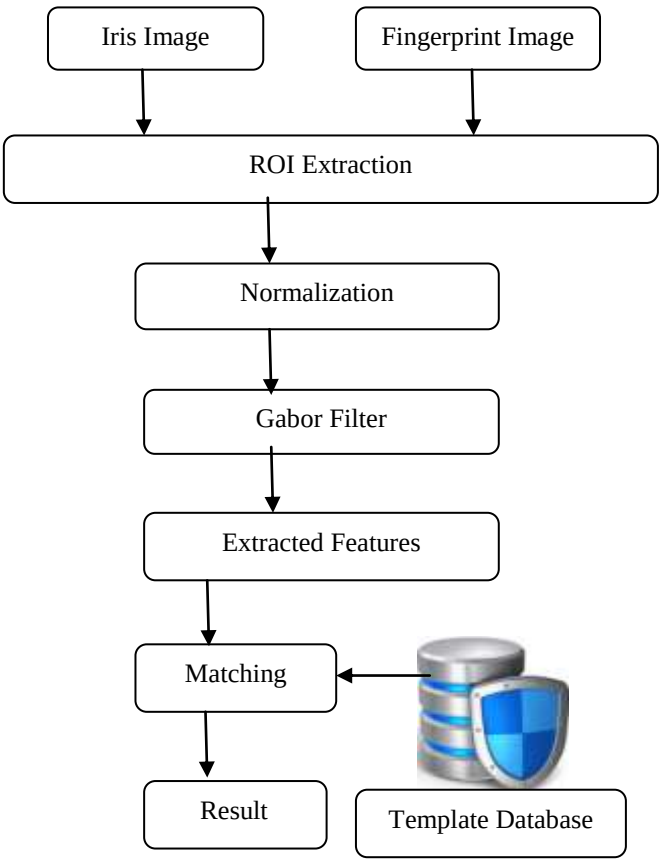

Figure6. Matching Module

A. ROI extraction :

The Region of Interest is the process of extracting the area of interest of given image. The ROI focuses on the center part of the image.

B. Normalization:

The images of iris and fingerprint of different people may have different size. The process of normalization must be performed after ROIs extraction. For a person biometric feature size may vary because of illumination changes during the iris acquisition phase or pressure variation during the fingerprint acquisition phase [5].

C. Gabor filter:

A Gabor filter is obtained by modulating a sinusoid with a Gaussian. For the case of one dimensional (1D) signals, a (1D) sinusoid is modulated with a Gaussian. These filters will there-fore respond to some frequency, but only in a localized part of the signal. For 2D signals such as images a (2D) sinusoid is modulated with a Gaussian. The Gabor filter can be de-fined as follows

$$\psi(x,y,\varpi,\theta)=\frac{1}{2\pi\sigma^2}e^{-\left(\frac{x'^2+y'^2}{2\sigma^2}\right)}[e^{i\varpi x'}-e^{\frac{\varpi^2\sigma^2}{2}}]$$

$$x'=x\cos\theta+y\sin\theta, y'=-x\sin\theta+y\cos\theta$$

…….. (1)

where (x, y) is the pixel position in the spatial domain, ω is the radial center frequency, θ is the orientation of Gabor filter and σ is the standard deviation of the round Gaussian function along the x- axes and y-axes. In addition, the second term of the Gabor filter compensates for the DC value because the cosine component has nonzero mean while the sine component has zero mean. Gabor filter bank with five frequencies and eight orientations is used to extract the Gabor feature for iris & fingerprint representation. The real part of the Gabor filters with five frequencies and eight orientations is shown in Fig.3. The Gabor feature representation of an image I(x, y) is the convolution of the image with the Gabor filter bank ψ(x, y, ωm, θn) as given by:

$$O_{m,n}(x,y)=I(x,y)*\psi(x,y,\varpi_m,\theta_n)$$

…… (2)

Where * denotes the convolution operator. The homogenous biometric vectors from fingerprint and iris data are made. But we understand that the time require for Gabor feature extraction is somewhat more and the dimension of Gabor feature vector is large. Then from homogenous biometric vector we generate fused template [1].

D. Extracted features:

The features are extracted by using Gabor filter of an image and can be stored in the template database

E. Matching:

The comparison is done between iris images and fingerprint images that are stored in database and query images [3]. This code of matching shows the result that the image is same or different. It also shows the percentage of the matching.

V. RESULT

In the enrollment process we have the database of iris and fingerprint that are downloaded from the internet the name of this database is UBIRIS and FINGERPRINT. This database is password protected. We get the password from the user by the mail. We take the image from database for the processing first we calculate the Region of Interest of both the images iris and fingerprint. After the ROI extraction the normalization is performed because the different people have the different iris & fingerprint size. The Gabor filter performed on the input image after the normalization process. The Gabor filter extracts the features then it stored in the template database for the matching with the input image and it shows the result.

 ISSN: 2321-8169
6308 - 6312

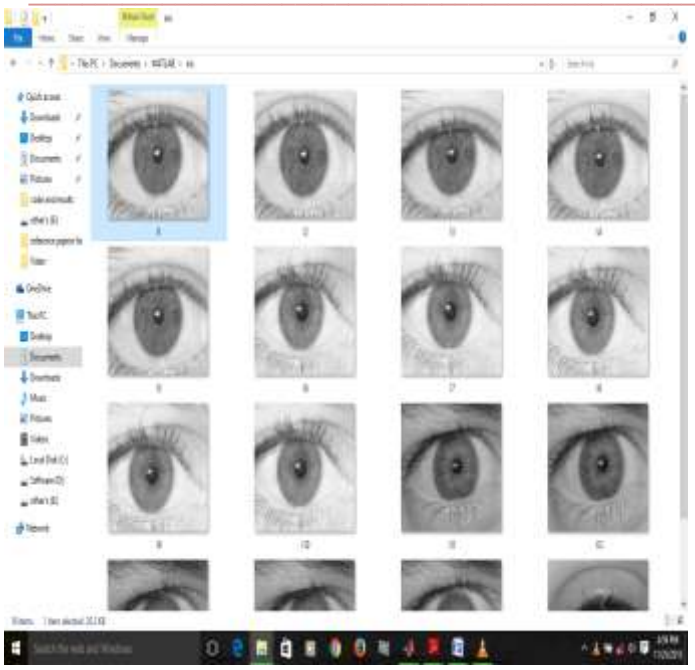

Figure7. Iris Images

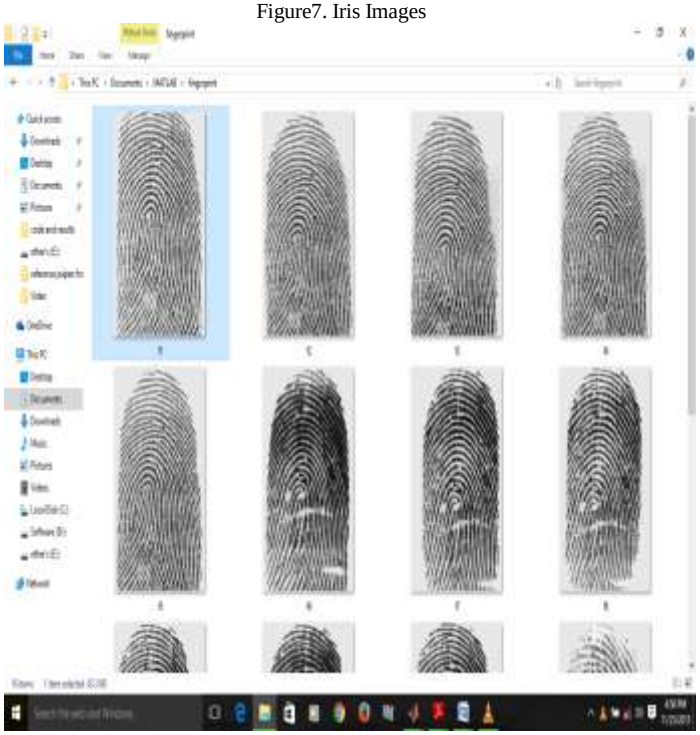

Figure8. Fingerprint Images

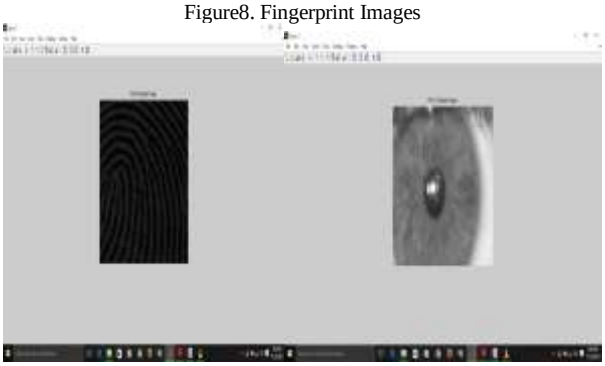

Figure9. ROI of fingerprint & iris

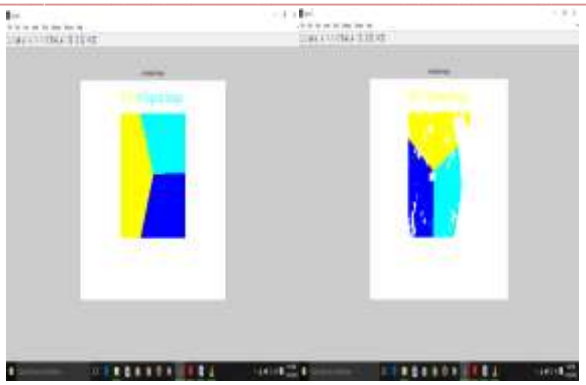

Figure10. Normalization of fingerprint & iris

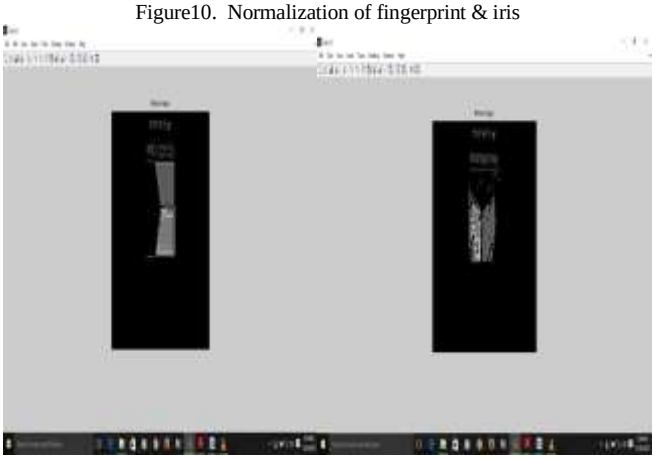

Figure11. Gabor filter of fingerprint & iris

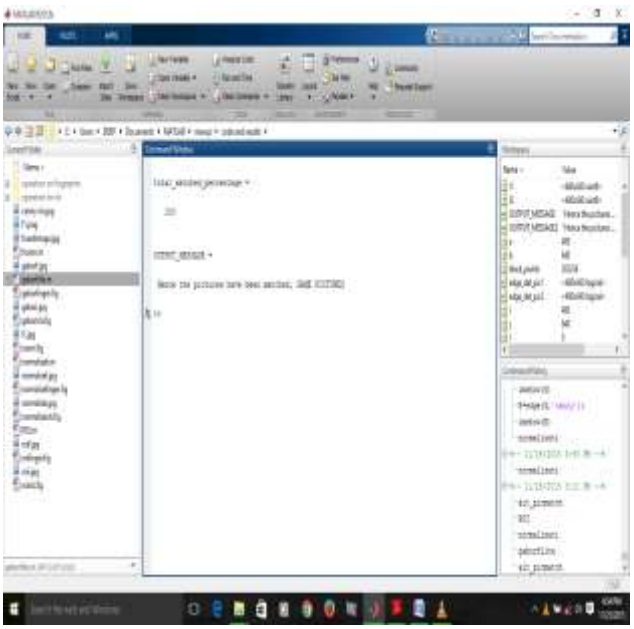

Figure12. Matching

VI. CONCLUSION

This paper shows the biometric multimodal system is the security system. In this paper we study about the fingerprint and iris for providing the security of a system by authentication. The authentication is done by matching algorithm. The future work of this is that the security can be increased by using three biometric traits.

VII. REFERENCES

[1] Lahane P.U., Prof. Ganorkar R.S., "*Fusion of Iris & Fingerprint Biometric for Security Purpose*", International Journal of Scientific & Engineering Research, August-2012.

[2] Randive S. D., Patil M.M., "*Iris and Fingerprint Fusion for Biometric Identification* ",International Journal of Computer Applications, September 2013.

[3] Gawande1 G., Sapre2 A, Jain3 A., Bhriegu4 S., Sharma5 S. ," *Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance Matcher* ", International Journal of Engineering Inventions, February 2013.

[4] Abate F.A., Nappi M., Daniel Riccio, Gabriele Sabatino, "*2D and 3D face recognition: A survey*", Elsevier, January 2007.

[5] Lahane P.U., Prof. Ganorkar R.S, "*Efficient Iris and Fingerprint Fusion for Person Identification* ", International Journal of Computer Applications, July 2012.