ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology
Volume 1, Issue 4, June 2012

A Multimodal Biometric System Using Fingerprint and Face

Sona Aggarwal, **Yogita Gulati**

***Abstract*— Biometric identification system, which uses physical or behavioral features to check a person's identity, ensures much greater security than passwords and number systems. Biometric features such as face or fingerprint can be stored on a microchip in credit card, for example. A single feature, however, sometimes fails to be exact enough to identification. Another disadvantage of using only one feature is that the chosen feature is not always readable; a multi-modal identification that uses two different features face, and fingerprint to identify people. With its two modalities, this achieves much greater accuracy than single-feature systems. Even if one modality is somehow disturbed, the ether one modality still leads to an accurate identification. This article goes into detail about the use of face and fingerprint modalities for identification.**

***Index Terms*— Face Recognition, fingerprint Verification, Performance Evaluation, Decision Fusion, Databases.**

I. INTRODUCTION

In recent years, biometric authentication has been considerable improvement in reliability and accuracy, with some of the traits offering better performance. However none of the biometrics are 100% accurate. Multimodal systems [7], remove some of the drawbacks of the uni-biometric systems by grouping the multiple sources of information. These systems utilize more than one physiological or behavioral characteristic for enrollment and identification/verification. Biometric systems utilizing personal physiological or behavioral characteristics[1] have become widely popular in providing security for information technology and entry to sensitive location like airports, governments, finance, health care, military, and any other type of business that connected by a network [4]. In today's electronically wired information society there are a number of situations e.g., accessing multiuser computer system which require an individual, these approaches have a number of significant drawbacks. Tokens may be stolen, lost, forgotten. Passwords may be forgotten or compromised. All these approaches are unable to differentiate between a valid user and an imposter. Therefore, token or knowledge based authentication does not provide sufficient security. Biometric system uses physiological or behavioral characteristics for identification [6]. These characteristics are unique to each user. It is more reliable and has a higher discrimination capability than token based and knowledge-based approaches, because the physiological or behavioral characteristics are unique for every user. Currently different types of biometric indicators are either widely used or are under intensive evaluation, including face, fingerprint, iris, gait, speech, key-stroke, hand geometry, facial thermo gram, signature, palm, etc. All these biometric indicators have their own advantages and disadvantages in terms of the accuracy, user acceptance etc.

In order to enable a biometric system to operate effectively in different applications and environments, a multimodal biometric system which makes a personal identification based on multiple physiological or behavioral characteristics is preferred. For example, a airport security system application where a biometric system is used for passenger authentication system. If a passenger cannot provide good finger print images (e.g. due to dust, dry finger, cuts, etc.) then the face may be better biometric indicator. If the "background" is cluttered, then the face location algorithm, which is necessary for face recognition, may not work very well. Then from these two indicators one of them may produce the accurate result.

Some work on multimodal biometric system has already been replaced in the literature. Dieck mann et. al[5] have proposed an abstract level fusion scheme: "2-from-3 approach", which integrate face, lip motion, and voice based on the principle that human user multiple clues to identify a person. Brunelli and Falavian[1] have proposed a measurement level scheme and a hybrid rank/measurement level scheme to combine the outputs of sub-classes. Jain et. al[2] have combining the three indicators Face, Fingerprint, and Speech, which have sufficient performance to identify authenticated user. Kittler et.al[10] have demonstrated the efficiency of an integration strategy which fuses multiple snapshots of a single biometric property using Bayesian framework. Bigun et. al[3] have proposed a Bayesian integration scheme to combine different pieces of evidence. Maes et. al[11]have proposed to combine biometric data (e.g., voice) with non-biometric data (e.g., password) .

Sona Aggarwal,M.Tech, Research Scholar, Dept. of Comp. Sc. & Engineering, H.C,T,M, Kaithal,Kurukshetra University, India, e-mail:sonaaggarwal56@yahool.com, M.No. 7206493254.
Yogita Gulati, M.Tech, Research Scholar, Dept. of Comp. Sc. & Engineering, H.C,T,M, Kaithal,Kurukshetra University, India, e-mail:yogitagulati1111@yahool.com, M.no. 9215653212

Multimodal biometric system which integrates face and fingerprint to make a personal identification[13]. The combination of these two specific biometric traits is based on the fact they have been used routinely in many communities. Most of the successful commercial biometric systems currently rely on both fingerprint and face. These biometric indicators complement one another in their advantages and strengths. While fingerprint provides an extremily high verification accurate result, it is difficult for an untrained human to match fingerprints. Face, on the other hand, is routinely used by all of us in our daily recognition tasks. Face and fingerprint verification system is targeted for verification applications to authenticate the identity claimed by a user such in a multiuser account authentication. The block diagram of verification system is shown in figure1, which mainly consists of four components (i) Acquisition module (ii) enrollment module (iii) template database (iv) verification module. The acquisition module is responsible for acquiring data samples

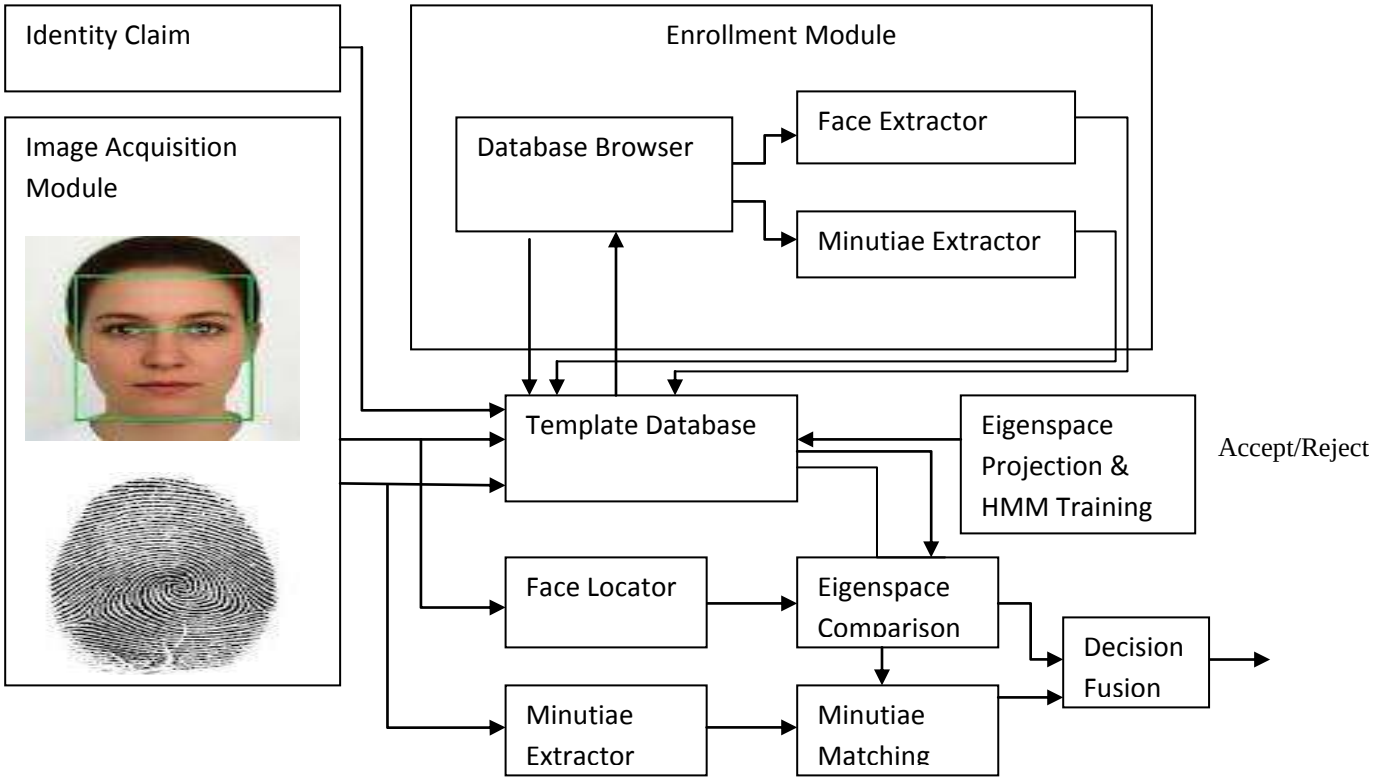


Figure 1: The block diagram of multimodal biometric system using face and fingerprint.

of face, fingerprints of a user who intends to access the system. The enrollment module is system management which includes user enrollment, training, user update etc. The template database is a physical database which contains all the template records of the user. The verification module is responsible for authenticating the identity claimed by a user at the point – of – access. The verification process essentially consists of three stages: i) Fingerprint verification, ii) face recognition, iii) decision fusion. Fingerprint verification is responsible for matching the input fingerprint against the fingerprint templates stored in the database to obtain the fingerprint matching score. Face verification is responsible for

matching the input face against the face templates stored in the database to obtain the face matching score. The decision fusion integrates the matching scores from fingerprint verification, face recognition to establish the final decision. The only valid user can access the system.

II. FORMULATION

Let β denote a given biometric system, and let $\phi^1, \phi^2, \ldots \phi^n$ denote the templates of the n users enrolled in β, who are labeled by numerical indicators, 1, 2, 3….n. Assume, for simplicity, that each enrolled user has only one template (for each type of indicator) stored in the system. So the template for ith user, $\phi^i = \{ \phi^i_1, \phi^i_2 \}$, has two components, where ϕ^i_1, ϕ^i_2 are the template for fingerprint and face respectively. Let

(ϕ^0, *I*) denote the biometric indicator and the identity claimed by a user. Again ϕ^0 has two components, $\phi^0 = \{ \phi^0_1, \phi^1_2 \}$, corresponding to the measurements of the two biometric indicators. The claimed identity, *I*, either belongs to category w1 or category w2, where w1 indicates that the user claims a true identity (a genuine user) and w2 that the user claims a false identity (an imposter). The biometric system β matches ϕ^0 against ϕ^1 to determine which category, w1 or w2 the claimed identity I falls in, i.e.

$$I \in \begin{cases} w_1, if\, \mathcal{F}\left(\Phi^0, \Phi^1\right) > \varepsilon, \\ w_2, otherwise, \end{cases} \quad (1)$$

Where *f* (ϕ^0, ϕ^1) is a function which measures the similarity between ϕ^0 and ϕ^1 and € is a threshold.

For a claimed identity *I* which can be in either w1 or w2, the biometric system may determine whether *I* is in w1 or w2. Therefore, there are a total of four possible outcomes: (i) a claimed identity in w1 is determined to be in w1, (ii) a claimed identity in w1 is determined to be in w2, (iii) a claimed identity in w2 is determined to be in w1, (iv) a claimed identity in w2 is determined to be in w2. Outcome (I) corresponds to a genuine user being accepted, outcome (ii) Outcome (i) corresponds to a genuine user being rejected, (iii) corresponds to an imposter being accepted, Outcome (iv) corresponds to an imposter being rejected. Obviously, outcomes (i) and (IV) are correct whereas outcomes (ii) and (iii) are incorrect. Ideally, a biometric system should make only accurate decisions. Due to large intraclass variations in the acquired digital representation of the biometric indicator decisions are unavoidable. Typically (i) false acceptance rate (FAR) and (ii) false reject rate (FRR) are used to characterize the performance of a biometric system. The false acceptance rate corresponds to the probability of outcome (iv) and the false reject rate is defined as the probability of outcome (ii). The lower the values of the FAR and FRR, the more reliable is the decision made by the system are determined by the inherent interclass and the intraclass variations of the indicator and the design (e.g., feature extraction, decision making) of the system.

A. Fingerprint Verification

Fingerprint recognition identifies people by using the impression made by the minute ridge formations or patterns found on the fingertips. Fingerprinting takes an image of a person's fingertips and records its characteristics – whorls, arches and loops are recorded along with patterns of ridges, furrows and minutiae. Information is processed as an image and further encoded as a computer algorithm. The two most prominent ridge characteristics, called minutiae are (i) ridge ending and, (ii) ridge bifurcation. Fingerprint verification depends on the comparison of minutiae and their relationships to make a personal identification. This usually consists of two stages [8]. (i) Minutiae extraction and (ii) minutiae matching. The minutiae extraction module extracts minutiae from input fingerprint image and the minutiae matching module determines the similarity of two minutiae patterns.

Let ϕ^i_1 denote the minutiae pattern extracted from the input fingerprint image with claimed identity *I* and ϕ^i_1 the *I*th fingerprint template stored in the database. The similarity function between an input fingerprint ϕ^0_1 and a template is defined as follows.

$$\mathcal{F}_1\left(\Phi^0_1, \Phi^I_1\right) = \frac{100C^2}{PQ} \quad (2)$$

Where P and Q are the total number of minutiae in ϕ^0_1 and ϕ^i_1 respectively and C is the total number of corresponding minutiae pairs between ϕ^0_1 and ϕ^i_1 established by the minutiae matching algorithm [8].

B. Face Recognition

Robust face recognition systems are in great demand to help fight crime and terrorism. There are two major tasks in face recognition (i) face location and, (ii) face recognition. Face location finds whether there is a face in the input image and if so, the location of the face in the image. Face recognition finds the similarity between the enrolled face and the stored templates to determine the identity of the user. In this system, the eigenspace approach [9] is used.

The eigenspace based recognition method is divided into two stages (i) training stage and, (ii) operational stage. In the training stage, a set of orthonormal images that best describe the distribution of the training facial images in a lower dimensional eigenspace is calculated. Then, the training facial images are project onto the eigenspace to generate the representation of the facial images in the eigenspace. In the operational stage a detected facial images is projected onto the same eigenspace and the similarity between the input facial image and the template is, thus calculated in the eigenspace. Let ϕ 02 denote the representation of the input face image with claimed identity I and ϕ i2 denote the representation of the Ith template. The similarity function between ϕ 02 and ϕ i1 is defined as follows:

$$\mathcal{F}_2\left(\Phi^0_2, \Phi^I_2\right) = -\left\|\Phi^I_2, \Phi^0_2\right\|, \quad (3)$$

Where $\| \bullet \|$ denote the L2 norm.

C. Decision Fusion

The final decision made by the system is based on integration of the decisions made by the fingerprint verification module, the face recognition module. If the output module of each level is category based, either W1 (claimed identity is true) or W2 (claimed identity is false). Which is not associated with any confidence, then the integration of these multiple decisions can only be performed at an abstract level, in which a majority rule can be employed to reach a more reliable decision [12]. If the output of each module is similar value, then more accurate decisions can be made at a rank

level or at measurement level by accumulating associated with each individual decision.

Let X1, X2 be the random variables used to indicate the similarity (dissimilarity) between an input and a template for fingerprint verification, face recognition respectively. Let Pj (Xj|Wi), where j=1, 2 and i = 1, 2 be the class- conditional probability density functions of X1, X2. Assume that X1, X2 are statically independent. Then, the joint class- conditional probability density function X1 and X2 has the following form:

$$\mathcal{P}\left(X_1, X_2/w_i\right) = \prod_{j=1}^{2} \mathcal{P}_j\left(X_j/w_i\right), i = 1,2 \tag{4}$$

Depending on the application requirement on verification accuracy, any one of a number of different statistical decision theory frameworks can be used. In biometrics, the performance requirements usually specified in terms of the FAR. In this case, the decision fusion scheme should establish a decision boundary which satisfies the FAR and minimizes the FRR. Let R2 denote two dimensional space spanned by (X1, X2); R21 and R22 denote the W1 region and W2 region respectively (R21+ R22) ; ϵ 0 denote the pre specified FAR. According to the Neyman Pearson rule, a given observation, X0 = (X01, X02), is classified as:

$$\left(X_1^0, X_2^0\right) \in \begin{cases} w_1, if \dfrac{\mathcal{P}_1\left(X_1^0, X_2^0/w_1\right)}{\mathcal{P}_2\left(X_1^0, X_2^0/w_2\right)} > \lambda \\ w_2, otherwise, \end{cases} \tag{5}$$

Where λ is the minimum value that satisfies the following:

$$\lambda = \frac{\mathcal{P}_1\left(X_1, X_2/w_1\right)}{\mathcal{P}_2\left(X_1, X_2/w_2\right)} and \tag{6}$$

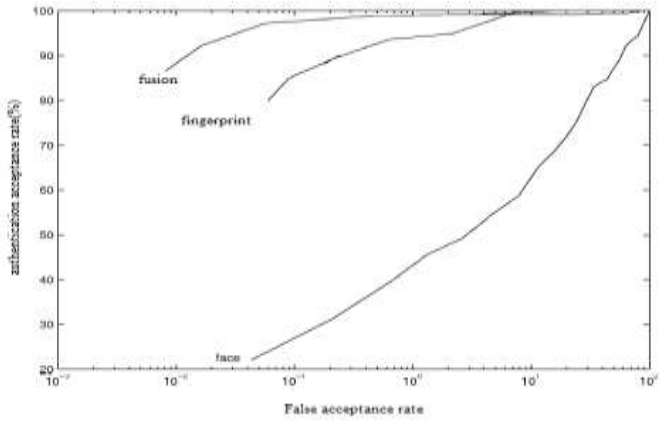
$$\in_0 = \int_{R_1} \mathcal{P}_2\left(X_1, X_2/w_2\right) dX_1 dX_2 \tag{7}$$

III. PERFORMANCE EVALUATION

The performance benchmark assesses the capability of the system at the point of identification, which depends how the system is used, how the users cooperate with the system, how the system produce the accurate result etc, . A test which simulates the operating environment is needed to access the performance benchmark of an implemented system. We have evaluated the performance of face and fingerprint recognition on a small piece of data

A. Databases

A training database of fingerprints and faces of 30 users collected. For each user, 10 fingerprint images (a total 300 images), 10 face images (a total 300 images), were acquired using an optical fingerprint scanner manufactured by digital biometrics with the restriction that fingers be placed approximately at the center of the scanner and the orientation of fingers be within 900. The face images were acquired using a Panasonic video camera under normal indoor lighting conditions. The rotation of the face was restricted to [-250, +250] and the scaling factor was allowed to be in the internal [0.90, 1.10]. Examples of acquired fingerprint images and face images are shown in figure 2. A test database involving 25 users (a subset of the 30 users in the training set) that were available during the second round of data, collection was collected . For each user, 15 fingerprint images



(a total of 375 images), 10 face images (a total of 250 samples) were collected.

The receiver operating curve of face recognition, and fingerprint verification are plotted in figure 3, in which the authentic acceptance rate (percentage) of genuine user being accepted, i.e. , 1- FRR) is plotted against FAR. We can conclude from this test the integration of fingerprints and face leads to an improvement in verification performance.

IV. CONCLUSION

In this paper the integration of face and fingerprint are discussed. The unimodal biometric system where one biometric trait is used not produced the accurate result. The combination of more than one biometric trait is multimodal that produces the efficient result. If one biometric trait is fail to identify the person then the other biometric trait is useful. By combining multiple biometric traits, the performance of biometric system can be improved. The multimodal biometrics is very popular in these days due to its performance and advance level of security. Though some complexity also exists in multimodal system which reduces its acceptability in many areas.

REFERENCES

[1]. Jain, A.K., Bolle, R., Pankanti, S., eds: Biometrics Personal identification in Networked security. Kluwer Academic Publishers (1999).

[2]. Anil Jain, Lin Hong, Yatin Kulkarni: A Multimodal Biometric System using Fingerprint, Face, and Speech , East cansina, MI 48824-1226.

[3]. E.S. Bigun, J.Bigun, B.Duc, and S.Fischer.Expert Conciliation for multimodal person authentication systems by Baysian statistics. In proc, 1st international conf. on audio video-based personal authentication, pages 327-334, crans-montana Switzerland, march 1997.

[4]. Multimodal biometric identification for large user population using fingerprint, face and iris recognition. IEEE print ISBN-0-7695-2479-6.
[5]. U. Dieckman P. Plankensteiner, and T. Wagner Sesam: A biometric person identification system using sensor fusion, pattern recognition letters, 18(9) : 827-833, 1997.
[6]. A. Jain, R. Bolle, and S. Pankanti, biometrics: Personal identification is networked society, Kluwer Academic Published, Boston, 1998.
[7]. A.K. Jain and A.Ross, " Multibiometric Systems", communications of the ACM, 47(1), pp. 34 - 40, 2004.
[8]. A. Jain, L. Hong, and R. Bolle. On-line finger-print verification. IEEE Trans. Pattern Anal. And Machine Intell., 19(4) :302-314, 1997.
[9]. M. Kirby and L. Sirvich. Application of the Karhunen-Loeve procedure for the characteristics of human faces. IEEE Trans. PAMI, 12(1) : 103-108, 1990.
[10]. J. Kittler, Y. Li, J. Mates and M.U. Sanchez Combiniy evidence in multimodal personal identity recognition system. In pros, 1st international conf. on audio video-based personal authentication, pages 327-334, crans-montana Switzerland, march 1997.
[11]. S. Maes and H. Beigi. Open sesame! Speech, password or key to secure your door? In Proc. 3rd Asian Conference on Computer Vision, pages 531-541, Hong Kong, China, 1998.
[12]. Y.A.Zuev and S.K. Ivanov. The voting as a way to increase the decision reliability. In Proc. Foundations of Information/Decision Fusion with Applications to Engineering Problems, pages 206-210, Washington, D.C., August 1996.
[13]. L. Hong and a. Jain. Integrating faces and fingerprints for personal identification. In proc.

Sona Aggarwal is pursuing her M.Tech in Computer Science and Engineering fromHaryana College of Technology & Management, Kaithal. She obtained her Master in Computer Application Degree from Punjab Technical University, Jalandhar in 2009.

Yogita Gulati is pursuing her M.Tech in Computer Science and Engineering from Haryana College Of Technology & Management, Kaithal. She obtained her Bachelor of Technology degree in computer science and engineering from N.C.C.E, Israna in 2010.