Identification of biometrics System for feature extraction of Iris and fingerprint

CHHAYA S.KHANDELWAL[1], RANJAN MAHESHWARI[2], ULHAS SHINDE[3]

1. *Assistant Professor,* 2.Professor, 3. Principal,

Department of Electronics and Telecommunication,

MGM,s Jawaharlal Nehru Engineering College,Aurangabad,(M.S.), 431005, India [1]

Abstract : This paper presents fusion of two biometric traits, i.e., iris and fingerprint, at matching score level architecture The features are extracted from the pre-processed images of iris and fingerprint. These features of a query image are compared with those of a database image to obtain matching scores. The individual scores generated after matching are passed to the fusion module. The biometrics system is a pattern recognition system that is used for a verifying individual using different biometric traits. For authentication system, one biometrics modality may not satisfy the properties such as accuracy, precision, and sensitivity. To overcome this problem we use multimodal biometrics.Multimodal biometrics means using multiple sources of information. In this paper, we use two biometrics traits such as fingerprint and iris. In terms of methodology, we propose using principal component analysis and linear differential analysis techniques and minutiae for feature extraction of iris and fingerprint traits. Afterword, we use rank level fusion.

Index Terms: Multimodal biometrics, PCA, LDA, Iris recognition, Fingerprint recognition, Rank level fusion.

I. INTRODUCTION

Biometrics is the science and technology of measuring Analysis of biological data. In information technology, biometrics refers Techniques that measure and analyze the human body Features, such as DNA, fingerprints, eye retina and irritation,For voice patterns, face patterns and hand measurements, Purposes of authentication.Biometrics proposes a new key that is user-friendly, intelligent and reliable for an individual Validation system using human iris pattern. In fact, no two irises are the same in the world. However, identical twins have the same DNA, forming their tissue structure.Different iris patterns. Each iris is unique because a completely random process during the embryo Evolution makes it. Even a person's left and right eyes have completely different iris patterns. Therefore, it can also be used as a kind of live password. Biometrics is an authentication mechanism that depends based on automatic identification or verification Unique physical or person based Behavioral characteristics.Biometric systems can be classified into two typesNamely, unimodal and multi-modal biometric systems.An unimodal biometric system is one in which only A..A type of component components exists.Whereas, more than multi-modal biometric systems A type of component exists. Arun Ross [2].The advantages of using multimodal biometric [2] are

1.It addresses the issue of non-universality Encountered by uni-biometric systems.

2. It becomes an increasingly difficult to A validly exaggerating multiple biometric symptoms nominated person.

3. Address the problem of noise data effectively. If Single property is contaminated with noise,Availability of other symptoms may help in reliable Determination of identity.

4. It is a fault tolerant system and continues to operate Even when some become biometric sources Unreliable due to sensor or software malfunction, Or intentional user manipulation.

5.Multi-biometric systems can facilitate filtering Or indexing large-scale biometric databases.

6. These systems can also help in continuous Monitoring or tracking a person Conditions when not a single symptom is sufficient.

The biometric system has the following two modes of operation:

Enrollment Mode: In this mode the system receives stores user's biometric and required data received from people in database. In the template is tagged with the user's identity Authentication facility

Authentication Mode: It also receives mode the person's biometric and uses to verify it Identity claimed.

As a result, there is also a growing need for technology assessment evaluation. And benchmarking, depending on Availability of biometric data. Biometric databases allow us To define evaluation protocols and strategies, so that Research community may follow common assessment Procedures. In this way, we can get comparativeMeasures are often expressed as lies Acceptance and False Rejection Rate (FAR and FRR).

2.Literature survey

Multimodal technology is not new to the medical world. Regular and confirmatory examination is also often preferred in regular medical checkups. Incorporating evidence from more than one source will increase the overall accuracy of the system. [15]

Table 1. Literature Survey

Author	Biometric Modalities	Level of fusion	Accuracy reported
A. Muthukumar et al. [4]	Iris and fingerprint	Score fusion	95.5%
Vincenzo Conti et al. [5]	Fingerprint and iris	Feature level fusion	96%
Sumit Shekhar, et al. [6]	Iris, fingerprint, and face	Sparse matrices	97.5%
Abhishek Nagar et al. [7]	Iris, fingerprint, and face	Feature level fusion	97%
Robert Snelick et al. [8]	fingerprint, face	Simple-Sum fusion	95.5%

3.Materials and Methods:-

A simple biometric system has four basic components: A simple biometric system has four basic components:

1) sensor module that receives biometric data;

2) Feature extraction modules are processed to extract feature vectors;

3) matching modules where query images are compared with nomination templates;

4) Decision-making module in which the identity of the user is accepted or rejected.

Any human physical or behavioral characteristic can serve as a biometric facility as long as it does not meet the following requirements [1] [3] [9]

Block diagram of multimodal biometrics. In multimodal biometrics, we have used two methods 1) fingerprint 2) iris characteristics
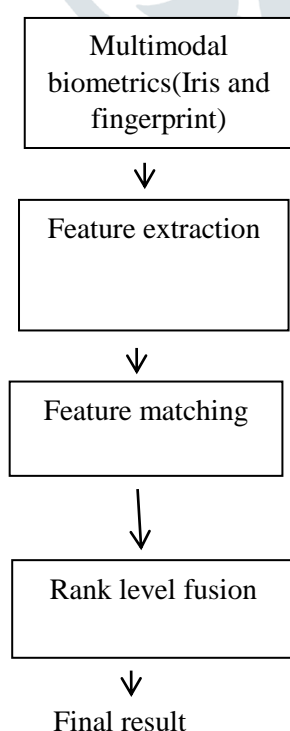
Multimodal biometrics(Iris and fingerprint)

↓

Feature extraction

↓

Feature matching

↓

Rank level fusion

↓

Final result

Figure 1: Multimodal biometrics

Preprocessing of fingerprint:We collected live data from the computer science department to improve image quality and then performed preprocessing on the fingerprint image.

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 a person. Fingerprint is basically a combination of ridges and valleys on the surface of the finger

The main steps in the proposed algorithm include

1) captured the fingerprint image using the Futronic FS88.

2) Histogram of image.

3) Threshold the image

4) adaptive binarization

5) Area of interest (ROI)

6) Facility extraction using Minutia

7) Matching is done using an edge.

The fingerprint image is corrupted due to various types of noise such as creases, smudges and holes. It is almost impossible to recover real ridge / valley formations from erosive areas; Any attempt to improve fingerprint image quality in these areas may be futile.Therefore, any well-known enhancement algorithm can be used to improve the clarity of streak / valley structures of fingerprint images in recoverable areas and to exclude extraneous regions.The enhanced fingerprint image is binarized and stored in a thinning algorithm that reduces the thickness of the ridge to one pixel wide. The skeletal image is used to extract minutiae points that are ridge endings and points of bifurcation. The minutiae points along the orientation are taken out and stored to set the form.The enlarged fingerprint image is binarized and stored in a thinning algorithm that reduces the thickness of the ridge to one pixel wide. The skeletal image is used to extract minutiae points that are ridge endings and points of bifurcation. Minutiae points with orientation are taken out and stored to set the form. Matching is done using edge.

We can find out Recall, Precision, Specificity, and f_score using the following formula.
Recall=tp/(tp+fn)
Precision:
speficity=tn/(fp+tn);
precision=tp/(tp+fp);
F-score: The harmonic mean of precision and recall(sensitivity)
f_score=2*tp/(2*tp+fp+fn)

Preprocessing of Iris :: We collected live data from the Department of Computer Science. Then captured the image using Eye Scan 2 Cross Match Technologies Inc.

Iris is unique to each person and remains constant over a person's life. The eyeball has a round black disk known as the pupil. The pupil becomes weak when exposed to light and shrinks into darkness. Thus the size of the pupil varies with respect to light and it comes into contact with it. The iris is the annular ring between the sclera and pupil border and has a floral pattern unique to each individual.

The main steps in the proposed algorithm include
1) Capture the image
2)Localize the image
3)Normalized the image
4)Enhancement of image
5)Feature Extraction
6)Feature Extraction after PCA,ICA and LDA ,

Principal Component Analysis

The PCA is mostly used as a tool in exploratory data analysis and predictive model making purpose. It can be done by eigenvalue decomposition of a data correlation matrix. The normalization of each attribute consists of mean centering – subtracting each data value from its variable's measured mean so that its empirical mean (average) is zero and, possibly, normalizing each variable's variance to make it equal to1.PCA is mathematically defined as an orthogonal linear transformation that transforms the data to a new coordinate system such that the greatest variance by some projection of the data comes to lie on the first coordinate (called the first principal component), the second greatest variance on the second coordinate, and so on.

Linear Discriminator Analysis (LDA), also known as Fisherface, is an appearance-based technique that is used for dimensionality reduction and has demonstrated great performance in facial recognition..PCA (Turk and Pentland, 1991) finds a set of the most representative projection vectors such that the projected samples retain most information about original samples. ICA (Bartlett et al., 2002; Draper et al., 2003) captures both second and higherorder statistics and projects the input data onto the basis vectors that

are as statistically independent as possible. LDA (Belhumeur et al., 1996; Zhao et al., 1998) uses the class information and finds a set of vectors that maximize the between-class scatter while minimizing the within-class scatter.

Fusion in multimodal biometrics

In a multimodal biometric system, after the enrollment phase, the images are average and normalized and then given to its matching phase in which the features are matched and then it is ranked according to the availability of data and the results are obtained. Later, we add both methods using the rank mode fusion.
Fusion

Rank-level fusion is a relatively new fusion approach. When the production of each biometric match is a subset of possible matches sorted in decreasing order, then fusion can be done at the rank level. The aim of the rank level fusion is to consolidate the rank output by the individual biometric subsystem (matchers) so that consensus rank can be obtained by using three methods to combine the ranks determined by different matchers for each match. [14].
 1. The Highest Rank Method,
2. The Borda Count Method and
3. The Logistic Regression Method.
In the highest rank method, each possible match is assigned the highest (minimum) rank, as computed by different matchers.
The Borda count method uses the sum of the ranks assigned by individual matchers to calculate the final rank.
 In the logistic regression method, a weighted sum of the individual ranks is calculated. The weight to be assigned to different matchers is determined by logistic regression.[7][15]
Experimental Results

After applying feature extraction technique on fingerprint and iris.the combined images of both are used as input of rank level fusion for getting the final outputs.

Table 2: Performance parameter

Traits	Recall	Precision	Specificity	F-score
Fingerprint	0.9553	0.9605	0.9942	0.9576
Iris	0.8681	0.8762	0.9823	0.8712

Conclusion

 In unimodal biometrics was less accurate in various parameter to fulfill the identification, security and privacy problems. To overcome this problem we use multimodal biometrics. In which we used a fingerprint and iris images to develop a highly secure and accurate system. The accuracy of iris and fingerprint is 87.21%   and 95.79%. and combining using rank level fusion there get 99.72%. In future research work on multiple parameters such as Iris, fingerprint using a high-resolution camera.

Acknowledgments

References

[1]Kresimir Delac 1, Mislav Grgic 2, A survey of biometric recognition methods, 46th International Symposium Electronics in Marine, Elmar-2004, 16-18 June 2004; Zadar, Croatia

[2]Arun Ross, (2007). "An Introduction to Multibiometrics", Proceedings of the 15th European Signal Processing Conference (EUSIPCO), Poznan, Poland.

[3]. Anil Jaina, Karthik Nandakumar, Arun Ross, Score normalization in multimodal biometric systems, Pattern Recognition 38 (2005) 2270– 2285, accepted18 January 2005

[4].A. Muthukumar1, C. Kasthuri2, and S. Kannan3, Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris, ICTACT Journal on Image and video processing, February 2012, volume: 02, Issue: 03

[5]. Vincenzo Conti, Carmelo Militello, Filippo Sorbello, Member, IEEE, and Salvatore Vita bile, Member, IEEE, A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems, IEEE Tractions on the system, Man, and. cybernetics— part C: Application and Reviews, vol. 40, no. 4, July 2010

[6]. Sumit Shekhar, Student Member, IEEE, Vishal M. Patel, Member, IEEE Nasser M. Nasrabadi, Fellow, IEEE, and Rama Chellappa, Fellow, IEEE, Joint Sparse Representation for Robust Multimodal Biometrics, IEEE Tractions on pattern analysis and Machine Intelligence, vol. 36, no. 1, January 2014.

[7]. Abhishek K. Nagar, Student Member, IEEE, Karthik Nandakumar, Member, IEEE, and Anil K. Jain, Fellow, IEEE, Multibiometric Cryptosystems Based on Feature-Level Fusion, IEEE Tractions on Information Forensics and Security, vol.7, no.1, February 2012.

[8]. Robert Snelick1, Umut Uludag2*, Alan Mink1, Michael Indovina1, and Anil Jain2 Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems IEEE Transactions on Pattern Analysis and Machine Intelligence Vol. 27, No. 3, Mar2005, pp 450-455.

[9]. Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE, An Introduction to Biometric Recognition, IEEE Transactions on circuits and systems for Video Technology, Vol.14, No.1, January 2004.

[10]. C. Sanderson, K.K. Paliwal, Information fusion and person verification using speech and face information, Research Paper ID IAP-RR 02-33, IDIAP, September 2002.

[11]. U. M. Bubeck and D. Sanchez, Biometric authentication: Technology and evaluation, San Diego State Univ., San Diego, CA, 2003. Tech. 9.Rep.

[12]. Md.Maruf Monwar, and Marina L. Gavrilova, the unimodal biometric system using Rank Level Fusion Approach, IEEE Transactions on System, Man and Cybernetics – Part B: Cybernetics, Vol.39, No.4, August 2009.

[13]. M. P. Down and R. J. Sands, "Biometrics: An overview of the technology, challenges, and control considerations," Inf. Syst. Control J., vol.4, 2004; pp. 53– 56

[14]. S. Prabhakar, S. Pankanti, A. K. Jain, Biometric Recognition: Security and Privacy Concerns, IEEE Security & Privacy, March/April 2003; pp. 33-42.

[15]..A.Muthukumar1, C. Kasthuri2, and S. Kannan3, Multimodal Biometric Authentication using Particle Swarm Optimization Algorithm with Fingerprint and Iris, ICTACT Journal on Image and video processing, February 2012, volume: 02, Issue: 03

[16]. C.S Khandelwal, R Maheshwari, U.B. Shinde," Review paper on applications of principal component analysis in multimodal biometrics system"Procedia Computer Science 92, 481-486.

[17], L. Flom, & A. Safir, Iris Recognition System, U.S. Patent No. 4641394, 1987.