ISSN:2249-5789
Ahmed Omar Elkhateeb et al , International Journal of Computer Science & Communication Networks,Vol 3(4),226-230

Multimodal Biometric Personal Identification System Based On IRIS & Fingerprint

Prof:Ahmed M. Hamad,
Information System Dept.
FCIS's Dean British University,

Dr.Rasha Salah Elhadary,
Information System Dept.
FCIS MansouraUniversity

Ahmed Omar Elkhateeb,
Information System Dept.
FCIS MansouraUniversity

Abstract

Biometric systems can recognize individuals according to their physiological or behavioral characteristics. Many times due to some problems like noisy data, non-university, spoof attacks, and unacceptable error rates, a single biometric system can not meet the desired requirements for many user applications. Algorithm based on facts and existing data show that the recognition of an identification or verification system performance can be improved by using more than one biometric "Multimodal Biometric".

The proposed system introduced in this paper is based on two biometrics (IRIS and Fingerprint).

Keywords: Biometrics, Fingerprint, iris, ridges, valleys.

1. Introduction

Biometric refers to the process of recognition of individuals according to their physiological and/or behavioural characteristics. This technology acts as a front end to a system that requires precise identification before it can be accessed or used ([1] and [3]). Biometric systems recognize users based on their physiological and behavioral characteristics [2]. A unimodal biometric system uses a single biometric trait for user recognition.

Identification technologies could be one of three types; first is "What you know" like passwords, PIN, and ID however it may be forgotten, shared, or guessed. Second is "What you have" like key, and cards how ever it may be lost or stolen and it can be duplicated. Third is "What you are" like IRIS, fingerprint, face,.. etc.

2. Types of Biometrics

There are two types: Physiological Biometrics & Behavioral Biometrics.

2.1 Physiological Biometrics

In this category the recognition is based upon physiological characteristics. Some examples are: Fingerprint, Hand Geometry, Iris Recognition, Retinal Scanning, and Facial Recognition.

2.1.1 Fingerprint Recognition

Fingerprint is a unique feature to an individual. The lines that create fingerprint pattern are called ridges and the spaces between the ridges are called valleys or furrows. It is through the pattern of these ridges and valleys that the unique fingerprint is matched for authentication and authorization [4].

2.1.2 Iris Recognition

Iris patterns are complex and unique. In 1985 the concept that no two irises are alike was proposed. This technology is known for it's extreme accuracy: The probability of two individuals having the same iris pattern is 1 in 1078. [6]

2.2 Behavioural Biometric [5,6]

Behavioural biometrics is traits that is learned or acquired over time as differentiated from physiological characteristics. Some examples are: Voice Recognition, Signature Recognition and Keystroke Recognition.

3 Multimodal Biometric

As now known, A single biometric system, sometimes, may have a problem identefying users for some reasons like noisy data, non-university, spoof attacks, and unacceptable error rates. So there was a need for multimodal biometric systems to avoid these problems and improve recognition rate.

A Multimodal biometric system uses more than one biometric for user verification or identification so it can perform better than unimodal biometric systems. The major reason of using mutltimodal biometric system is to reduce false accept rate

(FAR), false reject rate (FRR), or failure to enroll rate (FTR). The advantages of multimodal systems grown from the fact that there are more than one biometric to be used in the system. Using such a system can increase accuracy, decrease enrollment problems, and enhance security.

4. Related Work

In a practical biometric system, there are a number of other issues which should be considered, including [13],

1. Performance,
2. Acceptability,
3. Circumvention,

However, a single biometric system has some limitations, such as noisy data, limited degrees of freedom [14]. In searching for a better more reliable and cheaper solution, fusion techniques have been examined by many researches, which also known as multi-modal biometrics. This can address the problem of non-universality due to wider coverage, and provide anti-spoofing measures by making it difficult for intruder to "steal" multiple biometric traits [14].

Chandran et al. (2009)presented iris and finger print multimodal biometrics to improve the performance. They presented multimodal biometrics using two lip texture, lip motion and audio and they performed the fusion by reliability weighting summation. Brunelli and Falavigna (2005) presented multimodal face and voice for identification. Kumar et al. (2007) presented multimodal personal verification system using hand images by combining hand geometry and palm image. Directional convolution masks are used to extract the palm futures from normalized palm image, whereas, finger length and width is extracted for hand geometry palm and finally, different level of fusion is performed Chin et al. (2009) integrate palm print and fingerprint at feature level. Series of preprocessing steps are applied on palm and finger print to increase efficiency and for feature extraction of 2D. Gabor filter is used and fusion is performed at feature level. Shahin et al. (2008) used three trait, that is, hand veins, hand geometry and fingerprint to provide high security by calculating the ridges, and the direction is calculated in frequency domain. Yao et al. (2007) performed feature level fusion on palm print and face for single sample, and features are extracted using PCA over Gabor filter. Zhou et al. (2007) presented multimodal authentication system using face and fingerprint, and multi route detection is used by using SVM fusion, whereas, the face image with zero turning is used as face template and other face images are used for self learning. Tayal et al. (2009) presented multimodal iris and speech authentication system using decision theory. Iris and speech biometrics are combined using energy compaction and time frequency resolution. Chu et al. (2007) presented multimodal biometrics using face and palm at score level fusion. Poinsot et al. (2009) presented palm and face multimodal biometrics for small sample size problems and Gabor filter is used for feature extraction of both palm and face images. Veins recognition utilized the vascular patterns, visible with infrared light illumination inside the human body, that is, hand, finger etc. Thus finger veins identification is difficult to falsify. Yang et al. (2009) presented finger veins recognition by using the feature combination extracted through circular Gabor filter and the feature are exploited on structural, topological and local moments. The segmentation of finger veins was based on multichannel and even the symmetric Gabor filter in spatial domain used eight orientation filters to exploit veins. Information in finger and finger veins image is segmented using threshold. Kang and Park (2009) presented multimodal finger veins recognition using score level fusing for finger geometry and finger veins. Based on SVM and minutiae point of finger veins, geometric features with sequential deviation are utilized for finger veins and geometry identification, respectively. Lee et al. (2009) presented finger veins recognition using minutia-based alignment and local binary pattern based on feature extraction. They also presented manifold learning and point manifold distance for finger veins recognition and ONPP is used for manifold recognition.

5. Proposed Scheme

Proposed scheme works at two levels (as shown in figure 2); at first level extracted IRIS features are compared, and at next level the extracted minutiae points are compared and matched. Level-II works only if Level-I is not passed. If Level-I is matched, the system avoids for matching minutiae points extracted further at level-II. In multimodal, two or more biometrics are employed (e.g. IRIS, fingerprint, palm print etc.) to enhance system

performance and accuracy. The proposed system uses two biometrics : IRIS and Fingerprint.

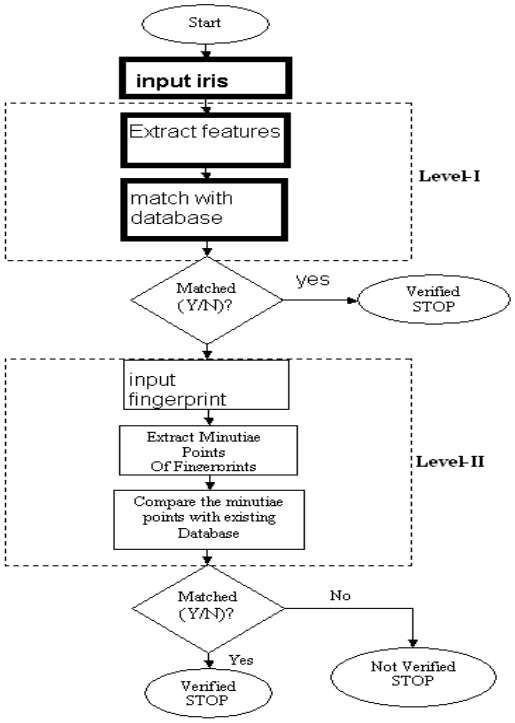

Figure 2 the proposed multimodal biometric system based on IRIS and Fingerprint

Level I: Iris

A non-invasive biometric system is the use of color ring around the pupil on the surface of the eye. Iris contains unique texture and is complex enough to be used as a biometric signature. Compared with other biometric features such as face and fingerprint, iris patterns are more stable and reliable. It is unique to people and stable with age [10].

Iris is highly randomized and its suitability as an exceptionally accurate biometric derives from [11],

- Its extremely data-rich physical structure
- Its genetic independence, no two eyes are the same
- Its stability over time
- Its physical protection by a transparent window (the cornea) that does not inhibit external view ability

The wavelet transform can obtain an accuracy of 82.5% [**Error! Bookmark not defined.**]. Other methods such as Circular Symmetric Filters [12] can obtain correct classification rate of 93.2% to 99.85%.

Level II: Fingerprints

One of the oldest biometric techniques is the fingerprint identification. Fingerprints were used as a means of positively identifying a person as an author of the document and are used in law enforcement. Fingerprint recognition has a lot of advantages, a fingerprint is compact, unique for every person, and stable over the lifetime. A predominate approach to fingerprint technique is the uses of minutiae [18].

The traditional fingerprints are obtained by placing inked fingertip on paper, now compact solid state sensors are used. The solid state sensors can obtain patterns at 300 x 300 pixels at 500 dpi, and an optical sensor can have image size of 480 x 508 pixels at 500 dpi [18].

6. System Performance

An important issue for the adoption of biometric technologies is to increase the performance of individual biometric models and overall systems in a convincing and objective way. For verification applications, a number of objective performance measures have been used to characterize the performance of biometric systems. In these applications a number of 'clients' are enrolled onto the system.

False Acceptance Rate (FAR) is defined as the ratio of frauds that were falsely accepted over the total number of frauds tested described as a percentage. This indicates the likelihood that a fraud may be falsely accepted and must be minimized in highly security applications[19].

False Reject Rate (FRR) is defined as the ratio of patrons that are falsely rejected to the total number of patrons tested described as a percentage. Ideally this should be minimized especially when the user community may stop using the system if they are wrongly denied access[19]..

The biometric verification process includes computing a distance between the stored template and the real sample. The decision to accept or reject is based on a defined threshold. If the distance is less than this threshold then we can accept the sample. It is now clear that the performance of the system significantly depends on the choice of this threshold and there is a swap between FRR and FAR. The Equal Error Rate (EER) is the threshold level for which the FAR and the FRR are equal. Figure 1 shows a general example of the FRR and FAR curves. The Equal Error Rate (EER) is often quoted as a single figure to describe the overall performance of biometric systems.

Another important performance parameter is the verification time defined as the average time taken for the verification process. This may include the time taken to present the live sample.

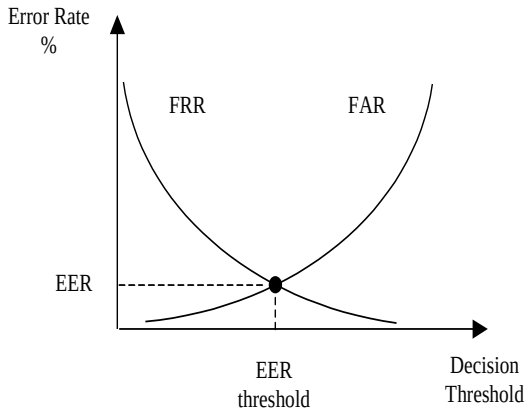

Figure 1 FRR and FAR curves.[19]

A number of databases have been developed for the evaluation of biometric systems. In this paper CASIA AND NIST are recommended

6. Results

In this paper the proposed system is based on IRIS and fingerprint. It is implemented and tested by matlab program with a combined test set from CASIA database for IRIS AND NIST database for fingerprint. Using the confusion matrix with 50 stored samples in the system database and another 50 samples not stored in the database. True Positives (TP) which are stored database 48 out of 50 samples are identified by the system, while False Negatives (FN) only 2 out of 50 samples are not identified by the system. False Positives (FP) which are not stored database 1 out of 50 samples are identified by the system, while True Negatives (TN) are 49 out of 50 samples are not identified by the system. The following results are appeared:

Accuracy = (TP + TN)/All
= (48+49)/100
= 0.97
Error = 1 – Accuracy
= 1- 0.97
= 0.03

The overall accuracy of the system is about 97% with FAR and FRR of 2.46% and 1.23% respectively

7. Conclusion

The paper presents simple and effective method of personal identification and verification system based on IRIS and fingerprint identification and verification system. The system works in two phases. At first phase first works on iris recognition (Level-I) and then goes to fingerprint recognition (Level-II).

In the last experiment, all the traits are combined at matching score level using sum of scores technique. The results are found to be very encouraging and promoting further research in this field. The overall accuracy of the system is about 97% with FAR and FRR of 2.46% and 1.23% respectively.

8. References:

[1] S. Rahal Authentication Fingerprint System, First National Information Technology Symposium (NITS 2006): Bridging the digital Divide: Challenges and Solutions, College of Computer & Information Sciences, King Saud University – 2006.

[2] Jain, A.K., Bolle, R., Pankanti, S., eds.: Biometrics: Personal Identification in Networked Security. Kluwer Academic Publishers (1999).

[3] Java Card Special Interest Group JCSIG-Introduction to Biometrics

http://www. javacard. org/others/ biometrics_intro.htm

[4] D. Maltoni, D. Maio, A. K. Jain, S. Prabahakar Handbook of Fingerprint Recognition, Springer - 2003

[5] Anil K. Jain, Arun Ross and Salil Prabhakar **An** Introduction to Biometric Recognition IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, August 2003

[6] Dave Mintie's http://www.biometricwatch.com/ Copyright © 2003

[7] Arun Ross, Salil Prabhakar and Anil Jain http://biometrics.cse.msu.edu/index.html

[8] Biometric Sensor Interoperability: A Case Study In Fingerprints Arun Ross and Anil Jain Appeared in Proc. of International ECCV Workshop on Biometric Authentication (BioAW), May 2004

[9] S. Prabhakar and A. K. Jain, "Decision-level fusion in fingerprint verification," Pattern Recognit., vol. 35, no. 4, pp. 861–874, 2002.

[10] Yong Zhu, Tieniu Tan, Yunhong Wang. 2000. Biometric personal identification based on iris patterns. *Proceedings 15th International Conference on Pattern Recognition*. 2, 801-4.

[11] Negin, M., Chmielewski, T.A., Jr., *et. al.* 2000. An iris biometric system for public and personal use. *Computer*, 33 (2), Feb, 70 -75.

[12] Li Ma, Yunhong Wang, Tieniu Tan. 2002. Iris recognition using circular symmetric filters *Pattern*

Recognition, 2002. Proceedings. 16th International Conference, 2, 414 -417.

[13] Lin Hong; Anil Jain. 1998. Integrating faces and fingerprints for personal identification. *Pattern Analysis and Machine Intelligence, IEEE Transactions*, 20(12), Dec, 1295 -1307.

[14] Jain, A.K., Ross, A. 2002. Learning user-specific parameters in a multibiometric system. *Image Processing. 2002. Proceedings. 2002 International Conference*, 1, I-57 -I-60.

[15] Dugelay, J.L., Junqua, J.C., Kotropoulos, C., Kuhn, R., Perronnin, F., Pitas, I. 2002. Recent advances in biometric person authentication. *Acoustics, Speech, and Signal Processing, 2002 IEEE International Conference*, 4, IV-4060 -IV-4063.

[16] Kittler, J., Messer, K. 2002. Fusion of multiple experts in multimodal biometric personal identity verification systems. *Neural Networks for Signal Processing, 2002. Proceedings of the 2002 12th IEEE Workshop*, 3 -12.

[17] Czyz, J., Kittler, J., Vandendorpe, L. 2002. Combining face verification experts. *Pattern Recognition, 2002. Proceedings. 16th International Conference*, 2, 28 -31.

[18] Jain, A., Ross, A., Prabhakar, S. 2001. Fingerprint matching using minutiae and texture features. Image Processing, 2001. Proceedings. 2001 International Conference, 3, 282 -285.

[19] Jiawei Han, Micheline Kamber, and Jian Pei Czyz, "Data Mining: Concepts and Techniques", *University of Illinois at Urbana-Champaign &Simon Fraser University*. 2010.