© 2016 IJSRSET | Volume 2 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

An Efficient Human Authentication Using Multibiometric Approach for High Accuracy in Recognition Rate

U. Supriya[*1], G. Divya Sri[2], M. Kalaiselvi[3], K.R.Karthekk[4]

[*1]Assistant Professor, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India

[2,3,4]UG Scholar, Department of Computer Science and Engineering, SNS College of Technology, Coimbatore, Tamilnadu, India

ABSTRACT

In the development of recent technologies, a biometrics system has been the important affordable and more reliable system. A Biometrics identification system refers to the automatic recognition of individual person based on their characteristics. Biometrics system has two broad areas namely unimodal and multimodal biometric system. In Unimodal system it has some disadvantage due to its lack of non- universality and unacceptable error rate. To overcome the Unimodal challenging issues, Multimodal is the better system for its two or three level of identification and verification. In this paper, multimodal biometrics system characteristics are studied with various biometrics traits. The proposed system uses a multibiometric approach for authenticating a person. The multibiometric system comprises of multimodal (iris, fingerprint and face) and multi algorithm (Iterative Parallel Thinning Algorithm, Fuzzy Pattern Based with Laplacianfaces, Optimized Daugman Algorithm) biometrics whose recognition rate will be calculated separately using GAR, FAR and FRR scores. Finally, the matching scores of both the methods will be fused to find the final recognition rate, which will prove that multibiometric system provides high accuracy in recognizing a person, and highly secured against spoofing attacks.

Keywords: Unimodal, Multimodal, Recognition, Spoofing, FAR, FRR, GAR.

I. INTRODUCTION

With the growth of technology improvements biometric identification system is one of the important authentication techniques to provide a validation operation. For the past decades security like password and ID cards have been used for restricting the misbehavior of the secured system. This kind of security can be easily breached when the password is revealed or ID card is stolen by the impostor [3].To avoid this kind of breached the biometric authentication is used. The Biometric authentication of the secured system has been developed for several years and the recent enhancements in technology has made more affordable and more reliable. This biometric authentication gives protection from any misleading activities to the user. Biometric modalities can be divided into three main categories such as physiological, Behavioral and Chemical [3]. The category of physiological biometric modality is based on the nature of the body it includes finger print, retina, palm print, hand geometry, DNA, facial thermo grams. A finger print is the physiological nature that has been used more than 100 years [2]. The category of behavioral biometric is based on the behavior of the person like signature, voice, walking style, lips dynamics. Chemical biometrics is still an emerging field and involves a chemical cases such as body odor, human sweat etc.

II. METHODS AND MATERIAL

1. Proposed System

A Multi Biometric trait is being used. Multi Biometric comprises of Multimodal or Multi algorithmic biometrics. A Multimodal biometric authentication system enhances the security considerations as much as

possible. Here some basic Multimodal biometric authentication traits.

2. Multi-Biometrics

Fingerprint

Fingerprint is a graphical pattern of ridges and valleys on the surface of human finger. It has used on personal identification because of it is one of the human characteristics. The fingerprint recognition is mainly used on various forensic departments like criminal identification [1]. Most automatic system for fingerprint comparison is based on minutiae matching. The minutiae matching characteristics represent the termination and bifurcations of the fingerprints [3]. A good quality fingerprint image contains about 40 to 100 minutiae. A fingerprint is the feature pattern of one finger and it is believed that each fingerprint is unique. Each person has his own fingerprints with the permanent uniqueness. So fingerprints have being used for identification and recognition. A fingerprint is composed of ridges and furrows which are parallel and have same width [5].

The basic patterns of fingerprint ridges are arch, loop and whorl [22].

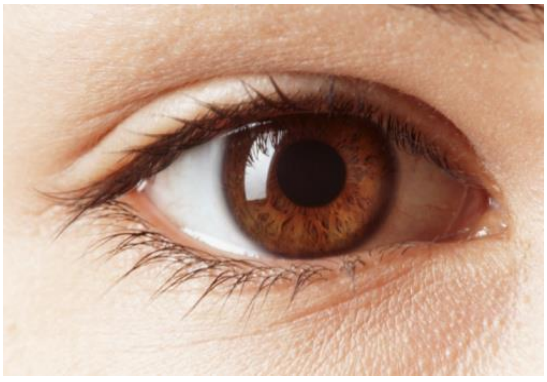
Arch: The ridges enter from one side of the finger, rise fr1om center forming an arc and exit from one side of the finger.

Loop: The ridges enter from one side of the finger, form a curve and exit on same side of the finger.

Whorl: Ridges form circularly around the center point on the finger

Iris

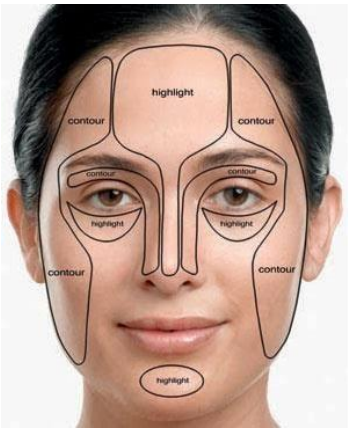
Iris is one of the biometrics authentication systems which are located between cornea and lens of the human eye. Basically the iris function is to control the amount of light entering through the pupil. It consists of a number of layers, in the lowest layer it contains dense color cells and also it determines the color of iris [1]. In image processing techniques it can be employed to convert iris pattern to unique code which can be stored in a database and allows comparison between templates. The overall process for acquiring and storing iris features with iris images as listed as follows, Image acquisition: take photo of iris with good resolution and quality [11]. Segmentation: process the acquiring image for separation of iris from eye image. Normalization. Feature extraction and feature encoding [13]. Storing extracted codes in database and comparing acquiring iris images with codes in database.



Face

The facial attributes are probably the most common biometric features used by humans to recognize one person to another. There are two most popular approaches are available, the first one is depends on the location and shape of facial attributes such as eyes, nose, lips and chin. Another analysis of the face image represents a face as a weighted combination of a number of canonical faces [3].

To provide high authentication, multimodal identification is the better choice. Multimodal authentication mechanism is nothing but a combination of unimodal system with two or three and so on. Furthermore, multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user [20]. By asking the user to present a random subset of biometric traits, the system ensures a live user is indeed present at the point of data acquisition. The choice and number of biometric traits is largely driven by the nature of the application, the overhead introduced by multiple traits and the correlation between the traits considered [20]. A multi biometric system offers several advantages like better recognition accuracy, increased population coverage, greater security and flexibility.



III. RESULTS AND DISCUSSION

Multi-Algorithm

FPBL (Fuzzy Pattern Based with Laplacianfaces)

Fuzzy Pattern Based with Laplacianfaces Biometric pattern matching Algorithm for faces is based on Laplacianfaces with Fuzzy level calculation. It utilizes two level of face image pixel value 0 or 1 as minimum and maximum value but fuzzy method uses intermediate value between o and 1 pixel value [8]. FPBL system evokes pixel wise value extraction of face image to different classification for classification of error reduction.

Fuzzy method for face recognition generates pixel wise information of face images. It collects pixel wise belongings for different classes which reduces the classification error [8]. Database images are separated into column vector for those the fuzzification process is applied. Fuzzy module generates pixel wise degree of association of face image to different classes using membership function (MF). Membership function is generalization of characteristics function of crisp set. The crisp set assigns the value of 1 to member function and 0 to non-member function. The input images are segmented into four portions. Feature vectors of all images are extracted in definite order. The distance is measured between input and other vectors is measured by distance measure and related person is recognized [8].

Laplacianfaces method of face recognition is an appearance based method. It uses locality preserving projections (LPP). LPP is that which preserves subspaces that captures the intrinsic geometry of data image and local structure [9]. The projection is obtained, then each face image in the image space is mapped to the low-dimensional face subspace. It is characterized into a set of feature images called Laplacianfaces. Low dimensional representation through kernel based technique has developed for face recognition can discover the non-linear structure of face image [9]. Laplacianfaces algorithm targets to preserve the local structure of digital image.

Iterative Parallel Thinning Algorithm (IPTA)

Iterative Parallel Thinning Algorithm (IPTA) is used for feature extraction of the fingerprint. The images are to be enhanced for increasing contrast between ridges and valleys and for connecting false broken points of ridges [21]. For enhancement of images canny edge detection method is used. But canny edge detection method consumes more processing time and would increase complexity. To reduce the complexities of canny edge detection method, the Histogram Enhancement and Fourier Transform method is used [21].

Histogram expands the pixel value distribution of an image as to increase the perceptional information. In Fourier Transform, the image is divided into processing block (32 by 32 pixels) and perform Fourier transform. The enhanced image is binarized using the Adaptive Threshold Method [21]. The ridges and valleys of the finger print is converted into binary. In Binarization the 256 level image is transformed to a 2 level image which gives same information. The value of object pixel is 1 and object pixel is 0.Binary image is created by coloring each pixel by white or black (Black for 0 and White for 1). In the Adaptive Threshold method, the image is divided into blocks (16 * 16), then mean intensity value is calculated for each block, then each pixel is turned into 1 if intensity value is larger than mean intensity value of current block [21].

In Iterative Parallel Thinning Algorithm, for each scan of fingerprint image the algorithm marks down redundant pixels in each small image window (3 *3) and finally removes all those marked pixels after several scans. The thinned ridge map is then filtered by morphological operation to remove some H breaks, isolated points and spikes. In this step, any single points whether they may be a single pint ridges or single point breaks in a ridges are eliminated. The Iterative Parallel Thinning Algorithm removes the noises in the image then the minutia marking is done easier [17]. The concept of Crossing Number (CN) is used for extraction of the minutiae. For each, 3*3 window, if center pixel is 1 and has exactly 3 one value neighbors, the center pixel is ridge branching, if center pixel is 1 and has 1 one value neighbor, the central pixel is ridge ending.

After the marking of the minutiae the templates are stored in the database. Then the fingerprint is matched for verification and identification purpose. In minutiae matcher, any 2 minutiae as reference pair and matches their associate ridges [17]. If the ridges are matched, then 2 fingerprint images are aligned and matching is done for remaining minutiae.

Optimized Daugman's Algorithm

In Optimized Daugman's Algorithm the integro-differential operator is proposed to ignore all circles if any pixel on this circle has a value higher than a certain threshold. The threshold for greyscale image is 200[15]. But the bright spot are usually higher than 245.

In Iris outer boundary localization detects upper and lower eye lids. It selects two search regions as a reference that are in the boundaries of pupil's center and Iris inner. The eye lids are detected to the search region by Sobel Edge Detection [15]. Sobel kernel reduces the false edge detection caused by eye lashes. After edge detection step the edge image is generated [15]. The eye lids are detected using Linear Hough Transform Method.

When iris region is successfully segmented from the image, it transforms the iris region so that it has fixed dimensions for comparison [15]. Inconsistency in eye image is caused due to the stretching of iris pupil that has varying level of illumination. Normalization process will produce the iris region which have constant dimensions, so that two photograph of same iris under different conditions will have characteristic feature in same spatial location. The automatic segmentation model using Daugman's integro-differential proved to be successful [13]. Integro-differential equation ad Hough transform methods on locating the pupil and limbus assumes that the boundary are different, all the methods as circular curves.

IV. CONCLUSION

To improve the security of the system, biometrics has been widely used. Unimodal Biometric system is easy to implement and has been used frequently, but it is found to be more prone for forgeries like spoofing attacks. So multi modal biometrics such as fingerprint, Iris, Face has been used with multi Algorithm like Iterative Parallel Thinning Algorithm, Fuzzy Pattern Based with Laplacianfaces, Optimized Daugman Algorithm to increase the security of the system. The Iterative Parallel Thinning Algorithm is used for feature extraction of the Fingerprint, Fuzzy Pattern Based with Laplacianfaces is used for feature extraction of the face and Optimized Daugman Algorithm is used for the feature extraction of the Iris. After the extraction of the feature from the biometrics the template has been stored in the database for the verification and validation purpose. As a result matching scores will be obtained and performance analysis will be performed by generating Recognition rate and error rate graphs. This proposed approach will be expected to give high accuracy in Recognition and security against security attacks.

V. REFERENCES

[1] S.Mohana Prakash, P.Betty, K.Sivanarulselvan, "Fusion of Multimodal Biometrics using Feature and Score Level Fusion", ISSN (Online):2394-6237, Volume 2: Issue 4: April 2016, pp 52-56.

[2] Padma Polash Paul, Marina L. Gavrilova, and RedaAlhajj ―Decision fusion for multimodal biometrics using social network analysis‖ IEEE transactions on systems, man, and cybernetics: systems, vol. 44, no. 11, november 2014.

[3] N.Gopal, Dr.R.K. Selvakumar, "Multimodal Biometric Identification System - An Overview", International Journal of Engineering Trends and Technology (IJETT) – Volume 33 Number 7- March 2016.

[4] Aggithaya et al., "A Multimodal biometric authentication system based on 2D and 3D palmprint features", Proc. of SPIE Vol. 6944 69440C-1- 2012.

[5] Ashraf Aboshosha , Kamal A. El dahshan, Ebeid A. Ebeid, Eman K. Alsayed, "Fusion of Fingerprint, Iris and Face Biometrics at Decision Level", ISSN: 2277 128X, Volume 5, Issue 2, February 2015.

[6] Byungjun Son and Yillbyung Lee. 2005. Biometric authentication system using reduced joint feature vector of iris and face. In audio-and Video-Based Biometric Person Authentication, pages 513–522. Springer.

[7] Heng Fui Liau and Dino Isa. 2011 Feature selection for support vector machine-based face-iris multimodal biometric system. Expert Systems with Applications, 38(9):11105–11111.

[8] Ajit Kumar Tiwari, Shrikant Lade, "Fuzzy Pattern-Based with Laplacianfaces Biometric Pattern Matching Algorithm for Face Recognition", ISSN: 0976-849, IJCST Vol. 6, ISSue 1, Jan - MarCh 2015.

[9] Jianjun Qian, Jian Yang, Yong Xu, "Local StructureBased Image Decomposition for Feature Extraction With Applications to Face Recognition", IEEE Transactions on Image Processing, Vol. 22, Issue 9, 2013, pp. 3591-3603.

[10] N. Goranin and A. Cenys, "Evolutionary Algorithms Application Analysis in Biometric Systems", Journal of Engineering Science and Technology Review 3 (1) (2010) 70-79.

[11] J. Abbazio, S. Perez, D. Silva, R. Tesoriero, F. Penna and R. Zack, Proc. Student-Faculty Research Day, CSIS, New York, USA, pp. C1.1-C1.8 (2009).

[12] André Aichert, "Feature extraction techniques", January 9, 2008.

[13] Khattab M. Ali Alheet, "Biometric Iris Recognition Based on Hybrid Technique" International Journal on Soft Computing (IJSC) Vol.2, No.4, November 2011.

[14] Chaohong Wu, "Advanced Feature Extraction Algorithms for Automatic Fingerprint Recognition Systems", April 2007.

[15] Prateek Verma, Maheedhar Dubey, Praveen Verma3 Somak Basu, "Daughman‟S Algorithm Method For Iris Recognition-A Biometric Approach", ISSN 2250-2459, Volume 2, Issue 6, June 2012

[16] Kalyan Veeramachaneni, Lisa Ann Osadciw, and Pramod K. Varshney , "An Adaptive Multimodal Biometric Management Algorithm" IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, vol. 35, no. 3, august 2005.

[17] S. Li, R. Chu, S. Liao, and L. Zhang, ―Illumination invariant face recognition using near-infrared images‖, IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 627–639, 2007.

[18] PP Chitte, JG Rana, RR Bhambare, VA More, RA Kadu, and MR Bendre. 2012. Iris recognition system using ica, pca, daugmans rubber sheet model together. International Journal of Computer Technology and Electronics Engineering, 2(1):16–23.

[19] A.Ross and R. Govindarajan, "Feature Level Fusion Using Hand and Face Biometrics", In Proceeding of SPIE Conference on Biometrics Technology for Human Identification, volume 5779, Florida, U.S.A., March 2005, pp.196-204.

[20] Faizan Ahmad, Aaima Najam and Zeeshan Ahmed, "Image Ima Imaggee Image--based Face Detection and Recognition" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 6, No 1, November 2012 ISSN (Online): 1694-0814.

[21] Zain S. Barham Supervised by: Dr. Allam Mousa, Fingerprint Recognition using MATLAB Graduation project.

[22] https://en.wikipedia.org/wiki/Fingerprint_recognition.

[23] https://in.mathworks.com/campaigns/products/ppc/google/matlab-trial-request.html?s_eid=ppc_29954890402&q=matlab.

[24] https://in.mathworks.com/support/learn-with-matlab-tutorials.html?requestedDomain=www.mathworks.com.

[25] https://www.tutorialspoint.com/matlab