Global Journals Inc.

Global Journal of Computer Science and Technology
Volume 11 Issue 16 Version 1.0 September 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Multimodal Biometric Authentication System: Challenges and Solutions

By Shyam Sunder Yadav, Jitendra Kumar Gothwal , Prof. (Dr.) Ram Singh

Maharana Pratap University of Agriculture and Technology, Udaipur, Rajasthan, India

Abstract - Biometric technologies are automated methods for measuring and analyzing biological data, extracting a feature set from acquired data and comparing this set against to the templates set in the database. Unimodal biometric system have variety of problems such as noisy data, spool attacks etc. Multimodal biometrics refers the combination of two or more biometric modalities in a single identification. Most biometric verification systems are done based on knowledge base and token based identification these are prone to fraud. Biometric authentication employs unique combinations of measurable physical characteristics- fingerprint, facial features , iris of the eye, voice print and so on- that cannot be readily imitated or forged by others. This paper discuss the various scenarios that are possible in multi model biometric system , the level of fusion that are plausible and the integration strategic that can be adopted to consolidate information. Fusion methods include processing biometric madalitics sequential until an acceptable match is obtained.

Keywords : Multimodal Biometrics, Authentication, Templates, Fusion, Fingerprint.

GJCST Classification : H.2.8, D.2.9

Multimodal Biometric Authentication System: Challenges and Solutions

Shyam Sunder Yadav[α], Jitendra Kumar Gothwal[Ω], Prof. (Dr.) Ram Singh[β]

Abstract - Biometric technologies are automated methods for measuring and analyzing biological data, extracting a feature set from acquired data and comparing this set against to the templates set in the database. Unimodal biometric system have variety of problems such as noisy data, spool attacks etc. Multimodal biometrics refers the combination of two or more biometric modalities in a single identification. Most biometric verification systems are done based on knowledge base and token based identification these are prone to fraud. Biometric authentication employs unique combinations of measurable physical characteristics- fingerprint, facial features , iris of the eye, voice print and so on- that cannot be readily imitated or forged by others. This paper discuss the various scenarios that are possible in multi model biometric system , the level of fusion that are plausible and the integration strategic that can be adopted to consolidate information. Fusion methods include processing biometric madalitics sequential until an acceptable match is obtained.

Keywords : Multimodal Biometrics, Authentication, Templates, Fusion, Fingerprint.

I. Introduction

The need for reliable user authentication techniques has increased in the wake of heightened concerns about security and rapid advancements in networking, communication and mobility. Biometrics, described as the science of recognizing an individual based on her physiological or behavioral traits, is beginning to gain acceptance as a legitimate method for determining an individual's identity. Biometric systems have now been deployed in various commercial, civilian and forensic applications as a means of establishing identity. These systems rely on the evidence of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermo gram, signature, voice, etc. to either validate or determine an identity [2]. Most biometric systems deployed in real-world applications are unimodal, i.e., they rely on the evidence of a single source of information for authentication (e.g., single fingerprint *or* face). These systems have to contend with a variety of problems such as:

(a) Noise in sensed data : A fingerprint image with a scar, or a voice sample altered by cold are examples of noisy data. Noisy data could also result from defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user's face in a face recognition system). (b) Intra-class variations : These variations are typically caused by a user who is incorrectly interacting with the sensor (e.g., incorrect facial pose), or when the characteristics of a sensor are modified during authentication (e.g., optical versus solid-state fingerprint sensors). (c) Inter-class similarities : In a biometric system comprising of a large number of users, there may be inter-class similarities (overlap) in the feature space of multiple users. (d) Non-universality : The biometric system may not be able to acquire meaningful biometric data from a subset of users. A fingerprint biometric system, for example, may extract incorrect minutiae features from the fingerprints of certain individuals, due to the poor quality of the ridges. (e) Spoof attacks : This type of attack is especially relevant when behavioral traits such as signature or voice are used.

Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [5]. Such systems, known as *multimodal biometric systems*, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence [7]. These systems are able to meet the stringent performance requirements imposed by various applications. In this paper we examine the levels of fusion that are plausible in a multimodal biometric system, the various scenarios that are possible, the different modes of operation, the integration strategies that can be adopted and the issues related to the design and deployment of these systems.

Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. This technology acts as a front end to a system that requires precise identification before it can be accessed or used .Utilizing biometrics for personal authentication is becoming more accurate than current methods (such as the utilization of passwords or Personal Identification Number - PINs) and more convenient (nothing to carry

Author [α] : Research Scholar ,Department of Computer Sci. & Engg., NIMS University Jaipur ,Rajasthan, INDIA. Telephone : +91-9992443747 E-mail :ssyadav78@gmail.com

Author [Ω] : Research Scholar ,Department of Computer Sci. & Engg., NIMS University Jaipur ,Rajasthan, INDIA. Telephone : +91-941449128 8 E-mail : jkgothwal@rediffmail.com

Author [β] : Principal & Professor Department of Computer Science & Engg., MIT, Bikaner (Raj.), INDIA Rajasthan, INDIA. Telephone:+91-9460191291 E-mail : dr_ramsingh@yahoo.co.in

or remember). Thus, Biometrics is not just about security, it's also about convenience. The need for biometrics can be found in a wide range of commercial and military applications.

II. Biometric Identification System

A biometric system have five important modules: i) sensor module – which captures the trait in the form of raw biometric data, ii) feature extraction modules- which process the data to extract a feature set that is a compact representation of the trait, iii) matching module- which employs a classifier to compare the extract feature set with the stored templets to generate the matching scores, iv) decision module- which uses the matching score to either determine an identity or validate a claimed identity, v) system database module- which uses database pattern using pattern matching technique .

The main working operation that the system can perform are enrolment and testing. During enrolment biometric information of individual are stored, during test biometric information are dedected and compared with the stored ones. The sensor module the interface between real world an our system. We can say it is an image acquisition but it can change according to the characteristics we want to consider. The feature extraction module performs all the necessary preprocessing- it removes artifacts from the sensor, to enhance the input and use some kind of normalization. In the matching module we extract the features we need and choose which features to extract how to do it, with certain efficiency to create a template. After this in the matching module we are match the input pattern and the database pattern with the pattern matching technique. In the last module authentication occurs based on pattern matching technique.

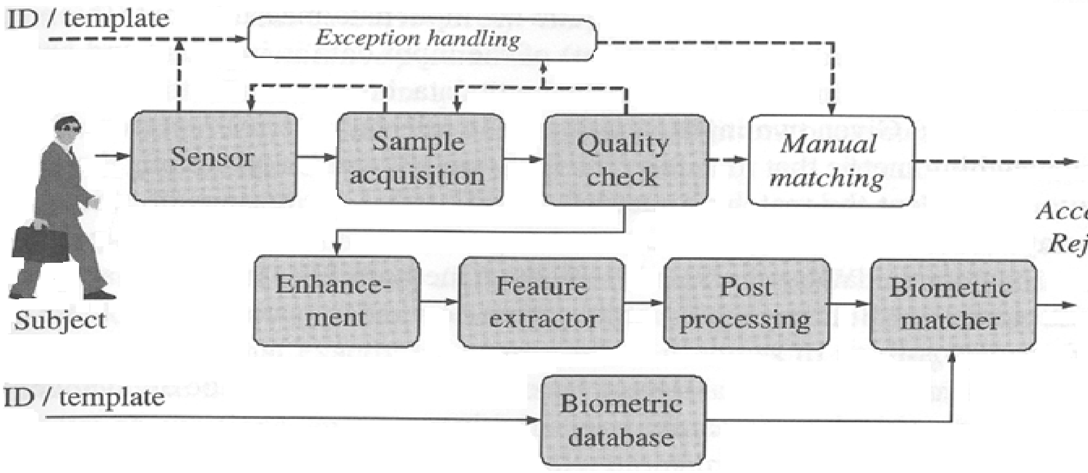

Figure 1

III. Proposed Multimodal Approach

Multimodal Biometrics System (MBS) strongly depend on the application scenario and refers to the use of a combination of two or more biometric modalities in a verification / identification system. The proposed system adopts identification based on multiple biometrics represents an emerging trend of an individual, to established the identity. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent. There are other reasons to combine two or more biometrics. One is that different biometric modalities might be more appropriate for the different applications. Another reason is simply customer preference.

The proposed system operates on five stages - stage-1 : the multiple sensor capture the raw biometric data and can be processed and integrate to generate a new data from which feature can be extracted, shown fig 2; stage-2: the preprocessor extract the necessary features that are subject to interest; stage-3: template will be generated for the extract features; stage-4: decision fusion integrate multiple cues ; stage-5: the input data will be compared with database data for matching. Finally a matching is genuine authentication is accepted, if not authentication is rejected

a) Proposed MBS Performance

The proposed system's performance is determined its accuracy. The main widely used standard metrics to determine the accuracy of a system are :

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artifacts or mimics

IV. Multimodal Biometric System Architecture

Here we discussed some of the existing architectures. A Multimodal biometric system using Face & Fingerprint, they have proposed various levels of combinations of the fusion this system is shown in Fig. 2.

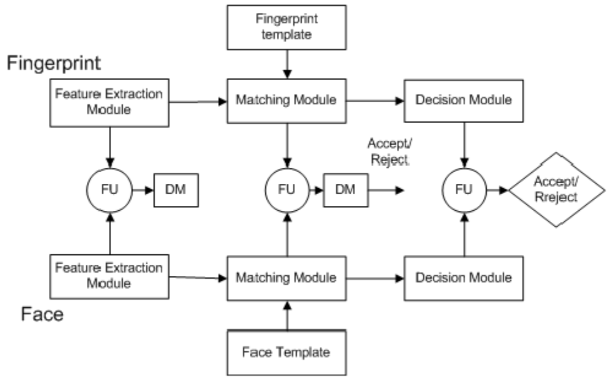

Figure 2 : Multimodal Biometric System using Face & Fingerprint

The promise of biometric technology for countering security threats Biometric authentication employs unique combinations of measurable physical characteristics--fingerprint, facial features, iris of the eye, voice print, hand geometry, vein patterns, and so on—that cannot be readily imitated or forged by others to determine or verify a person's identity. Initially the raw biometric data pertaining to multiple sensors are obtained. In our proposed system since we are using multiple biometric characters of an individual to establish identity. Here, we employ multiple sensors to Fig. 2 Proposed system an overview acquire data pertaining to different characters. The independence of the characters ensures good and reliable performance. Provide high level security by integrating the patterns by Decision level fusion.

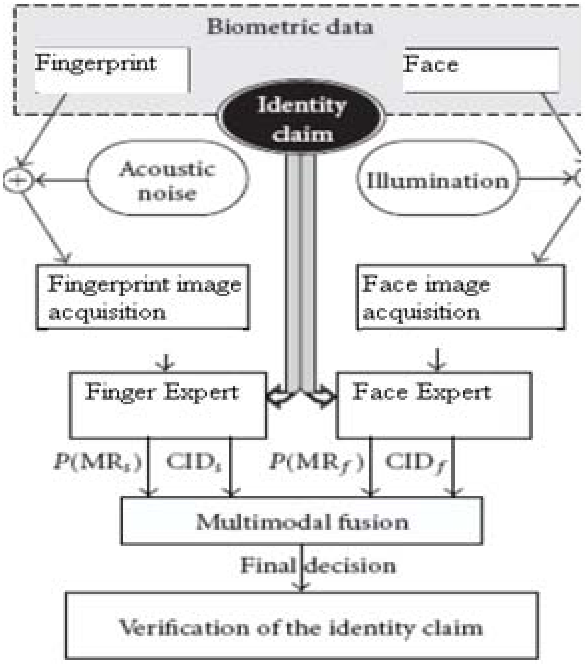

Figure 3 : Multimodal Biometric System with reliability information

V. Results

We took 09 combination sets of face images and fingerprint images from 80 users, to evaluate the performance of the proposed technique. By plotting the False Rejection Rate (FRR) against the False Accept Rate at various thresholds that summarizes the matching performance using ROC (Receiver Operating System). Using match score level fusion is 4.0 & 3.5 respectively with respect to Table i & ii, as per the databases shown in Figure 4 & 5. As expected, likelihood ratio based fusion leads to significant improvement in the performance. At a false accept rate of 0:001%, the improvement in the genuine Acceptance is achieved. FAR & FRR exits when the threshold level is >0.1

Result analysis of acceptance - Table (i)

Threshold	Finger	Face	Finger & Face
0.0	2	3	2
0.5	2	8	2
1.0	2	10	2
1.5	5	11	5
2.0	5	13	5
2.5	6	14	6
3.0	9	14	9
3.5	10	14	10
4.0	10	14	10

Receiver Operating Characteristics (ROC) Curve

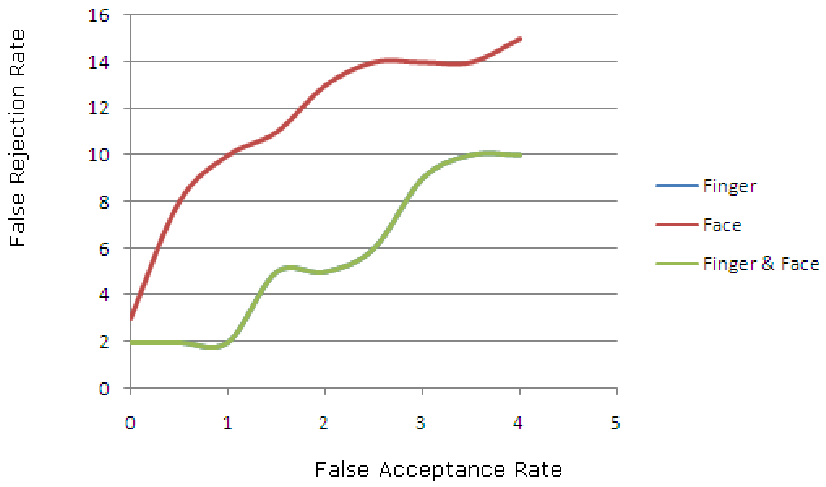

Figure 4

Result analysis of imposter

Threshold	Face	Finger	Finger & Face
0.0	4	2	2
0.5	8	3	3
1.0	14	5	5
1.5	14	8	8
2.0	14	8	8
2.5	14	9	9
3.0	14	10	10
3.5	14	10	10
4.0	14	10	10

Table (ii)

Receiver Operating Characteristics (ROC) Curve

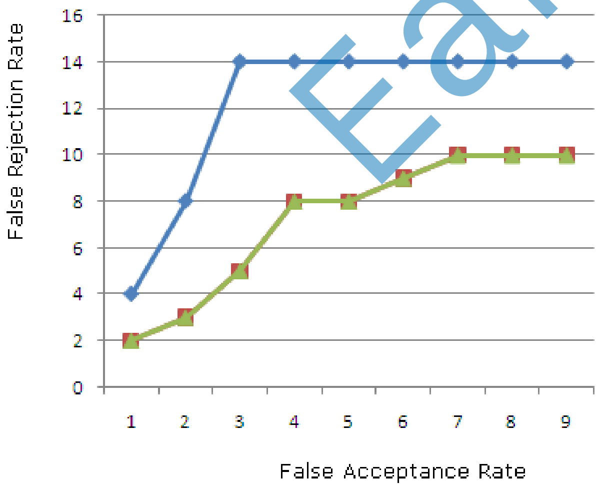

Figure 5

VI. Conclusions

Multimodal biometric systems elegantly address several of the problems present in ununimodal systems. By combining multiple sources of information, these systems improves matching performance, increase population coverage , deter spoofing and facilitate indexing . Various fusion levels and scenarios are possible in multimodal systems. Fusion at the match score level is most popular due to easy in accessing and consolidating matching scores, performance gain is pronounced when uncorrelated traits are use in multimodal system. With the wide spread deployment of biometric systems in several civilian and government applications. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of (a) reducing false acceptance and false rejection, (b) providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and (c) combating attempts to spoof biometric systems through non-live data sources such as fake fingers. The performance of multimodal biometric system shows great promise to personal identity in the biometric authentication society.

References Références Referencias

1. J.Wayman , A Jain, D. Maltoni, D.Maio, Biometric systems , Technology ,Degign Performance evaluation, Springer 2005.
2. A.K.Jain, A.Ross and S.Prabhakar, “An introduction to biometric recognition “, IEEE Trans. On Circuits and Systems for Video Technology, vol 14, pp. 4-20, Jan 2004.
3. Bounkong, S., Toch, B., Saad, D. and Lowe, D. (2003) ICA for watermarking digital images, Journal of Machine Learning Research, Pp. 1471-1498.
4. A.Ross , K.Nandakumar, and A.K.Jain, Handbook of Multibiometrics. Springer, 2006.

5. A.Ross and A.K. Jain, “Information fusion in biometrics”, Pattern Recognition Letters, vol. 24, pp. 2115-2125, Sep 2003.
6. K. Jain and U. Uludag, “Hiding biometric data,” IEEE Trans. Pattern Anal. Mach. Intelligence, vol. 25, no. 11, pp. 1493–1498, 2003.
7. L. I. Kuncheva, C.J. Whitaker, C.A. Shipp and R.P.W. Duin, “Is independence good for combining classifiers?”, in Proc. of International Conf. on Pattern Recognition, vol. 2, pp. 168-171, 2000.
8. D. Maltoni, D.Maio, A.K.Jain , S.Prabahakar, Handbook of finger print recognition , Springer 2003
9. M. Indovina, U. Uludag, R.Snelick, A. Mink and A.Jain, “Multimodal Biometric Authentication methods: A COTS Approach”.
10. R.M.Bolle, S.Pankati and N.K.Ratha, “Evaluation Techniques for Biometrics-Based Authentication Systems (FRR), “Proc. 15th Int’1 Conf.Pattern Recognition, vol 2, pp. 831-837, Sept.2000.
11. Teddy Ko,”Multimodal Biometric Identification for large user population using fringer print, face and iris recognition “, Proceedings of the 34th Applied Imagery and Pattern Recognition Workshop (AIPR05), 2005.
12. C.Soutar, “Biometric System Security”, White paper, Bioscrypt, http://www.bioscrypt.com.
13. N.Ratha, J.Connell, and R.Bolle,”Enhancing security and Privacy in biometrics-based Authentication Systems”, IBM Systems Journal, vol-40, no-3, pp-614-634, 2001.
14. R.W.Frischholz and U.Dieckmann,”Bioid: A Multimodal Biometric Identification System,” IEEE Computer, vol-33,no-2, pp. 64-68, 2000.
15. Monrose, F.,Rubin,A.D.,”Keystroke Dyanamics as a Biometric for Authentication” Future Generation computer systems, vol-16, no-4(2000) 351-359.
16. A.K.Jain and A.Ross, “Learning User-Specific Parameters in a Multibiometric System”,Proc. IEEE Int’1 conf. Image Processing , PP. 57-60, Sept. 2002.
17. A.K.Jain, K.Nandakumar, A.Ross, “Score normalization in multimodal biometric systems”, Pattern Recognition, 2005.
18. Richard W. Hamming. Error Detecting and Error Correcting Codes Bell System Technical Journal 26(2): 147-160, 1950
19. Y. Sutcu, Q.Li, and N.Memon, “Secure Biometric Template from fingerprint-face features”, in proceedings of CVPR Workshop on Biometrics , Minneapolis, USA, June 2007
20. Vetrro and N.Memon, “Biometric system security”, tutorial presented at second International Conference on Biometrics, Seoul, South Korea, August 2007.