Towards an Integrated Biometric Technique

Rashmi Singhal Narender Singh Payal Jain
Faculty at MAHARISHI MARKANDESHWAR UNIVERSITY
Mullana (Ambala), INDIA

ABSTRACT

A biometric system is basically a pattern recognition system. Biometrics based user authentication system serve as a reliable means for meeting the challenges in today's world of information and network security. It has gained enormous interest by scientists and researchers. Unimodal biometric systems that employ only a single biometric trait fails to achieve the desired security levels. Even the best unimodal biometric system suffers from various problems. To overcome these issues, we propose a multi-modal biometric system which employs iris and hand-geometry biometric traits. The iris patterns of human eye are very complex and random. It is almost impossible for an imposter to imitate them. Hand-geometry measurements are not so distinctive and hence are used only for verification purpose. By combining them with other biometric trait like iris, a more secure multi-biometric security system can be obtained for verification as well as identification purpose. In this paper we will present a brief introduction about unimodal biometric systems, need for biometrics integration, various integration levels, types of multi-biometric systems and some previous research work. In the last section (7^{th}), we have presented our proposed multi-biometric system.

General Terms

Biometric systems, authentication, verification, modalities, security, physiological and behavioral traits, template.

Keywords

Multi-biometric system, iris, hand-geometry, biometrics integration, multi-sensor, multi-algorithm, multi-sample, multi-instance, multi-modal, hybrid systems**.**

1. INTRODUCTION

There are various methods for user authentication: a) using the traditional combination of username/password where the user is authenticated on the basis of 'what he knows', b) using magnetic cards or IC cards where authentication is done on the basis of 'what the user has', and c) the most secure method is by the use of biometrics information where the user is authenticated on the basis of 'who the user is' [1]. Because of vulnerabilities in first two methods, like theft, biometrics today is being used as a principal method for user authentication and verification.

Biometrics refers to an automated recognition system that relies on the physiological or behavioral traits of human beings for their authentication or verification. Physiological traits include face, iris, retina, fingerprints, hand geometry and palm print. Behavioral traits are voice, signature and keystroke dynamics. Some more promising biometric strategies are hand veins, facial thermogram, DNA, odor and scent. With the increasing demand for enhanced security, biometrics is being used in multiple applications like access control, forensic investigations, verification and authentication, e-commerce, and security monitoring [2].

Biometric system consists of a hardware device to capture biometric data and software that interprets the data and output the final decision regarding acceptance/rejection. Systems based on a single source of biometric information (known as Unimodal) generally fail to provide the desired security. To overcome this drawback, information from multiple modalities is integrated to minimize security threats. Such a system is known as multi-biometric system. In this paper we propose a multi-modal biometric system based on iris and hand-geometry.

2. INTEGRATED BIOMETRIC SYSTEMS

The physical or behavioral traits of a human being like his fingerprints, iris, retina, face, signature, voice, signature etc. are known as biometrics. These are Unique and measurable. For improving the security and accuracy of biometric systems, information from multiple biometric sources is integrated into a single multi-biometric system. Such information integration is known as multi-biometric fusion [3]. Multi-biometric authentication systems (MBAS) can be developed a) by integrating several physiological and behavioral traits of an individual, b) using multiple sensor systems, c) using multiple matcher systems and/or d) combining soft and hard biometrics. Presence of multiple sources of information makes multi-biometric systems more reliable. While choosing a multi-biometric system various factors must be kept in mind: the choice of biometric traits to be used, the level at which information fusion will take place, technique adopted for integration and cost versus performance trade-off.

In recent years, different biometric modalities are being integrated to develop multi-biometric systems. Some are a) hand vein, hand geometry and fingerprint integration, b) ear and face, c) facial thermogram and face, d) Fingerprint and hand geometry, e) iris and face etc. Multi-biometric systems have two basic categories: synchronous and asynchronous. The former combines two or more biometrics within a single authorization process. Asynchronous system, on the other hand, uses two biometric technologies in sequence, one after the other [4].

3. NEED FOR BIOMETRICS INTEGRATION

Unimodal biometric systems suffer many drawbacks: problem of noisy data, intra-class variation, improper user-sensor adjustment, inter-class similarities, non-universality, insufficient population coverage and spoof attacks [5] [1]. These problems lead to higher false rejection Rate (FRR) and false Acceptance Rate (FAR). Anil K. Jain [6] says that a

Unimodal biometric system may not be able to achieve 100% performance. Multi-biometric systems are comparatively found to be more reliable due to integration of multiple, independent biometrics information. Moreover, they help in resolving various problems encountered by Unimodal biometric systems. They allow indexing or filtering of large biometric databases and are robust to noise, provide universal coverage and improve matching accuracy. Further, when two or more modalities are used for authentication, it becomes difficult to spoof the biometric system [7]. Experiments have shown that the accuracy of multimodality can reach 100% and its performance is far better than Unimodal identification [8].

Multi-biometric systems can also be regarded as fault tolerant systems that continue working even when certain biometric modalities involved become unusable.

4. INTEGRATION LEVEL'S

Information integration in a multi-biometric system can be done at four different levels [4]:

A. Integration at feature extraction level

Feature sets extracted from biometric traits are integrated and the combined feature vector thus obtained is passed to the matching module.

B. Image level integration

Each image representation in bit form is integrated to obtain a single bit sequence representing the final image.

C. Matching score level

Matching score values, representing the similarities between biometric information obtained and the already stored biometric templates for each modality are combined. Applying fusion at this level is preferred as it is easy to obtain and combine matching scores.

D. Decision level

Separate authentication process is carried out for each biometric modality and the decisions taken by individual systems are integrated to obtain the final result. Integration at this level is supposed to be rigid because of availability of limited information.

Integrating information at an early stage is believed to be more effective since the feature set contains more information about the input data. An effective fusion scheme is the key to a successful multi-biometric system. Fusion rules must be chosen according to the type of application, biometric traits to be used and the level of fusion. Different matching algorithms and several rules are then applied to the Information obtained for reaching at a decision [2].

5. CLASSIFICATION OF MULTI-BIOMETRIC SYSTEMS

System using multiple biometric traits can be classified into six categories [4]:

A. Multi-sensor systems

Multiple sensors are used to capture the images of a single biometric trait of the user. For example- complementary information corresponding to fingerprints can be acquired using different types of sensors (like optical and capacitive sensors). Information obtained using these different sensors are then integrated using sensor level fusion technique.

B. Multi-algorithm systems

Multiple matching algorithms are applied to a single biometric trait. To get the final decision, any of the matching fusion technique (feature level, score level, rank level etc.) can be applied on the results obtained using different matching algorithms. These systems are more economical as no extra device is required to capture the data, but are also more complex because of application of different algorithms.

C. Multi-instance systems

Multiple instances of a single biometric trait are captured. For example- images of the left and right irises can be used for iris recognition. If a single senor is used to acquire these images in a sequential manner, the system can be made really cost effective.

D. Multi-sample systems

Multiple samples of a same biometric trait are captured. For example: along with the frontal face, the left and right profiles are also captured.

E. Multi-modal systems

More than one biometric trait is used for user identification. For example- the information obtained using face and voice features can be integrated to establish the identity of the user. To obtain better results, physically uncorrelated traits (like face and fingerprints) must be integrated. This can be more costly because it requires multiple sensors to capture different traits but, the improvement in performance is substantial.

F. Hybrid systems

It is a system which integrates more than one of the above mentioned multi-biometric systems. For example- two face recognition algorithms can be combined with two fingerprint recognition algorithms. Such a system will be multi-modal and multi-algorithmic system. If multiple sensors are used to obtain these images, then it will be multi-sensory and if multiple instance of the finger are used, it will be multi-instance system also.

6. PREVIOUS WORK DONE

R. Zewail et al. [3] in 2004 reported a multimodal biometric system in which iris color, a soft biometric, was integrated with the output of a primary biometric system comprising of fingerprint and iris texture as hard biometrics. The frequency and orientation of ridges was captured to provide distinct representations. In case of iris, local spatial patterns were used. The fingerprint matching was performed using a steerable filter based representation and the iris texture analysis was done using multi-channel log-Gabor filtering. Two classifiers, Weighted Averaging and Parzen Classifier, were used to calculate Genuine Accept Rate (GAR). Using various combinations of biometric traits and different classifiers, following results were obtained: i) combining fingerprint and iris color and using weighted average method as score combiner resulted in an improvement of 8% in GAR. ii) By combining iris texture and iris color and applying weighted average combiner, an improvement of 15% was recorded in GAR. iii) Far better overall performance was achieved by using fingerprint, iris texture and iris color biometric techniques together. From ROC graph it was evident that GAR of 100% was obtainable using Parzen combiner.

In 2005, Hashemi et al. [9] used hand geometry for authentication purpose. 200 hand images were collected from 40 users. Three phases were carried out: preprocessing, feature

measurements and feature selection. Euclidean distance, Gaussian mixture modelels (GMM) and Radial basis function neural networks (RBF) methods were used. Document scanner was used instead of conventional scanners.

In 2006, Kung et al. [10] combined both voice and facial images for biometric authentication. Audio clips were captured using high quality microphone. An audio classifier based on Gaussian Mixture model and visual classifier based on FaceIT was used. An indirect fusion scheme was proposed. Mixture-of-expert fusion architecture was used to integrate the classifiers.

C. Lupu et al. in 2007 [11] used fingerprint, voice and iris recognition technologies to identify or verify a person who wants to access a car. Two fingerprint readers were used; one was placed on the door of the car and other on the steering wheel. A microphone was used to record the voice of the user and a specialized iris camera was used to capture the image of the user. After all these biometric devices successfully identify the user as genuine, only then he is allowed to start the car. The main user can also allow other persons to use the car by storing their biometric characteristics in the database.

S. Asha et al. [1] in 2008 proposed that authentication process for e-learning can be enhanced by integrating the fingerprint biometrics with mouse dynamics. Fingerprints technology is the most common one. Mouse dynamics is a behavioral biometric and does not require any special hardware device. It involves a signature that is based on selected mouse movement. Mouse dynamics is considered to be a combination of following five factors: mouse movement speed, direction, traveled distance, time taken and action type.

In 2009, Md. Monwar et al. [12] integrated multi-algorithm and multi-modal approaches. Face, ear and signature were used as biometric traits. Following classification algorithms were used: multilayer perceptron, fisherimage and Bayesian network. Bi-level fusion was employed. At first rank fusion was used to combine the outcomes of these classifiers for face, ear and signature individually. The results of these three rank fusion methods' for face, ear and signature were then further combined using decision level fusion. Outcomes indicate that this hybrid multi-biometric system outperforms the single biometric systems.

Ryszard S. Chora´s in 2010 [13] presented a multi-biometric system that combined iris and retina features for biometric authentication. Both these features can be taken from same acquisition process and image. Gabor filters were used to extract the patterns. Experimental results showed improvement in iris and retina recognition for person identification.

Kai Yang and Eliza Yingzi Du worked on a new concept of "consent biometrics" in 2011 [14]. The recognition system was made to sense the willingness of the user by examining his consent signatures. Consent signatures may include active or passive physiological or behavioral data. Two biometric consent concepts were proposed: first, combinational systems in which both the biometric patterns are consent signatures are processed separately. Second, Incorporating consent biometric scheme, in which biometric data and consent signatures are acquired simultaneously.

7. PROPOSED SYSTEM

In this paper we propose a multi-modal biometrics approach that uses two biometric modalities: iris and hand-geometry for authentication purpose. Both these biometric traits are unique and believed to be stable over the years.

7.1 Iris Biometrics

Iris is a small circle surrounding the pupil of the human eye. The structure of human eye is unique for every individual even this pattern is different for both the irises. Iris texture has a complex pattern that remains stable over time. Distance between the pupil and the boundary of iris is unique for every individual and hence can be used for recognition purpose. Further, there are approximately 266 distinct spots in iris like: furrows, ridges, freckles, corona, dark spots or rings. The presence of so many distinct points and their uniqueness makes iris scan the most reliable technique.

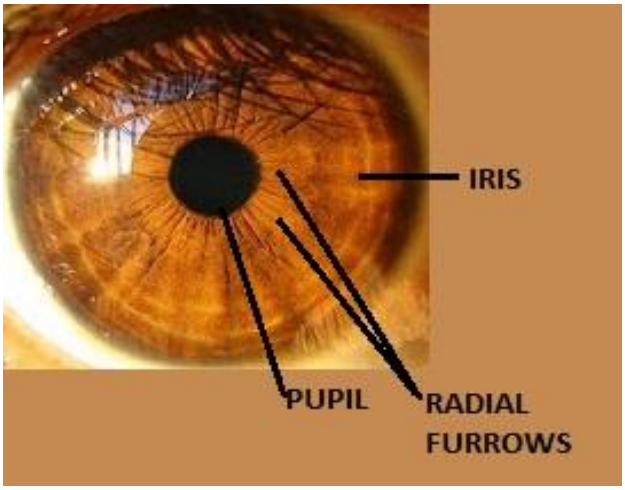

Figure 1: Internal Structure of Human Eye

An iris scan can be performed from about 10 cm to a few meters away and is not affected by the presence of lenses or glasses. It is expected to be the most accurate biometric source for authentication process Iris recognition system has following phases:

A. A sensor captures an iris image with sufficient resolution and sharpness, good contrast in the interior patterns and well framed iris texture.

B. Sensor will capture the image of the iris as a part of a larger image containing data from the surrounding areas as well. Before performing iris matching, it is necessary to localize the area corresponding to iris.

C. After localization, the useful patterns are filtered for analysis and corresponding to these useful patterns a vector set is generated.

D. An algorithm (wavelet transform) converts this vector set into an IrisCode of 512 bytes.

E. Distance between the IrisCodes (Hamming Distance) corresponding to the captured image and stored template is used for deciding whether both the iris patterns were derived from same iris source or not.

During iris scan two influences must be taken care of. First, the level of illumination, and second, changes in pupil size.

7.2 Hand Geometry Biometrics

Hand-geometry biometric measures the physical characteristics of the user's hand. A flat surface scanner is used on which the user places his hand, palm facing downwards. Pegs are used for proper alignment of hands. A three-dimensional image of the hand is captured by the hand reader. Metrics commonly used are finger length, width, thickness, area and circumference of

the hand image, and distance between the joints. Finger tip points and valley points are used as landmark points. More than 90 dimensional measurements can be collected by the scanner.

Hand-geometry scanning process has following phases:

A. Image is acquired using a Charged Couple Device Camera.

B. If the pegs were used, delete pegs from the captured image.

C. The reference points captured are mapped onto a three-dimensional grid.

D. Reference values are calculated corresponding to the metrics being used and a template is generated.

E. The template is compared against the stored sample and decision is made.

In literature three categories for hand verification are proposed:

- Constrained and Contact based.
- Unconstrained and Contact based.
- Unconstrained and Contact-free.

Main advantage of using hand-geometry from user's perspective is that this system is easy to use. A low cost scanner can be employed, template size is also less (almost 9 bytes) and less complex algorithms are applied. Moreover, a hand-geometry scanner can work under varied environments and temperatures.

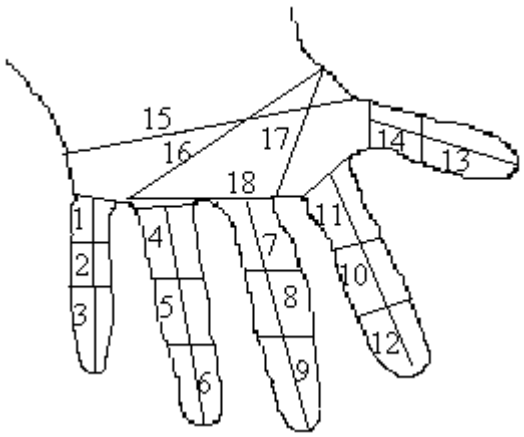

Figure 2: Representing Various Reference values

Hand-geometry is not distinctive. In this we look for moderately unique points and hence it is best suitable for verification and not identification purpose.

8. CONCLUSION

In this paper we presented an introduction to multi-biometric systems, their classification and various integration strategies. Multi-biometric systems employ more than one biometric trait and hence provide greater level of security as compared to unimodal biometric systems. A multi-biometric system based upon iris and hand-geometry is presented here. Iris being an internal organ of human eye remains unaffected by the outer environment and is almost impossible to imitate. Its patterns are complex and have a high degree of randomness in them. Iris scan is expected to be one of the most accurate biometric techniques. Hand-geometry measurements remain stable over time, have no effect of environment and are easy to obtain. Since hand-geometry patterns are not distinctive, they can be used only for verification. By integrating these patterns with iris patterns a multi-biometric system can be obtained for both verification and identification purpose. The proposed system also conforms to cost versus performance trade-off as hand-geometry scanning is less costly and iris is one of the most accurate biometric source of information.

9. REFERENCES

[1] S. Asha, Dr.C. Chellappan, "Authentication of E-Learners using Multimodal Biometric Technology", IEEE 2008.

[2] S.K. Dahel, Q. Xiao, "Accuracy Performance Analysis of Multimodal Biometrics", IEEE 2003.

[3] R. Zewail, A. Elsafi, M. Saeb, N. Hamdy, "Soft and Hard Fusion for Improved Identity Verification", The 47th IEEE International Midwest Symposium on Circuits and Systems, IEEE 2004.

[4]. Mohamed Deriche, "Trends and Challenges in Mono and Multi Biometrics", IEEE 2008.

[5]. M.K. Shahin, A.M. Badawi, M.E. Rasmy, "A Multimodal Hand, Vein, Hand Geometry, and Fingerprint Prototype Design for High Security Biometrics", Proceedings of the 2008 IEEE, CIBEC'08.

[6] Anil K. Jain, "An identity-Authentication system using Fingerprints", proceedings of the IEEE, vol. 85, No. 9, pp-1365-1387, September-1997.

[7]. Sanjay Kanade, Dijana Petrovska-Delacretaz, Bernadette Dorizzi, "Obtaining Cryptographic keys using feature level fusion of Iris and Face Biometrics for secure User Authentication", IEEE 2010.

[8]. Cheng Lu, Jisong Wang, Miao Qi, "Multimodal Biometric Identification Approach based on Face and Palmprint". Second International Symposium on Electronic Commerce and Security, IEEE 2009.

[9]. Javad Hashemi, Emad Fatemizadeh, "Biometric identification through Hand Geometry", EUROCON, IEEE 2005.

[10]. S.Y. Kung, Man-Wai Mak, "On Consistent Fusion of Multimodal Biometrics", ICASSP, IEEE 2006.

[11].C. Lupu, V. Lupu, "Multimodal Biometrics for Access Control in an Intelligent Car", International Symposium on Computational Intelligence and Intelligent Informatics, IEEE 2007.

[12]. Md. Maruf Monwar, Marina L. Gavrilova. "Enhancing Security through a Hybrid Multibiometric System", IEEE 2009.

[13]. Ryszard S. Chora´s, "Hybrid Iris and Retina Recognition For Biometrics", IEEE 2010.

[14]. Kia Yang, Eliza Yingzi Du, "Consent Biometrics", IEEE 2011.