Volume 3, No. 4, July- August 2012

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Novel Approach of Human Recognition using Multiple Traits

Arun Jain*
Research Scholar, Department of CSE
Singhania University,
Pacheri Bari ,Rajasthan ,India
erarunjain@rediff.com

Dr. Chander Kant Verma
Department of Computer Science and Application
Kurukshetra University,
Kurukshetra, Haryana, India
ckverma@rediffmail.com

Abstract: Biometrics is the discipline of recognizing a person's identity based on his/her physical or behavioural characteristics, Biometric systems for today's high security applications must meet stringent performance requirements Multiple biometric systems perform better than unimodal biometric systems. In this paper we propose a multimodal biometric system which employs iris and finger knuckle print . In this paper we will present a brief introduction about multimodal biometric systems, different levels of integration and some previous research work. In the last section , we have presented our proposed multi-biometric system.

Keywords: Knuckle Print Multiple Biometric, Feature extraction, Matching score, Authentication, Verification, Modalities.

I. INTRODUCTION

Biometric-based authentication systems represent a valid alternative to conventional approaches. Most of the biometric systems deployed in real world applications are unimodal which rely on the evidence of single source of information for authentication (e.g. fingerprint, face, voice etc.). Traditionally biometric systems, operating on a single biometric feature, have many limitations, which are as follows [1].

a. Trouble with data sensors: Captured sensor data are often affected by noise due to the environmental conditions (insufficient light, powder, etc.) or due to user physiological and physical conditions (cold, cut fingers, etc).
b. Distinctiveness ability: Not all biometric features have the same distinctiveness degree (for example, hand geometry-based biometric systems are less selective than the fingerprint-based ones).
c. Lack of universality: All biometric features are universal, but due to the wide variety and complexity of the human body, not everyone is endowed with the same physical features and might not contain all the biometric features, which a system might allow.

The term Multi Biometrics refers to the design of personal identity verification or recognition systems that exploit different biometric traits, multiple samples and multiple algorithms to establish the identity of an individual. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. These systems allow the integration of two or more types of biometric systems known as multimodal biometric systems. These systems are more reliable due to the presence of multiple, independent biometrics. Over any single biometric system, they have the advantage of increasing the population coverage, offering user choice, making biometric authentication systems more reliable and resilient to spoofing, and most importantly, improving the authentication performance[1]. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. The aim of multi biometrics is to reduce one or more of the following :

a) False accept rate (FAR)
b) False reject rate (FRR)
c) Failure to enroll rate (FTE)

Information fusion can in principle be performed at data, feature or decision level[2]. Although there may be merits in fusing information at low levels, from the multi biometric system design point of view, it is most appealing to focus on the decision level fusion, as in this way the construction of biometric experts can be delegated to specialist in the respective biometric modalities to be integrated. The logical consequence of this argument is that the fusion should be performed at the symbolic decision level where each expert has already determined the user's most likely identity. Some form of voting would then be sufficient to resolve any conflicts of opinions of a given set of experts. However, it has been demonstrated that the symbolic level fusion is not as effective as soft decision fusion, where the fusion process relates to the scores delivered by the experts for the respective hypotheses.

Biometric authentication is a chain process, as depicted in Figure 1

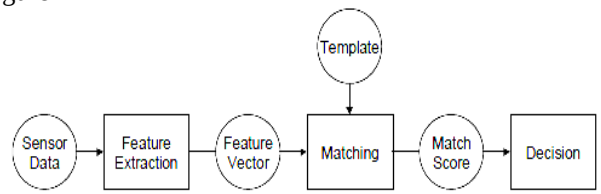

Figure 1: Authentication Process Flow

The performance of a Biometric system can be measured by reporting its False Accept Rate(FAR) and False Reject Rate(FRR) at various thresholds. These two factors are brought together in a receiver operating characteristic (ROC) curve that plots the FRR against the FAR at different thresholds A genuine matching score is obtained when two feature vectors corresponding to the same individual are

compared, and an impostor matching score is obtained when feature vectors from two different individuals are compared.

In particular, biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data acquisition in certain environments [3]. Multi biometrics is a relatively new approach to overcome those problems. Driven by lower hardware costs, a multi biometric system uses multiple sensors for data acquisition. This allows it to capture multiple samples of a single biometric trait and/or samples of multiple biometric traits.

In literature Jain and Ross [4] has discussed a multimodal biometric system using body weight and finger print and proposed various levels of combinations of the fusion. This is shown in Figure-2.

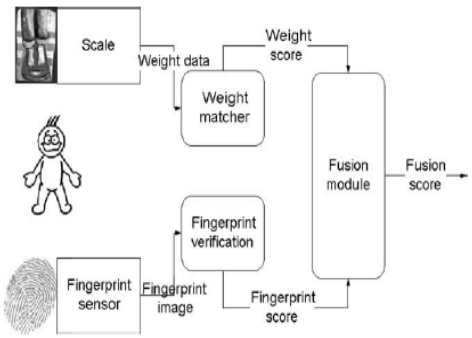

Figure 2 Multimodal biometric system using weight and fingerprint

II. CLASSIFICATION OF MULTIPLE BIOMETRICS

A multibiometric system relies on the evidence presented by multiple sources of biometric information. Based on the nature of these sources, a multibiometric system can be classified into one of the following six categories:[4] multi-sensor, multi-algorithm, multi-instance, multi-sample, multimodal and hybrid.

a. ***Multi-sensor systems:*** Multi-sensor systems employ multiple sensors to capture a single biometric trait of an individual. For example, a face recognition system may deploy multiple 2D cameras to acquire the face image of a subject; an infrared sensor may be used in conjunction with a visible-light sensor to acquire the subsurface information of a person's face. The use of multiple sensors, in some instances, can result in the acquisition of complementary information that can enhance the recognition ability of the system.

b. ***Multi-algorithm systems:*** Multi-algorithm systems consolidate the output of multiple feature extraction algorithms, or that of multiple matchers operating on the same feature set. These systems do not necessitate the deployment of new sensors and, hence, are cost-effective compared to other types of multibiometric systems. Lu et al [5]. discuss a face recognition system that combines three different feature extraction schemes (Principal Component Analysis (PCA), Independent Component Analysis (ICA) and Linear Discriminant Analysis (LDA)). The authors postulate that the use of different feature sets makes the system robust to a variety of intra-class variations normally associated with the face biometric.

c. ***Multi-instance systems:*** These systems use multiple instances of the same body trait and have also been referred to as multi-unit systems in the literature. For example, the left and right index fingers, or the left and right irises of an individual, may be used to verify an individual's identity. 2.4. Multi-sample systems: A single sensor may be used to acquire multiple samples of the same biometric trait in order to account for the variations that can occur in the trait, or to obtain a more complete representation of the underlying trait. A face system, for example, may capture (and store) the frontal profile of a person's face along with the left and right profiles in order to account for variations in the facial pose. Uludag et al. [6] discuss two such schemes in the context of fingerprint recognition.

d. ***Multimodal systems:*** Multimodal systems establish identity based on the evidence of multiple biometric traits. For example, some of the earliest multimodal biometric systems utilized face and voice features to establish the identity of an individual. Physically uncorrelated traits (e.g., fingerprint and iris) are expected to result in better improvement in performance than correlated traits (e.g., voice and lip movement). The cost of deploying these systems is substantially more due to the requirement of new sensors and, consequently, the development of appropriate user interfaces. The identification accuracy can be significantly improved by utilizing an increasing number of traits.

e. ***Hybrid systems:*** Chang et al.[7] use the term hybrid to describe systems that integrate a subset of the five scenarios discussed above. For example, Brunelli et al. [8] discuss an arrangement in which two speaker recognition algorithms are combined with three face recognition algorithms at the match score and rank levels via a HyperBF network. Thus, the system is multi algorithmic as well as multimodal in its design.

III. LEVEL OF INTEGRATION

As suggested in the literature [4], multibiometric systems are categorized into four system architectures according to the strategies used for information fusion:

a) Fusion at the Sensor Level
b) Fusion at the Feature Extraction Level
c) Fusion at the Matching Score Level
d) Fusion at the Decision Level

That is, we classify the systems depending on how early in the authentication process the information from the different sensors is combined. Fusion at the feature extraction level stands for immediate data integration at the beginning of the processing chain, while fusion at the decision level represents late integration at the end of the process. The following sections describe each of these architectures in detail and report on related research activities.

A. Fusion at the Sensor Level:

The raw biometric data (e.g., a face image) acquired from an individual represents the richest source of information although it is expected to be contaminated by noise (e.g., non-uniform illumination, background clutter, etc.). Sensor level [9] fusion refers to the consolidation of (a) raw data

obtained using multiple sensors, or (b) multiple snapshots of a biometric using a single sensor

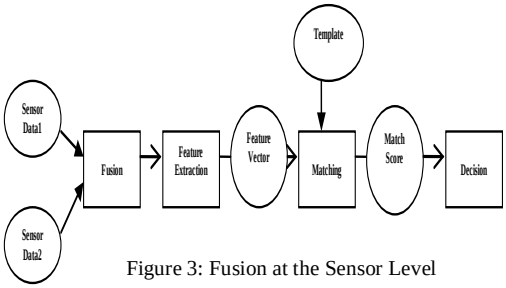

Figure 3: Fusion at the Sensor Level

B. Fusion at the Feature Extraction Level:

In feature-level fusion, the feature sets originating from multiple biometric algorithms are consolidated into a single feature set by the application of appropriate feature normalization, transformation and reduction schemes. In this architecture, the information extracted from the different sensors is encoded into a joint feature vector, which is then compared to an enrollment template (which itself is a joint feature vector stored in a database) and assigned a matching score as in a single biometric system .

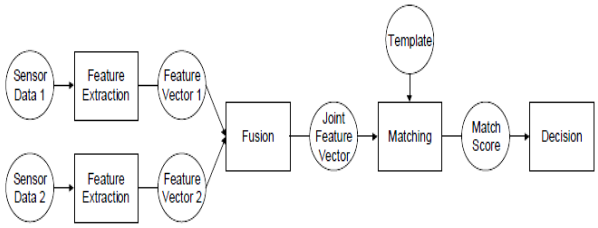

Figure 4: Fusion at the Feature Extraction Level

C. Fusion at the Matching Score Level:

A match score represents the result of comparing two feature sets extracted using the same feature extractor. A similarity score denotes how “similar” the two feature sets are, while a distance score denotes how “different” they are. In a multibiometric system built on this architecture, feature vectors are created independently for each sensor and then compared to the enrollment templates, which are stored separately for each biometric trait. Based on the proximity of feature vector and template, each subsystem now computes its own matching score. These individual scores are finally combined into a total score, which is handed over to the decision module. The whole process is shown in Figure 5:

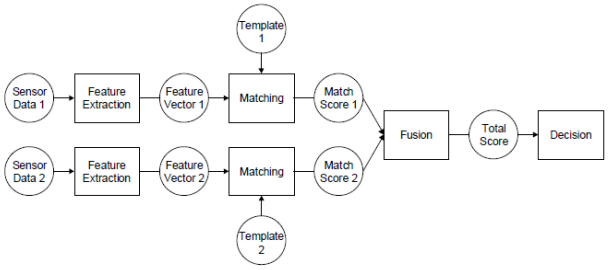

Figure 5: Fusion at the Matching Score Level

D. Fusion at the Decision Level:

In this fusion strategy, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote, as shown in Figure 6:

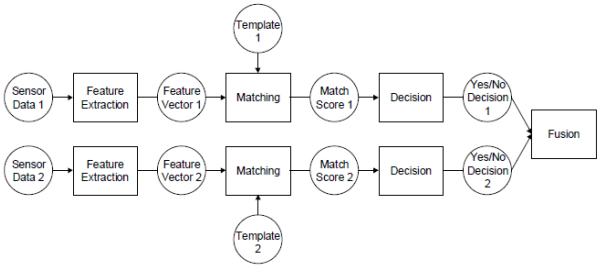

Figure 6: Fusion at the Decision Level

Fusion at the decision level [10] is a rather loosely coupled system architecture, with each subsystem performing like a single biometric system. Many different strategies are available to combine the distinct decisions into a final authentication decision. They range from majority votes to sophisticated statistical methods. In practice, however, developers seem to prefer the easiest method: boolean conjunctions. The renowned BioNetrix Authentication Suite, for example, offers the following combination strategies :

The AND rule requires a positive decision from all verification modules. While this will certainly lead to low false authentication rates, it will also result in high false rejection rates.

The OR rule attempts to authenticate the user using one biometric trait. If this fails, he is offered another attempt with another verification module. This policy is trading a low false rejection rate for a high false authentication rate.

IV. RELATED WORK

Recently, it has been noticed that the textures in the outer finger surface has the potential to do personal authentication. Woodward et al. [11] used the 3D range image of the hand to calculate the curvature surface representation of the index, middle, and ring fingers for similarity comparison. In 2006,

Kung et al. [12] 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 [13] 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. In 2009, Md. Monwar et al. [14] 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 [15] 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 [16]. 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.

V. PROPOSED SYSTEM

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

A. 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. 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.

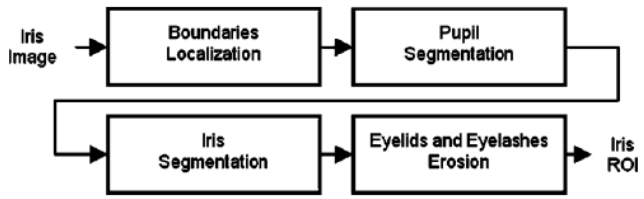

Figure 7. Iris ROI Extraction scheme of IRIS Region of Interest.

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.

B. Finger Knuckle Print:

The finger-knuckle print (FKP) refers to the image of the outer surface of the finger phalangeal joint. The FKP Recognition system has following phases:

a. First a specific data acquisition device is constructed to capture the FKP images.
b. The local convex direction map of the FKP image is extracted.
c. A region of interest (ROI) is cropped for feature extraction.
d. A competitive coding scheme, which uses 2D Gabor filters to extract the image local orientation information, is employed to extract and represent the FKP features.
e. Then FKP feature matching is done. Given two competitive code maps of two FKP images, a matching algorithm determines the degree of similarity between them.

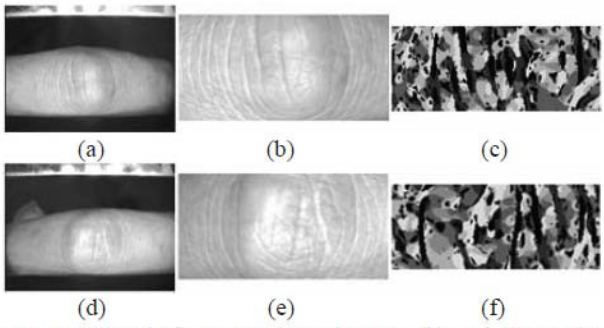

Figure 8 : Finger Knuckle print images (a) and (d); Region of interest (b) and (e); Code maps (c) and (f);

C. Fusion Scheme:

In this paper, several decision-level fusion rules are suggested to combine the Iris and knuckle print matchers. In specific, we can test our method with AND- and OR-voting rules, sum rule, as well as weighted sum rule. The AND- and OR-voting rules are the simplest fusion techniques. The AND-voting rule fusion decision is made only when all the classifiers agree. For OR-voting rule fusion, a decision is reached when one of the classifiers makes a decision.

On the other hand, sum rule takes the average of the scores from the two modalities. The summation of both single-modal classifier matching score or distance is calculated as

$$\mathbf{S= I_{ms} + K_{ms}}$$

Where I_{ms} and K_{ms} represent the matching score of Iris and knuckle print respectively and output the class with the smallest value of S. The main advantage of this rule is its simplicity, and the fact that it does not need any training. The last type of fusion scheme is the weighted sum rule. There exist different classifiers with different performances, thus weights can be used to combine the individual classifiers. Since only two models of biometrics are used in our system, the weighted sum Sw can be formed as

$$Sw=wI_{ms} +(1-w)K_{ms}$$

Where w is the weight that falls within value from 0 to 1.

VI. CONCLUSION

Multi biometric systems offer the scope for enhancing the reliability of automatic identity recognition and verification. We have discussed several different approaches to multibiometric systems. 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 finger knuckle print 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. Finger knuckle print measurements remain stable over time, have no effect of environment and are easy to obtain. By integrating Finger knuckle print 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 Finger knuckle print scanning is less costly and iris is one of the most accurate biometric source of information. Meanwhile, the proposed technique has advantages such as user friendliness, no remains, moderate size, cost-effectiveness, etc. It has a great potential to be future improved and employed in real applications.

VII. REFERENCES

[1]. Daugman, John. "Combining Multiple Biometrics". CambridgeUniversity,http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html

[2]. B. Ulery, A. Hicklin, C. Watson, W. Fellner, and P. Hallinan. Studies of Biometric Fusion. Technical Report NISTIR 7346, NIST, September 2006.

[3]. A. K. Jain, A. Ross, and S. Prabhakar. An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, 14(1):4–20, January 2004.

[4]. A. Ross, K. Nanda Kumar and A.K. Jain. Handbook of Multibiometrics. Springer, New York, USA, Ist edition,2006.

[5]. X. Lu, Y. Wang, and A. K. Jain. Combining Classifiers for Face Recognition. In IEEE International Conference on Multi -media and Expo (ICME), volume 3, pages 13–16, Baltimore, USA, July 2003.

[6]. U. Uludag, A. Ross, and A. K. Jain. Biometric Template Selection and Update: A Case Study in Fingerprints. Pattern Recognition, 37(7):1533–1542, July 2004.

[7]. K. I. Chang, K. W. Bowyer, and P. J. Flynn. An Evaluation of Multimodal 2D+3D Face Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(4):619–624, April 2005.

[8]. R. Brunelli and D. Falavigna. Person Identification Using Multiple Cues. IEEE Transactions on Pattern Analysis and Machine Intelligence, 17(10):955–966, October 1995.

[9]. R. Singh, M. Vatsa, A. Ross, and A. Noore. Performance Enhancement of 2D Face Recognition via Mosaicing. In Proceedingsof the 4th IEEE Workshop on Automatic Identification Advanced Technologies (AuotID), pages 63–68, Buffalo, USA, October 2005.

[10]. Prabhakar, S. and Jain, A. K. "Decision-level Fusion in Biometric Verification".Pattern Recognition v35 n4,2002,URL:http://www.cse.msu.edu/cgiuser/web/tech/document?NUM=00-24

[11]. D.L. Woodard and P.J. Flynn, "Finger surface as a biometric identifier", CVIU, vol. 100, pp. 357–384, 2005.

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

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

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

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

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