International Conference on Smart Electronic Systems - 2016
KLE Society's Dr M S Sheshgiri College of Engineering & Technology, Belagavi

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 40-45

Multimodal Biometric System using Fingerprint, Iris & Ear

Abhijit V. Naik[1], Dr. H. G. Virani[2]
[1] Goa College of Engineering/Electronics & Telecommunication Department, Goa, India
Email: naik.abhijit@hotmail.com
[2] Goa College of Engineering / Electronics & Telecommunication Department, Goa, India
Email: virani@gec.ac.in

Abstract— **Biometric systems based solely on one-modal biometrics are often not able to meet the desired performance requirements for large user population applications, due to problems such as noisy data, intra-class variations, restricted degrees of freedom, non-university, spoof attacks, and unacceptable error rates. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a single identification system. The most compelling reason to combine different modalities is to improve the recognition accuracy. In this paper, multimodal biometric approach is discussed using three biometrics are used i.e. iris, fingerprint and ear. The three biometrics are combined using score level fusion.**

Index Terms— **Biometric fusion, Eear recognition, fingerprint recognition, Iris recognition, minutiae extraction, multi-modal biometric fusion, Score Level Fusion.**

I. Introduction

Biometric identification is an effective method for human identification. Also, it has received a lot of attention in recent years [1]. It should provide reliable personnel recognition schemes to either confirm or determine the identity of an individual. Moreover, the biometric systems are advantageous because they do not require a person to carry cards or remember information, unlike the conventional authentication systems based on smart cards or passwords. It has also reduced the various drawbacks of personal identification systems such as entering Personal Identification Number (PIN), typing logins and passwords and displaying identification cards. The biometric identification method is a natural method that can easily deal with those problems [2]. In real world applications, various unimodal biometric systems are used that depend on the single biometric marker for personal recognition. In addition, the unimodal biometric recognition systems are not much efficient, accurate and robust due to the difficulty caused by external factors [3]. It often confronts a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks and unacceptable error rates [4]. The problems caused by unimodal biometrics can be reduced by a multimodal biometric authentication system. The multimodal biometric authentication system is reliable and more accurate due to the presence of multiple evidences in biometrics [4]. The important concept of multimodal biometrics system is that it integrates multiple sources of information obtained from different biometrics [5], [6].

II. Multi Biometric Systems

It is clear that some people have poor quality fingerprints, their face image depends on lighting, their voice can get hoarse due to cold, and also original image of iris projected on a lens can make different biometric authentication systems. All these disadvantages can be overcome with multi-biometric systems which combine the results of two or more biometric characteristics independent from each other. Uni-modal biometric systems perform identification based on single source of biometric information. These systems are affected by many problems like noisy sensor data, non-universality, lack of individuality, lack of invariant representation and susceptibility to circumvention. Because of these problems, the uni-modal biometric systems error rate is quite high which makes them unacceptable for security applications. Some of these problems can be alleviated by using two or more uni-modal biometrics as multi-biometric systems. The architecture of a multi-biometric system depends on the sequence through which each biometrics are acquired and processed. Typically these architectures are either serial or parallel. In the serial architecture, the result of one modality affects the processing of the subsequent modality. In parallel design, different modalities operate independently and their results are combined with appropriate fusion method. The proposed design in this paper is parallel design. There are several paper on different multi-biometric. Multi-biometric systems use five different methods for solving single biometric disadvantages:

Multi-sensor: using two or more sensors for obtaining data from one biometric. (Fingerprint image with two optical and alter sound sensors).
Multi-presentation: several sensors capturing several similar body parts. (Multi fingerprint image from multi finger of one person).
Multi-instance: the same sensor capturing several instances of the same body part. (Different position face image).
Multi- algorithm: the same sensor is used but its input is processed by different algorithm and compares the results.
Multi-modal: using different sensors for different biometrics and fusion the results. (Like fusion iris and fingerprint code as multi-biometric).

International Conference on Smart Electronic Systems - 2016
KLE Society's Dr M S Sheshgiri College of Engineering & Technology, Belagavi

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 40-45

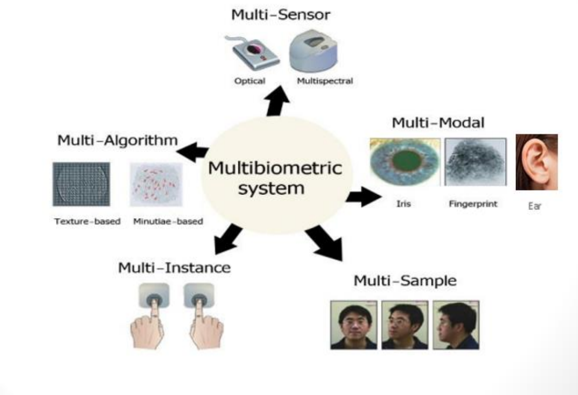


Fig. 1. Five different methods for solving single biometric disadvantages

III. Proposed Approach

In this paper multi-modal approach will be discussed using three biometric traits namely fingerprint, iris and ear. Each individual biometric model has to go under different level of processing like Pre-processing, Normalization, Feature Extraction and Matching to get proper Matching score of both biometric individually and we apply fusion technique at matching score level with obtained matching score.

1. Fingerprint Recognition

Fingerprint recognition is the most consistent biometric modality in use, The main reason behind the use of fingerprint biometric is that it is the most proven technique to identify the individual. Digital fingerprints are more convenient and less disturbing than most of the other biometric methods and they are already accepted as an immutably single identifier. The fingerprint is basically the combination of ridges and valleys on the surface of the finger. However, revealed by rigorous research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by Minutia, which are typical points on the ridges[7] . There are several minutia types: Termination (the immediate ending of a ridge), Bifurcation (the point on the ridge from which two branches derive),Island (a ridge that commences, travels a short distance and then ends), Ridge enclosures (a single ridge that bifurcates and reunites shortly afterward to continue as a single ridge), Spur (a bifurcation with a short ridge branching off a longer ridge), Crossover or bridge (a short ridge that runs between two parallel ridges)[7][8]. In this paper only two types of minutia points are take into consideration, which are termination and bifurcation. The major steps involved in fingerprint recognition using minutiae matching approach after image acquisition are:

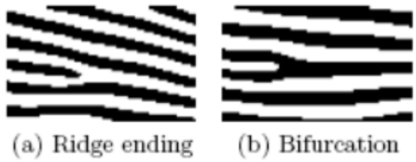
1. Image Enhancement
2. Minutiae Extraction
3. Matching

1.1. Image Enhancement

A fingerprint image is corrupted due to various kinds of noises such as creases, smudges and holes. It is almost impossible to recover the true minutia points from the unrecoverable regions The fingerprint image is enhanced to make it clearer for easy further operations by increasing the contrast between ridges and furrows. The image is converted to grayscale and thiined and binarized

1.2. Minutia Extraction

The endings and bifurcations of the fingerprint images are known as the minutia. The most commonly employed method of minutiae extraction is the Crossing Number (CN) concept.

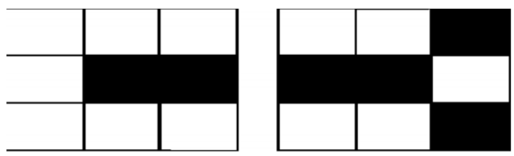


.

Fig 2: Example of ridge ending and bifurcation

The minutiae are extracted by processing the whole image pixel by pixel using a 3x3 matrix with the centre element being the focus of each process[9]. The CN value is then computed, which is defined as half the sum of the differences between pairs of adjacent pixels in the eight-neighborhood[7]. Using the properties of the CN as shown in table, the ridge pixel can then be classified as a ridge ending, bifurcation or non-minutiae point[8]. For example, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation. The Crossing Number (CN) method is used to perform minutiae extraction[7]. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using a 3*3 window[7]. After the CN for a ridge pixel has been computed, the pixel can then be classified according to the property of its CN value. A ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation[7]. For each extracted minutiae point, the following information is recorded:

- x and y coordinates,
- Orientation of the associated ridge segment, and
- Type of minutiae (ridge ending or bifurcation).



International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 40-45

Fig 3: a) corresponds to ridge ending b)corresponds to bifurcation

Minutia extraction is processed in 4 steps:

- Fingerprint ridge thinning
- Minutia marking
- False minutia removal
- Unification of terminations and bifurcations.

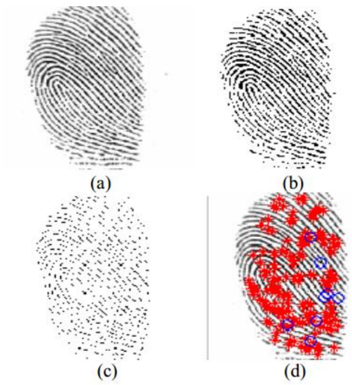


Fig 4: a)original image b)binarized image c)thinned image d)minutia points

1.3. Matching

The minutia match algorithm settles on whether two set of minutia of two fingerprint images belong to the same finger or not .The first step consists in aligning the couple of fingerprint Images to be matched[10].Thus we choose a minutia from each image and calculate the similarity of the associated ridges[11].

2. Iris Recognition

Iris is plainly visible, colored ring that surrounds the pupil which is unique to each individual and remains constant over the life of a person. The iris is the annular ring between the sclera and pupil boundary and contains the flowery pattern unique to each individual. The eyeball has a circular black disk in the center known as pupil. The pupil dilates when exposed to light and contracts in dark. Thus the size of pupil varies with respect to light. There is no detailed correlation between the iris patterns of even identical twins, or the right and left eye of an individual[12]. The preprocessing stage for iris recognition consists of resizing, conversion to grayscale followed by noise removal. Feature extraction is done using Lineary Binary Pattern Algorithm. Local Binary Pattern (LBP) is an efficient method used for feature extraction and texture classification it was first introduced by Ojala et al in 1996 [13] , this was the first article to describe LBP. The LBP operator was introduced as a complementary measure for local image contrast, and it was developed as a grayscale invariant pattern measure adding complementary information to the "amount" of texture in images. LBP is ideally suited for applications requiring fast feature extraction and texture classification Due to its discriminative power and computational simplicity, the LBP texture operator has become a popular approach in various applications, including visual inspection, image retrieval, remote sensing, biomedical image analysis, motion analysis, environmental modeling, and outdoor scene analysis. In this paper LBP is introduced in order to extract the iris features from the normalized iris image. Table 1 illustrates an example of the input sub-image with size 3×3, the center is threshold value such that, If the gray level of the neighboring pixel is higher or equal, the value is set to one, otherwise the value is set to zero.

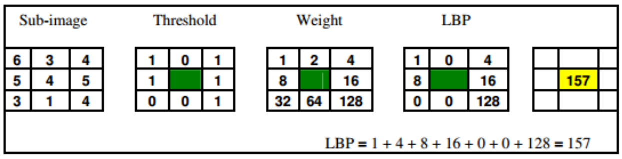


Fig 5: Example of LBP computation

For matching, LBP value of iris image is compared with the LBP values of database images.

3. Ear Recognition

The ear image has some unique aspects like the shape and the edges, which help in the better extraction of features. The different shapes of the ear are round, oval, triangular and rectangular. The other factors include the edges found inside the ear. The shape and the pattern of the ear image are different for every human. So in feature extraction, the first thing to be considered is the shape of the ear. The ear image has to be resized so as to get only yhe region of intrest. Then the image has to be converted to grayscale and binarized. The next step after finding the shape of the ear is the edge detection. Only through edge detection, the important and relevant information can be extracted from the ear image. The technique used here for edge detection is the canny edge detection, which gives better results under illumination condition. After the edge detection process, the broken edges were joined using a method called dilation.

If w is the width of the image and h is the height, canny edge detectot used takes as input an array $w*h$ and outputs a binary image with value 1 for edge pixels and value 0 for all other pixels. At feature extraction stage, the features extracted are all angles. The feature vectr is found using the outer shape of the ear i.e outer edge. To find angles, max-line and normal is used. Max line can be defined as the longest line that can be dran with both the endpoints on edges of ear. The length of line is measured interms of Euclidean distance. Normal lines are the lines which are perpendicular to max-line and which divide the max line into (n+1) equal parts, where n is apositive integer.

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 40-45

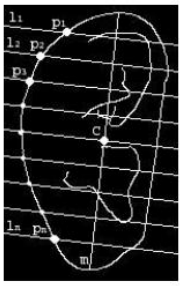


Fig 6: Image with max-line and normals

Above figure shows image with max line m and normal lines perpendicular to line m. Let $p_1, p_2 \ldots p_n$ be the points where outer edge and normal lines intersect. It is assumed that the outer edge is continuous. The feature vector is defined by

$$FV1 = [\theta_1, \theta_2, \ldots, \theta_n]$$

Where θ_i is the angle between max-line and line joining center of max-line to point p_i. The images are said to be matched if the angles are approximately same and also thet correspond to the same normal line.

4. Fusion

A generic biometric system consists of four modules namely sensor module, feature extraction module, matcher module and decision module. In a multimodal biometric system, fusion can be performed depending upon the type of information available in any of these modules. According to Sanderson and Paliwal [14] various levels of fusion can be classified into two broad categories: fusion before matching and fusion after matching as shown in Fig. 6 . This classification is based upon the fact that once the matcher of a biometric system is invoked, the amount of information available to the system drastically decreases. Fusion prior to matching includes fusion at the sensor and feature extraction levels and fusion after matching includes fusion at the match score and decision levels. It is generally believed that a fusion scheme applied as early as possible in the recognition system is more effective. The amount of information available to the system gets compressed as one proceeds from the sensor module to the decision module [15].

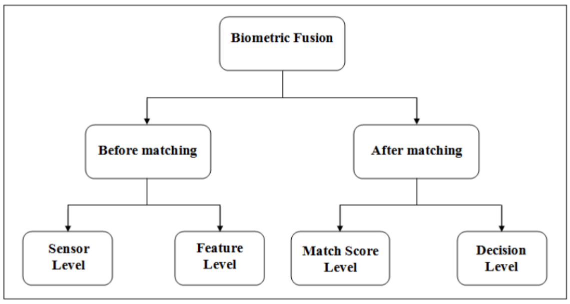


Fig 7: Classification of level of fusion

The structural design of proposed multimodal biometric recognition system integrating iris, face and voice is shown in Fig. 7. In the operational phase, the three biometric sensors capture the images individually from the person to be identified and converts them to a raw digital format, which is further processed by the feature extraction modules individually to produce a compact representation that is of the same format as the templates stored in the corresponding databases taken during the enrollment phase. The three resulting representations are then fed to the three corresponding matchers. Here, they are matched with templates in the corresponding databases to find the similarity between the two feature sets. The match scores generated from the individual biometrics are then passed to the fusion module to perform fusion at match score level using simple sum rule.

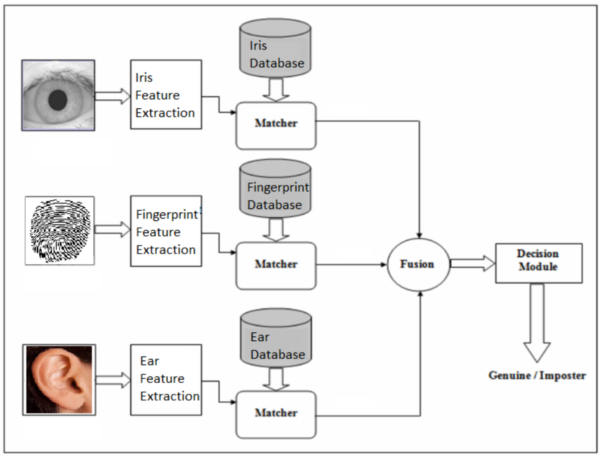


Fig 8: Architecture of proposed multimodal biometric recognition system integrating iris, fingerprint and ear.

The first step involved in fusion is score normalization. Since the match scores output by the three biometric traits are heterogeneous because they are not on the same numerical range, so score normalization is done to transform these scores into a common domain prior to combining them. Here, min-max normalization is used to transform all these scores into a common range [0, 1]. The three normalized scores are fused using sum rule to generate final match score. Finally, fused matching score is passed to the decision module where a person is declared as genuine or an imposter. The normalized scores are obtained by following min-max equation

$$S_i' = \frac{S_i - S_{\min}}{S_{\max} - S_{\min}}$$

where S_i is the normalized matching score, S_i is the matching score, S_{min} is the minimum match score and S_{max} is the maximum match score for ith biometric trait. In order to combine the match scores output by the three individual matchers (iris, fingerprint and ear), simple sum rule is used and its equation is given below

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 40-45

$$Sum = \sum_{i=1}^{n} S_i$$

IV. Implementation and Result

This paper presents a new multimodal biometric recognition system integrating iris, face and voice based on score level fusion. The proposed system was implemented using Matlab software. The proposed system is tested using different databases. Fingerprint samples are taken from FVC2004 database. Iris samples are taken from CASIA Iris V4 database. Ear samples are taken from AMI Ear database.

In the enrollment process, fingerprint, iris and ear image of one person is captured. These images are preprocessed and features are extracted and saved in the database. In identification process we enter the same images again. After processing we get the correct output that is person recognized correctly which gives a message as Authenticated. Same way if we enter the fingerprint, iris & ear images of different person from the database we get the output as Not Authenticated. If we take the images which are not from the database then we get the output as Not Authenticated.

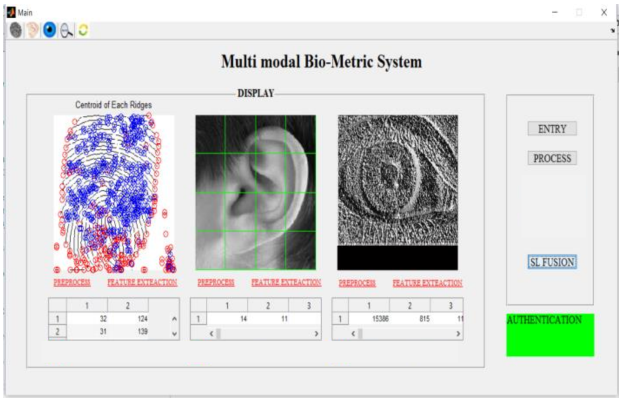


Fig 9: Training and Testing Graphical User Interface

Above figure shows a graphical user interface of Matlab software.

Metric	Fusion of iris & fingerprint [16]	Fusion of fingerprint, iris and ear
False Acceptance Rate	0.3%	0.1%

Table 1: Performance of Multimodal System

Acknowledgment

I would like to thank my guide and H.O.D of ETC Department Dr.H.G. Virani for his valuable inputs, encouragement and support. I am grateful to my parents and all my friends who were supportive throughout the course of this work.

References

[1] Gandhimathi Amirthalingam and Radhamani. G, "A Multimodal Approach for Face and Ear Biometric System", International Journal of Computer Science Issues, Vol. 10, No 2, 2013.

[2] MichałChoras, "Ear Biometrics Based on Geometrical Feature Extraction",Electronic Letters on Computer Vision and Image Analysis, Vol. 5, No.3, pp.84-95, 2005.

[3] Steven Cadavid, Mohammad H. Mahoor and Mohamed AbdelMottaleb, "Multi-modal Biometric Modeling and Recognition of the Human Face and Ear", International Workshop on safety security and Rescue Robotics, pp.1 – 6, 2009.

[4] Xiaona Xu and Zhichun Mu, "Feature Fusion Method Based on KCCA for Ear and Profile Face Based Multimodal Recognition", IEEE International Conference on Automation and Logistics, 2007.

[5] A. Rattani, D. R. Kisku, M. Bicego, and M. Tistarelli, "Robust feature-level multibiometric classification," Proceedings of the Biometric Consortium Conference – A special issue in Biometrics,pp. 1 –6, 2006.

[6] A. K. Jain and A. K. Ross, "Multibiometric systems," Communications of the ACM, Vol. 47, No.1, pp. 34–40, 2004.

[7] Y. Zhu, T. Tan, and Y. Wang, ―Biometric personal identification on iris patterns,‖ in Proc. 15th Int. Conf. Pattern Recogn. , 2000.

[8] A. K. Jain, A. Ross, and S. Pankanti, ―An introduction to biometric recognition,‖ IEEE Trans. Circuits Syst. Video Technol. , vol.14, no. 1, pp. 4–20, Jan. 2004.

[9] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, ―Robust fingerprint authentication using local structural similarity, in Proc. 5th IEEE Workshop Appl. Comput. Vis., Dec. 4–6, 2000, pp. 29–34. DOI 10.1109/WACV.2000.895399.

[10] Vincenzo Conti, Carmelo Militello, Filippo Sorbello, and Salvatore Vitabile, ―A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems,‖ IEEE transactions on systems, man, and cybernetics—part c: applications and reviews, VOL. 40, NO. 4, july 2010.

[11] L. Ma, Y. Wang and D. Zhang, ―Efficient iris recognition by characterizing key local variations‖ IEEE Trans. Image Process., vol. 13, no. 6, pp. 739–750, Jun. 2004.

[12] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, ―Robust fingerprint authentication using local structural similarity,‖ in Proc.5th IEEE Workshop Appl. Comput. Vis. , Dec. 4–6, 2000, pp. 29–34. DOI 10.1109/WACV.2000.895399.

[13] T. Ojala, M. Pietikäinen , and D. Harwood, "A Comparative Study of Texture Measures with Classification Based on Feature Distributions", Pattern Recognition, vol. 29, pp.51-59, 1996.

[14] C. Sanderson and K. K. Paliwal, Information Fusion and Person Verification Using Speech and Face, Information. Research Paper IDIAP-RR 02-33, IDIAP, September 2002.

International Journal of Technology and Science, ISSN (Online) 2350-1111, (Print) 2350-1103 Volume 3, Issue 3, 2016, pp. 40-45

[15] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, New York: Springer, 2006.

[16] P.U.Lahane , Prof. S. R. Ganorkar, "Fusion of Iris & Fingerprint Biometric for Security purpose", International Journal for Scientific & Engineering Research Volume 3, Issue 8, August 2012.