A Multimodal Approach to Improve the Performance of Biometric System

Chander Kant[1]

Submitted in January 2015; Accepted in April, 2015

Abstract - Biometric systems have very success rate in identifying an individual based on ones biological traits. In biometric history some features like weight, age, height etc. are also there to provide user recognition to some extent but not fully upto the mark because of their changing nature according to time and environment. These features are called soft biometric traits. Soft biometric traits are lack of permanence but they have some positive aspects in respect of enhancing the biometric system performance. Here in this paper, we have also highlighting the similar point but with a new aspect that is integrating the soft biometrics with fingerprint and face for improving the performance of biometric system. Here we have proposed an architecture of three different sensors to evaluate the system performance. The approach includes soft biometrics, fingerprint and face features, we have also proven the efficiency of proposed system regarding FAR (False Acceptance Ratio) and total response time, with the help of MUBI tool (Multimodal Biometrics Integration).

Index Term - primary biometric, soft biometric, FAR, minutiae point, multimodal biometrics.

1.0 INTRODUCTION

Biometric systems automatically recognize the individuals based on their physiological and behavioural characteristics such as hand-geometry, fingerprint, iris, face, retina, voice, palmprint, signature, gait pattern and keystroke dynamics [1]. Unimodal biometric system used to recognize only a single trait. There are a number of problems such as noisy sensor data, non-universality and lack of distinctiveness of the chosen biometric trait, unacceptable error rates, and spoof attacks. On the contrast, Multimodal biometric systems help in solving the problems associated with unimodal biometric systems. In multimodal systems evidence can be obtained from multiple sources [2]. A multimodal biometric is expected to be more reliable than unimodal system. Multimodal system will have two major limitations. The first one is very high quality sensors and very large database is required that increases overall cost and the second limitation is Verification time is increased which causing inconvenience to the users.

Due to the no. of limitations, the identifiers in a multimodal biometric system are generally restricted to two or three. One of the possible resolutions to this problem is to use soft biometrics like height, weight, age, and eye colour. The information obtained from the soft biometrics is indistinctive, not reliable, and can be easily spoofed so it is not enough to establish the identity of a person. This paper describes an approach for integrating the information provided by the soft biometric traits (weight/height) with the input of the primary biometric system. The performance increase obtained from this integration with the input of a fingerprint and face biometric system (multimodal) is analyzed.

If the characteristics of soft biometric can be automatically extracted and used during the decision making process then the overall performance of the system will improve and the need of manual involvement will be reduced. Rest of the paper is organised as follows: section II describes related work, section III shows the proposed scheme, section IV describes mathematical formulas, section V extracts soft biometric, comparison of proposed scheme with existing biometric technologies explains in section VI, section VII shows result and finally conclusion and future prospect in section VIII.

2.0 RELATED WORK

The purpose to design biometric system for the identification of criminals [3]. Basically, the identification was based on three sets of features. First is an Anthropometric measurement: height of the arm, second, Morphological description: appearance and body shape like eye colour and anomalies of the fingers, and third is Peculiar marks: moles and scars observed on the body. This system was useful in tracking criminals but as the features like weight, height, age, gender are common and temporary. So this system had an unacceptably high error rate and not acceptable. The soft biometric traits can be classified into two categories: first is continuous (height, weight) and another is discrete (age, gender, eye colour) [4]. It was shown that a combination of personal characteristics like age, gender, eye colour, height, and other visible identification marks can be used to identify an individual only by a limited accuracy [5]. The use of soft biometric traits like gender and age, for organize a huge biometric database was invented later [6]. As shown below Figure 1 explains the fusion of soft biometrics (like height/weight) such as weight with the primary biometrics (finger print, face). Filtering is the process of restrictive the number of entries in a database to be searched that can be based on characteristics of the interacting user. For example, if gender of the user can somehow be identified, the number of search entries will be improved as the search can be restricted only to the subjects with this profile enrolled in the database. This greatly improves the speed or the search efficiency of the biometric system. Filtering and system parameters tuning require an accurate classification of a user into a particular class [7]. The accuracy and performance of multimodal biometric authentication systems is examined using

[1]*Assistant Professor, Department of Computer Science & Applications, K.U., Kurukshtra, Haryana, INDIA.*
E-mail:ckverma@rediffmail.com

state of the art Commercial Off-The-Shelf products [8]. Fusion of ear and soft- biometrics results in an improvement of approximately 5.59% over the primary biometric system i.e. ear [9]. Experiments on the MSU and NIST multimodal databases show that fusion rules achieve consistently high performance without adjusting for optimal weights for fusion and score normalization on a case-by-case basis [10]. A biometric approach can be used for continuous user authentication by fusing hard and soft traits [11]. The continuous user authentication using soft biometric traits can be used for E-learning purpose [12].

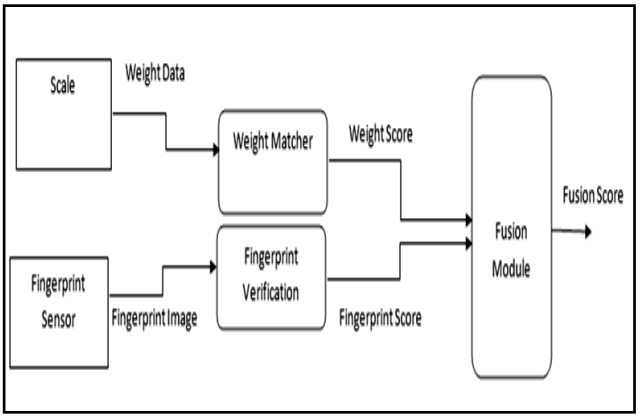

Figure 1: Fusion of Soft biometrics and primary biometrics

2.1 Soft Biometric Extraction

For using soft biometrics, a mechanism should be there to automatically (i.e. without user interaction) extract features from the user during the recognition phase [13]. This can be achieved using a particular system of sensors. For example, a collection of infrared beams could be used to measure the height, weighing machine can be used to measure the weight, a camera could be used for obtaining the facial image of the user, which can be used to obtain information like age, gender, and ethnicity [14]. The information obtained from soft biometrics could be used to count the identity information provided by the user's primary biometric identifier. Extensive studies have been made to identify the gender, ethnicity, and pose of the users from their facial images. The gender, ethnicity and pose of human faces are classified using a combination of experts by radial basis functions [15]. Their gender classifier can classify users as either male or female with a more than accuracy rate of 96 %. Age determination is a very difficult problem because physiological or behavioural changes in the human body are very limited as the person grows from one age to another [16]. Currently there are no reliable biometric indicators for age determination.

3.0 PROPOSED SCHEME

The proposed system combines the soft traits with fingerprint and face to get faster response time. Proposed method, as shown in figure 2, works by first comparing and matching soft biometric traits. If the result is not matched then it will directly rejects the user and if soft traits are matched then fingerprint and face traits are captured with the help of sensor. After that the feature sets of fingerprint and face are extracted. The system compares these values with the existing values in the database, and generates match scores of the respective traits. The system also generates the match score of soft trait. These match scores go through a (min-max) normalization process as explained in following section. After that the simple sum rule fusion technique is applied and a fusion match score is generated. If the resulting fusion score is equal to or above the set threshold value then the user is verified otherwise the system blocks the access and designate the user as imposter. There are number of advantages of proposed approach over the conventional system, as discussed below:

(i) The feature set of fingerprint and face are being calculated if and only if the user is found to be genuine at first stage (i.e. soft biometric phase)
(ii) This system improves the FAR(false accept rate)
(iii) Performance of the system improves.

The parallel execution of the process results in improved false acceptance rate. Though the proposed system improves the overall system performance yet it's not free from some drawbacks.

(i) Extra storage space is needed to store the templates with soft trait data like age, gender, height.
(ii) Total response time of the system increases for genuine user.
(iii) As the soft trait varies over period of time, the system must be used within those particular time period for which it remains invariant.

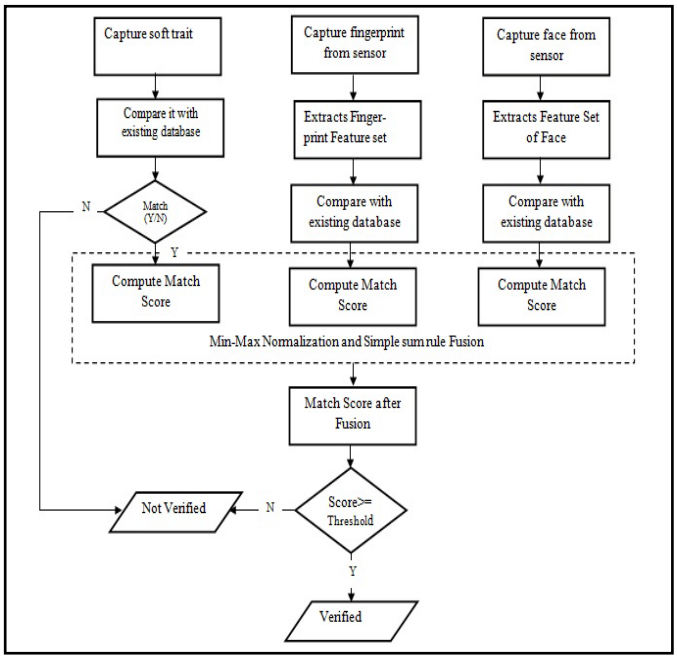

Figure 2: Proposed Scheme Architecture

Algorithm for verification/identification in proposed scheme

1) Capture Soft trait
2) Compare it with existing database
3) If (soft trait feature matched)
4) Compute match score of soft trait
5) Capture fingerprint from sensor
6) Extract fingerprint feature set
7) Compare with existing database
8) Compute fingerprint match score
9) Capture face from sensor
10) Extract feature set of face
11) Compare with existing database
12) Compute face match score
13) Apply (min-max) normalization on Soft, Finger and Face match scores
14) Apply simple sum rule fusion on normalized scores
15) If (fusion score >= threshold)
16) Verified/Identified
17) Else
18) Not Verified/Identified
19) End If
20) Else
21) Not Verified/Identified
22) End If
23) End

4.0 MATHEMATICAL FORMULAS

We are describing here in (min-max) normalization for score normalization and fusion formula to fuse the different modalities.

Let's matching score set is denoted as $\{S_k\}$ and normalized scores as $\{S'_k\}$:

- Min max normalization is top suited where the Upper and lower bounds (maximum and minimum values) of the scores produced by the matcher are known. This method is not vigorous; therefore, it is highly sensitive to outliers. [17]

$$S'_k = \frac{(S_k - \min)}{(\max - \min)}$$

If S_i is the matching score from i^{th} modality, S represents the resulting fused score.

- The *Simple Sum Rule* adds the scores as a linear transformation.

$$S = (a_1 S_1 - b_1) + \ldots + (a_n S_n - b_n)$$

a_i and b_i represents the weights and biases, respectively, which can be entered by the user.

5.0 COMPARISON OF PROPOSED SCHEME WITH EXISTING TECHNOLOGIES

The proposed scheme was implemented using MUBI software. Min-Max normalization and simple sum rule fusion method were used in the proposed scheme. The sample biometric data was taken from NIST website which is well recognized standards organisation. Figure 3-6 shows the comparison of proposed scheme on the basis of genuine acceptance rate and false acceptance rate.

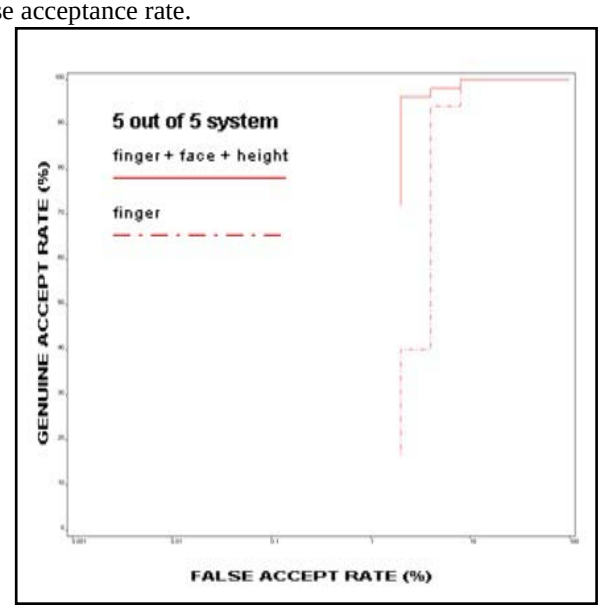

Figure 3: Proposed Scheme (i.e finger + face + height) v/s fingerprint system

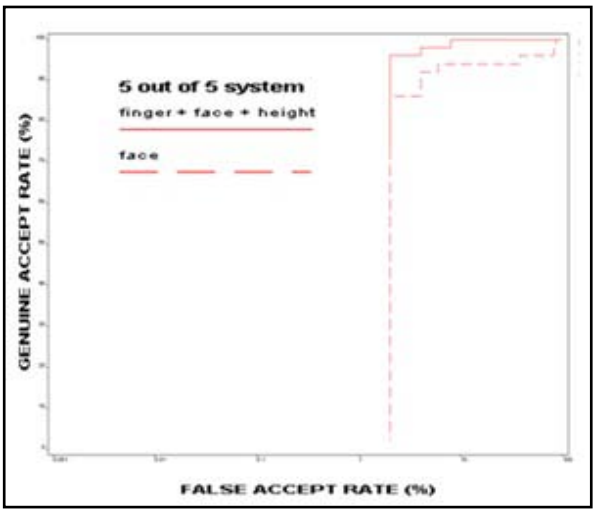

Figure 4: Proposed Scheme (i.e finger + face + height) v/s face system

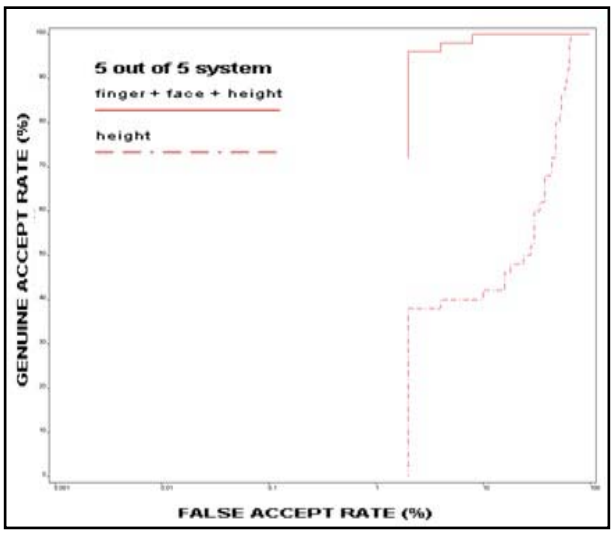

Figure 5: Proposed Scheme (i.e finger + face + height) v/s height system

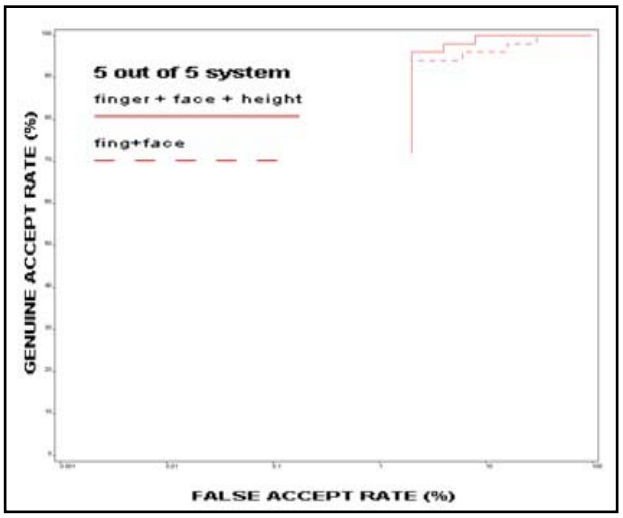

Figure 6: Proposed Scheme (i.e finger + face + height) v/s multimodal (i.e. finger + face) system

6.0 RESULT

Table 1: Comparison of proposed scheme with existing biometric techniques

S.No.	Biometric Technologies	GAR	FAR
1	Finger	72	3.946
	Proposed Scheme		1.859
2	Face	92	3.946
	Proposed Scheme		2.031
3	Height	72	47.106
	Proposed Scheme		2.051
4	Multimodal (finger+face)	95	5.623
	Proposed Scheme		1.943

It can be concluded from table 1 that the proposed scheme has improved false acceptance rate as compared to the other stated techniques.

7.0. CONCLUSION AND FUTURE SCOPE

This paper presents a simple and effective method of multimodal biometric authentication scheme based on soft biometric trait i.e. combination of fingerprint and face verification system. The proposed scheme shows that the soft biometric information such as blood group, gender, height, and age when combined with primary biometric traits will improve the performance of the traditional biometric systems. Methods to integrate time varying soft biometric information such as height and weight into the expected biometric framework is studied. This scheme allows us to completely control and automate fingerprint and face authentication with effective response time and FAR (False Accept Rate). Designed proposed scheme is not free from all loopholes. One of the negative aspects is that database will be very large due to accommodation of all the weight/ height, fingerprint and face template, therefore extra memory will be needed to store templates. As false rejection ratio is high in soft biometrics in future view, FRR can be improved and also a method can be developed for automatic extraction of soft biometric traits.

REFERENCES

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

[2]. 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.

[3]. Bertillon, A.: Signaletic Instructions including the theory and practice of Anthropometrical Identification, R.W. McClaughry Translation. The Werner Company (1896)

[4]. A. K. Jain, K. Nandkumar, X. Lu and U. Park, ―Imtegrating faces, fingerprints and soft biometrics traits for user recognition‖, in proceedings of ECCV international workshop on biometric authentication, volume LNCS 3087, pages 259- 269, prague, czeh republic, springer,may 2004.

[5]. Heckathorn, D.D., Broadhead, R.S., Sergeyev, B.: A Methodology for Reducing Respondent Duplication and Impersonation in Samples of Hidden Populations. In: Annual Meeting of the American Sociological Association, Toronto, Canada (1997)

[6]. Wayman, J.L.: Large-scale Civilian Biometric Systems – Issues and Feasibility. In: Proceedings of Card Tech / Secur Tech ID. (1997)

[7]. S. C. Dass, K. Nandakumar, and A. K. Jain. A Principled Approach to Score Level Fusion in Multimodal Biometric Systems. In Proceedings of Fifth International Conference on Audio- and Video-based Biometric Person Authentication (AVBPA), pages 1049–1058, Rye Brook, USA, July 2005.

[8]. K.Sasidhar, Vijaya L Kakulapati, Kolikipogu Ramakrishna and K.KailasaRao, Multimodal Biometric Systems – Study to improve accuracy and performance,

In: International Journal of Computer Science and Engineering Survey(IJCSES) Vol. 1, No. 2, November 2010

[9]. Shrikant Tiwari, Aruni Singh and Sanjay Kumar Singh, Fusion of Ear and Soft-biometrics for Recognition of Newborn, In: Signal and Image Processing : An International Journal (SIPU) Vol. 3, No. 3, June 2012

[10]. Sarat C. Dass, Karthik Nandakumar and Anil K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric Systems, In: proceedings of AVBPA 2005

[11]. A. Prakash, A Biometric Approach for Continuous User Authentication by Fusing Hard and Soft Traits, In: International journal of Network Security, Vol. 16, No. 1, PP. 65-70, Jan. 2014

[12]. Kalyani Tukaram Bhandwalkar and P. S. Hanwate, Continuous User Authentication Using Soft Biometric Traits for E-Learning, In : International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Special Issue 4, April 2014

[13]. X. Chen, P. J. Flynn, and K. W. Bowyer. IR and Visible Light Face Recognition. Computer Vision and Image Understanding, 99(3):332–358, September 2005.

[14]. Jain, A.K., Dass, S.C., Nandakumar, K.: Can soft biometric traits assist user recognition? In: Proceedings of SPIE International Symposium on Defense and Security: Biometric Technology for Human Identification . (2004)

[15]. E. Erzin, Y. Yemez, and A. M. Tekalp. Multimodal Speaker Identification Using an Adaptive Classifier Cascade Based on Modality Reliability. IEEE Transactions on Multimedia, 7(5):840–852, October 2005.

[16]. Jain, A.K., Dass, S.C., Nandakumar, K.: Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition. Proceedings of Biometric Authentication Workshop, LNCS 3087, pp. 259-269, Prague, May 2004.

[17]. A. K. Jain, A. Ross, and S. Prabhakar, “An Introduction to Biometric Recognition”, IEEE Transactions On Circuits And Systems For Video Technology, vol. 14, no. 1, pp. 4–21, January 2004