Volume 5, Issue 5, May 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Biometric Authentication System for Multimodal Descriptors using Face, Iris & Finger

Hardeep Bhangu
Research Scholar
Indo Global College of Engineering
India

Hemlata Rauthan
Assistant Professor
Indo Global College of Engineering
India

Abstract: Biometrics refers to metrics related to human characteristics Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. Biometric authentication system utilizes various biometric traits for the matching between various biometric traits. Various approaches have been used for the extraction of features from various types of biometric traits. In this paper biometric traits utilize are face, fingerprint and iris. Single Biometric trait system is failed to provide accuracy for the authentication of different identities because due to single biometric trait the chances of mismatching increases.

Keywords: Biometric, Multimodal, 2-DPCA, Morphological Operators and Fusion

I. INTRODUCTION

1.1 Biometric

Humans have used body characteristics such as face, Finger, Iris, voice, gait, etc. for thousands of years to recognize each other. Biometrics refers to metrics related to human characteristics Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice. Some researchers have coined the term behavior metrics to describe the latter class of biometrics.

Any human physiological and/or behavioral characteristic can be used as biometric characteristics long as it satisfies the following requirements:

Universality: each person should have the characteristic;

•Distinctiveness: any two persons should be sufficiently different in terms of the characteristic;

•Permanence: the characteristic should be sufficiently
Invariant (with respect to the matching criterion) over a period of time;

•Collectability: the characteristic can be measured quantitatively. However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a numberof other issues that should be considered, including:

•Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed;

•Acceptability, which indicates the extent to which people are willing to accept the use of a
Particular biometric identifier (characteristic) in their daily lives;

•Circumvention, which reflects how easily the systemcan be fooled using fraudulent methods.

A practical biometric system should meet the specified recognition accuracy, speed, and resourcerequirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

Fig 1.1: Biometric

1.2 Multimodal Biometric System

Multimodal biometric systems use multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance iris recognition systems can be compromised by aging rides and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken pass-code).Multimodal biometric systems can integrate these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refer to sequential, parallel, hierarchical and serial integration modes, respectively. Broadly, the information fusion is divided into three parts, pre-mapping fusion, midst-mapping fusion, and post-mapping fusion/late fusion. In pre-mapping fusion information can be combined at sensor level or feature level.

Sensor-level fusion can be mainly organized in three classes: (1) single sensor-multiple instances, (2) intra-class multiple sensors, and (3) inter-class multiple sensors.

Feature-level fusion can be mainly organized in two categories: (1) intra-class and (2) inter-class. Intra-class is again classified into four subcategories: (a) Same sensor-same features, (b) Same sensor-different features, (c) Different sensors-same features, and (d) Different sensors-different features.

1.3 Fusion in biometrics

In the biometric fusion three possible levelsof fusions are: (a) fusion at the feature extractionlevel, (b) fusion at the matching scores level, (c)fusion at the decision level.

(1) Fusion at the feature extraction level: The dataobtained from each sensor is used to computea feature vector. As the features extracted fromone biometric trait are independent of thoseextracted from the other, it is reasonable toconcatenate the two vectors into a single new vector. The newfeature vector now has a higher dimensionality and represents a person Nonidentity in a different (and hopefully more discriminating) hyperspace. Feature reduction techniquesmay be employed to extract useful featuresfrom the larger set of features.

(2) Fusion at the matching scores level: Each system provides a matching score indicating theproximity of the feature vector with the template vector. These scores can be combinedto assert the veracity of the claimed identity. Techniques such as logistic regression may beused to combine the scores reported by thetwo sensors. These techniques attempt to minimize the FRR for a given FAR (Jain et al., 1999b).

(3) Fusion at the decision level: Each sensor cancapture multiple biometric data and the resulting feature vectors individually classified intothe two classes—accept or reject. A majorityvote scheme, such as that employed in (Zuev and Ivanon, 1996) can be used to make thefinal decision.

Fusion in the context of biometrics can take the

Following forms:
(1) Single biometric multiple representation.
(2) Single biometric multiple matchers.
(3) Multiple biometric fusions

1. Single Biometric Fusion

Single biometric multiple matchersIt is also possible to incorporate multiplematching strategies in the matching module of abiometric system and combine the scores generated by these strategies.

2. Multiple biometric fusions

Multibiometric fusion refers to the fusion ofmultiple biometric indicators. Such systems seek toimprove the speed and reliability (accuracy) of abiometric system (Hong and Jain, 1998) by integrating matching scores obtained from multiplebiometric sources.

II. LITERATURE REVIEW

Lone, M.A. [1], According to this paper, For upgrading the execution and precision of biometric face distinguishment framework, author utilize a multi-algorithmic methodology, where in a blend of four distinctive individual face distinguishment systems is utilized. In this paper, author creates a face recognition systems focused around one mix of four individual strategies in particular Principal Component Analysis (PCA), Discrete Cosine Transform (DCT), Template Matching utilizing Correlation and Partitioned Iterative Function System (PIFS). They intertwine the scores of these four systems in a solitary face recognition framework. They perform a relative investigation of face distinguishment rate of this face recognition system at two accuracy levels specifically at Top-5 and at Top-10 Ids. They explore it with a standard ORL face database. Tentatively, authors find that distinguishment rate by PCA-DCT system is superior to by individual PCA and DCT procedures and distinguishment rate by PCA-DCT-Corr method is superior to the PCA-DCT strategy. By and large, we discover the framework focused around mix of the majority of the four individual strategies outflanks.

Patil, N.K. [2], According to this paper, This paper proposes a novel strategy for face recognition utilizing de-relationship of neighborhood peculiarities utilizing Discrete Wavelet Transforms (DWT) which enhances the distinguishment precision. It additionally keeps away from generalizability issue which is brought about because of subspace discriminant investigation or factual learning system by utilizing a non-measurable strategy which abstains from preparing venture for face tests. This proposed system performs well with pictures with halfway impediment and pictures with lighting varieties as the neighborhood patch of the face is isolated into a few diverse patches.

Vasudha, S. [3], This paper proposes a novel strategy which enhances the distinguishment precision and additionally stays away from face datasets being altered through picture joining procedures. It likewise maintains a strategic distance from generalizability issue which is brought about because of subspace discriminate examination or factual learning technique by utilizing a non-measurable method which abstains from preparing venture for face tests. This proposed strategy performs well with pictures with incomplete impediment and pictures with lighting varieties as the nearby fix of the face is isolated into a few distinctive patches. The execution change is indicated extensively high as far as distinguishment rate and storage room by putting away prepare pictures in packed area and selecting critical gimmicks from superset if characteristic vectors for genuine distinguishment.

Harsha, P. [4], the proposed framework comprises of three fittings modules: picture securing module, installed primary board, and human machine correspondence module. The structure chart of the system is, the picture securing module is utilized to gather finger-vein pictures. The Embedded principle board including the Microcontroller chip, memory (blaze), and correspondence port is utilized to execute the finger-vein distinguishment calculation and speak with the fringe gadget. The human machine correspondence module (LED or console) is utilized to show distinguishment results and get inputs from clients. Their proposed framework is savvy security framework. Here they created teller machine idea. On the off chance that finger vein matched, implies exchange fruitful through GSM engineering.

Meraoumia, A. [5], In this paper, FP and FKP are incorporated with a specific end goal to build an effective multi-biometric distinguishment framework focused around matching score level and picture level combination. In this study they utilize the base normal connection vitality (MACE) and Unconstrained MACE (UMACE) channels in conjunction with two relationship plane execution measures, max top esteem and crest to-side lobe degree, to focus the adequacy of this strategy. The trial results demonstrated that the composed framework accomplishes an excellent recognition rate on the Hong Kong polytechnic college (Polyu) FKP and high determination finger impression database.

III. PROBLEM FORMULATION

The pursuits of knowledge on the diverse biometric system envisage single biometrics feature is not sufficient to provide secure authentication. This dictates the importance of multi-modal system. Most of the multi-modal techniques are lacking in security aspect. Previous work presented the feature level fusion scenario with face and fingerprint modalities, using Gabor filter bank to extract the features individually but still this work is lacking in some another way like this is not used for low resolution images. By using this filter time complexity increases because size increases. Their features properties are also not properly define due to which it not give proper acceptance.

IV. METHODOLOGY

Biometric system utilize in various system for the identification or authentication approval. Biometric authentication system utilizes various biometric traits for the matching between various biometric traits. Various approaches have been used for the extraction of features from various types of biometric traits. In the proposed work the biometric traits utilize are face, fingerprint and iris. In this proposed work face features has been extracted by using 2DPCA (2-dimensiional principal component analysis). This method utilizes Eigenface for the extraction of various features from face image database. The feature dimension reduces due to horizontal and vertical calculation of Eigen values. Feature from finger database is extracted by using extraction of rigid and bifurcation minutiae extraction approach. Fingerprint image is firstly converted into binary form by using converter image to binary. After conversion various bio-morphological operations has been implemented to binary image. These operations are thinning, cleaning, H-break and spur. These operations normalize the image and then bifurcation and rigid extraction function has been implementing on normalized image. On the basis of the bifurcation and rigid minutiae from the image has been extracted and stored in a template for template matching in verification process. Next trait which is utilized in the proposed system is iris. Iris images have been taken from different databases and extracted features on the basis of circle iris and circle pupil. These features extracted from iris image have been used for person matching. Approach utilized for iris feature extraction is phase coding method. After extraction of feature from all types of biometric traits utilize fusion of all these feature vector has to be done for development of a single vector containing feature of all these three components. Two types of fusion approaches has been utilized for this purpose one is score level and another is rank level. In our proposed work score level fusion approach has been used for the fusion purpose. After fusion data base image has been used for feature extraction and fused and stored in a file with name id and feature values to the dataset. Same process has been implemented on the various test images for matching or authentication approval of person. After matching accuracy, FAR and FRR has been computed for performance evolution.

V. RESULTS

The biometric field comprise various techniques for the purpose of feature extraction from various biometric traits. These features has been extracted by firstly normalize the image of biometric field and then these features has to be extracted. Various tools have been used for processing of these biometric traits. These features has are in the form of numerical values computed from different images related to biometric trait databases. In this simulation 10 images has been used for training of the proposed system on the basis of different features and the simulation results of this work are described below.

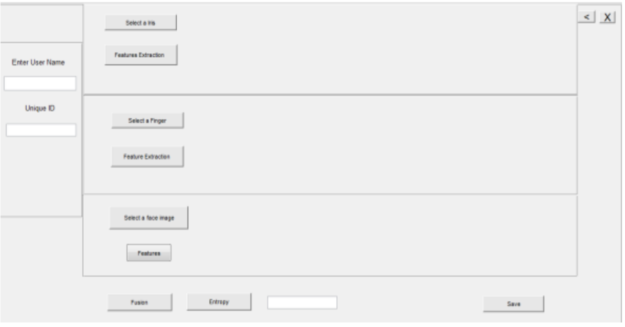


Figure 5.1: GUI for training the data

In this we create the database on the basis of Face, Finger and Iris. This graphical user interface contains the buttons and textboxes to perform various operations for the creation of database. These controls available on this graphic user interface provide help to perform various types of operations on different images. These buttons use various function for performing desired functioning.

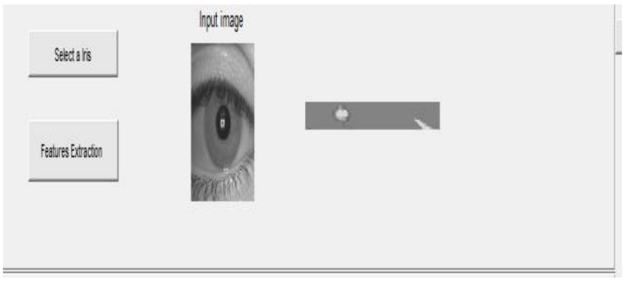


Figure 5.2: Input Iris Image for feature extraction

Feature extracted from iris image by using circle iris, circle pupil and phase coding extraction scheme. These features have been extracted by computing circle co-ordinates of pupil and iris of the image. The radii and angular divisions have been described on the basis of these parameters features from these iris images has to be extracted.

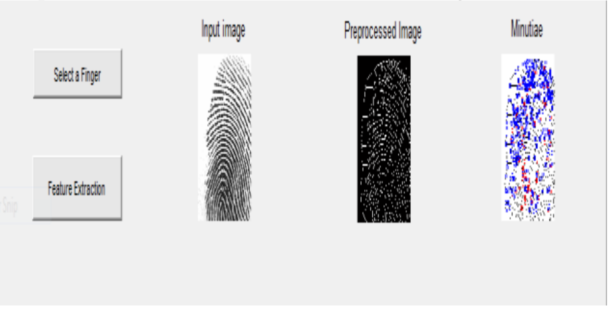
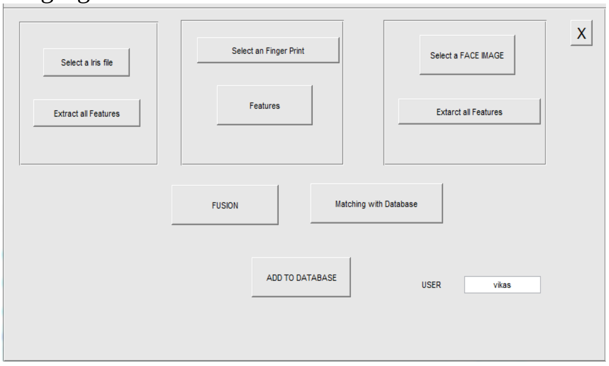


Figure 5.3: Input Finger Image for feature extraction

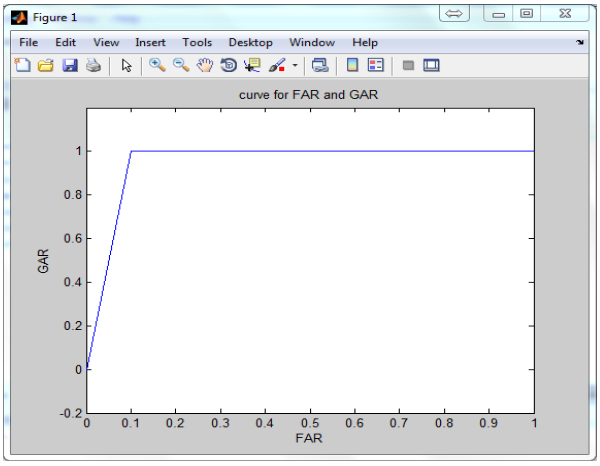
Pre-processing by using morphological operation of thinning like cleaning, h breaks etc. These morphological operations provides a pre-processed image on the basis of different operations utilized for different proposed. The feature of these fingerprints can be extracted by using rigid and minutiae extraction scheme.



USER vikas

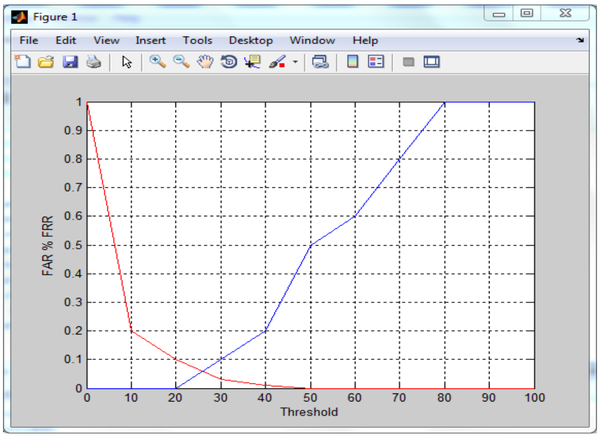
Figure 5.4: Match with database

This figure is used to represent the distance classification done with the database on the basis of different distance classifier. This classifier computes the distance between the different features of database images and to the query image features. These features described the similarity between different biometric traits. Where the minimum distance has been computed that is most matched feature vector. From that particular feature vector name of the identity is fetched out.



Graph 5.5: Genuine Acceptance Rate

This graph is use to represent the percentage of acceptance or we can say that is use to measure the accuracy.



Graph 5.6: FAR & FRR Percentage

This graph is use to represent the reliability of a system. Reliability is defined as the amount of time in which our system works properly.

Table 5.1 Comparison table for various approaches

Approach	FAR	FRR	GAR
Finger Print	1.762	2.5	97.5
Face	13.55	13.75	86.25
Fingerprint + Face	0.35	0.75	99.25
Finger + Face + Iris	0.20	0	100

This table represent the value of FRR (False Rejection Rate), FAR (False Acceptance Rate) and GAR (Genuine Acceptance Rate). This table represent the values of the parameters for different approaches used in biometric authentication system.

VI. CONCLUSION

Biometric system utilize in various system for the identification or authentication approval. Biometric authentication system utilizes various biometric traits for the matching between various biometric traits. Various approaches have been used for the extraction of features from various types of biometric traits. In the proposed work the biometric traits utilize are face, fingerprint and iris. Single Biometric trait system is failed to provide accuracy for the authentication of different identities because due to single biometric trait the chances of mismatching increases. So to overcome these disadvantages of single trait biometric system, multimodal biometric system come into existence. Computation speed increases due to reduction in feature dimension of fused features. This proposed system provides accuracy of 100%. This provides better security than other biometric system because illegal availability of all the traits of single person is not available to match and perform any illegal operation. So one can conclude that multimodal biometric system provides better result as compare to single biometric trait system.

REFERENCES

[1] Lone, M.A.Rajouri, Zakariya, S.M., Ali, R. "Automatic Face Recognition System by Combining Four Individual Algorithms" published in International Conference on Computational Intelligence and Communication Networks (CICN), 2011, pp 222-226.

[2] Patil, N.K., Belgaum, Vasudha, S. ; Boregowda, L.R. "Performance Improvement of Face Recognition System by Decomposition of Local Features Using Discrete Wavelet Transforms" published in International Conference on Electronic System Design (ISED), 2013, Pp 172 – 176.

[3] Vasudha, S., Patil, N.K., oregowda, L.R. "Rule based features selection for the performance improvement of face recognition system" published in International Conference on Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), 2013, Pp 1-6.

[4] Harsha, P. ; Subashini, C "A real time embedded novel finger-vein recognition system for authenticated on teller machine" published in International Conference on Emerging Trends in Electrical Engineering and Energy Management (ICETEEEM), 2012,pp 271 – 275.

[5] Meraoumia, A.,Chitroub, S. ; Bouridane, A. "Multimodal biometric person recognition system based on fingerprint & Finger-Knuckle-Print using correlation filter classifier" published in International Conference on Communications (ICC), 2012 IEEE, pp 820-824.

[6] Sharma, V.P.,Mishra, S.K. ; Dubey, D. "Improved Iris Recognition System Using Wavelet Transform and Ant Colony Optimization" published in 5th International Conference on Computational Intelligence and Communication Networks (CICN), 2013, pp 243 – 246.

[7] Aydi, W., Sfax, Tunisia ; Fadhel, N. ; Masmoudi, N. ; Kamoun, L. "A robust feature extraction method based on monogenic filter for iris recognition system" published in International Conference on Computer Applications and Information Systems (WCCAIS), 2014, pp 1-4.

[8] Nithyanandam, S,_ Amaresan, S., Haris, N.M., "An innovative normalization process by phase correlation method of Iris images for the block size of 32∗32" *Fifth International Conference on Applications of Digital Information and Web Technologies (ICADIWT), 2014,* pp. 189 – 194.

[9] Harder, S., Clemmensen, L.H.; Dahl, A.L. ,Andersen, J.D. "Correlation of iris biometrics and DNA" *International Workshop on Biometrics and Forensics (IWBF), 2013* ,pp. 1 – 4

[10] Joshi, A., Gangwar, A.K. Saquib, Z. "Person recognition based on fusion of iris and periocular biometrics" *12th International Conference on Hybrid Intelligent Systems (HIS), 2012* ,pp. 57 – 62.

[11] Connaughton, R. Sgroi, A. ; Bowyer, K.W. ; Flynn, P. "A cross-sensor evaluation of three commercial iris cameras for iris biometrics*" IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), 2011* ,pp. 90 – 97.

[12] Woodard, D.L., Pundlik, S. Miller, P. ; Jillela, R. "On the Fusion of Periocular and Iris Biometrics in Non-ideal Imagery" *20th International Conference on Pattern Recognition (ICPR), 2010,*pp. 201 – 204.

[13] Fernandez-Saavedra, B., Liu-Jimenez, J. ; Sanchez-Avila, C., "Quality Measurements for Iris Images in Biometrics*". The International Conference on &#34, 2007,* pp. 759 – 764.

[14] Rathgeb, C. "On application of bloom filters to iris biometrics" pp. 207 – 218, vol. 4, IEEE, 2014.

[15] Kanade, S. , Camara, D. ; Krichen, E. ; Petrovska-Delacrétaz, D. "Three factor scheme for biometric-based cryptographic key regeneration using iris" *Biometrics Symposium, 2008,* pp. 59 – 64.