ISSN No. 0976-5697

Volume 4, No. 3, March 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Efficient Ways to Make Biometrics System More Effective

Er.Neeraj Jindal
Research Scholar: Electronics & Communication Engg.
Bhai Maha Singh College of Engineering
Muktsar, India
er.neerajjindal@yahoo.com

Er.Sona Aggarwal
Research Scholar: Computer Science & Engg.
Haryana College of Technology & Management
Kaithal, India
sonaaggarwal56@yahoo.com

Er.Shweta Lakhara
Research Scholar: Computer Science & Engg.
Sri Balaji College of Engineering & Technology
Jaipur, India
shwetalakhara026@gmail.com

***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 and more different features face, fingerprint and soft biometrics(height, gender)to identify people. With its 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, fingerprint and soft biometrics modalities for identification.

***Index Terms*—** Biometric System, Performance Evaluation, Objectives, integrating multiple traits

I. INTRODUCTION

Verifying the identity of a person is known as person recognition or authentication and it is a critical task in any Identity Management System (I.M.S).The three fundamental ways to establish the identity of a person are: 1. "something you know" (e.g., password, personal identification number- Knowledge based approach) 2. "something you carry" (e.g., physical key, ID card-token based approach) 3. "something you are" (e.g., face, voice) [1]. Since, the knowledge based and token based approaches are not based on any inherent attributes of an individual so they suffer from many disadvantages such as tokens may be lost, misplaced, or stolen, and a PIN may be forgotten by a valid user or can be guessed by an impostor. Both approaches are unable to differentiate between an authorized person and an impostor who fraudulently acquires the token or knowledge of the authorized person [GOR, 2003] [PRA, 2003]. Therefore, it is clear that only knowledge-based and token-based mechanisms are not sufficient for reliable identity determination and therefore stronger authentication schemes based on "something you are", namely Biometrics, are needed. Biometrics comes from the Greek words bios (Life) and metric's (Measure) [2].

Basically it is a pattern-recognition system which is used to identify or verify users based on his or her unique physical characteristics or behavioural characteristics.Biometric systems are becoming popular and have now been deployed in various commercial, civilian, and forensic applications for establishing identity [PAN, 2002].Biometric systems automatically determine or verify a person's identity based on his physical and behavioral characteristics such as fingerprint, face, signature, ear, odor, DNA, iris, voice and gait. These Biometric traits constitute a strong and permanent link between a person and his identity and these cannot be easily lost or shared or forged or forgotten.

II. BIOMETRIC SYSTEMS

Many physical and behavioral body traits can be used for biometric recognition system (as shown in Figure 1.1).Examples of physical traits include fingerprint, face, iris, palmprint, ear shape and hand geometry. Signature, gait, and keystroke dynamics are some of the behavioral characteristics that they can be used for person authentication. Each biometric trait has its own advantages and limitations, therefore no single trait can be expected to effectively meet all the requirements such as accuracy, practicality and cost imposed by all applications [3]. Therefore, there is no one universally best biometric trait and hence the choice of biometric depends on the nature and requirements of the given application. The relevance of a specific biometric to an application is established depending upon the nature and requirements of the given application, and the properties of the biometric trait [5] have identified seven characteristics that determine the suitability of a physical or behavioral trait can be used in a biometric application. These seven characteristics are given below:

a. ***Universality:*** Means that every person should possess the trait.
b. ***Uniqueness:*** Means that no two persons should be same in terms of trait.

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

c. ***Permanence:*** It means that the trait should be invariant with respect to time. A trait which changes significantly with respect to time is not a useful biometric.

d. ***Acceptability:*** It means that the extent to which people are willing to accept a particular biometrics in their daily life.

e. ***Performance:*** It means that the achievable recognition accuracy, speed, robustness, and the resources required achieving the accuracy and speed.

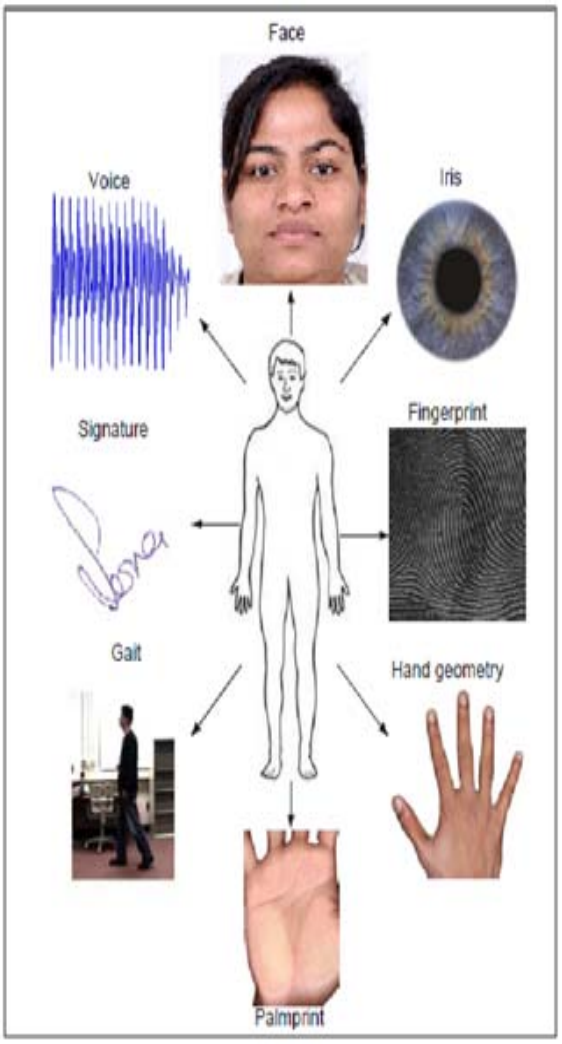


Figure 1.1: Different body traits that can be used for biometric recognition.

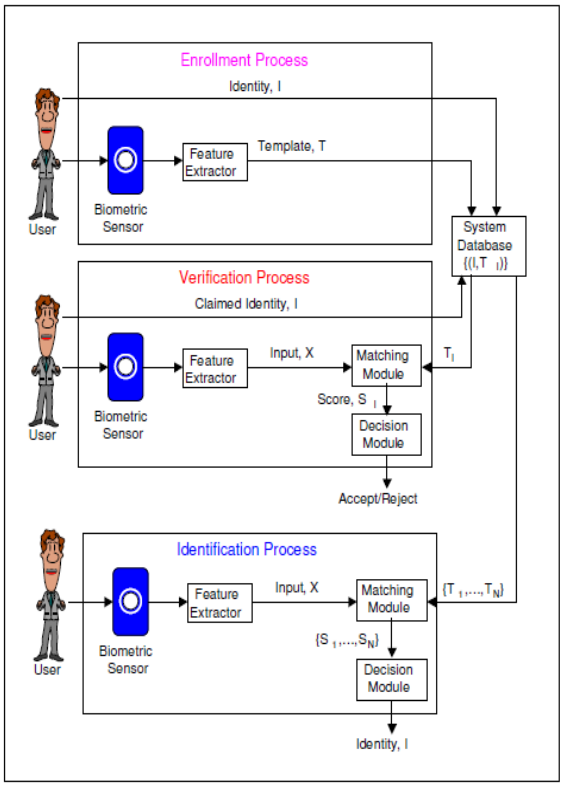
A typical biometric system consists of four modules. The sensor module is mainly responsible for acquiring the biometric data from an individual. The feature extraction module processes the acquired biometric data and extracts only the salient information to form a new representation of the data which is known as template. This new representation or template should be unique for each person and also relatively invariant with respect to changes in the different samples of the same biometric collected from the same person. The matching module compares the extracted feature set with the templates stored in the system database and determines the degree of similarity (dissimilarity) between the two. The decision module either verifies the identity claimed by the user or it determines the user's identity which is based on the degree of similarity between the extracted features and the stored templates in the system database.

The functionalities of a biometric system can be categorized1 as verification and identification. Figure 1.2 shows the enrollment and authentication stages of a biometric system which is operating in the verification and identification modes. In verification mode, the user claims an identity and the system verifies whether the claim is genuine or not. In this scenario, the given query is compared only with the template corresponding to the claimed identity. If the user's input and the template stored in the system database of the claimed identity have a high degree of similarity, then the claim is accepted as "genuine". Otherwise, the user claim is rejected and considered as an "impostor".

Identification functionality can be classified into positive identification and negative identification. In positive identification, the user attempts to positively identify himself to the system without any explicitly claiming an identity. A positive identification system determines the identity of the given user from a known set of identities. In contrast, the user in a negative identification application is considered as concealing his true identity from the system. Negative identification is also known as screening. This type of screening is often used at airports to verify whether a passenger's identity matches with any person on a "watch-list". Screening can also help to prevent the issue of multiple credential records (e.g., voter card, driver's license, passport etc.) to the same person. Negative identification also play an important role in critical applications such as welfare disbursement to prevent a person from claiming multiple benefits with different names. In both positive identification and negative identification, the user's biometric input is compared with the templates stored in system database of all the persons enrolled and the system outputs may be the identity of the person whose template has the highest degree of similarity with the user's input or a decision may be indicating that the user presenting the input is not an enrolled user.

It is clear that identification process is technically more challenging and costly. Accuracy of Identification generally decreases as the size of the database grows. Therefore records in large databases are categorized according to a sufficiently discriminating characteristic in the biometric data. Subsequent searches for particular records in the database are searched within a small subset only. This lowers the number of relevant records per search and increases the accuracy of the identification process [6]. The enrollment procedure as shown in Figure 1.2 registers individuals into the biometric system database and user's initial biometric samples are collected, assessed, processed, and stored for ongoing use in a biometric system database as templates

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India



III. BIOMETRIC SYSTEM PERFORMANCE

In case of Non-biometric systems, say password-based authentication systems they do not involve any complex pattern recognition techniques and hence almost perform accurately as intended by their system designers. On the other hand, biometric data and their representations in biometric systems are vary dramatically depending on the acquisition method, acquisition environment, user's interaction with the acquisition device, and in some cases variation in the traits due to various patho-physiological phenomena. There are many factors that affect the performance of a biometric system, some of them are concisely described below [JAI, 2006]:

a. ***Inconsistent Presentation:*** Data captured by the sensor from a biometric trait depends upon the intrinsic characteristic of a biometric trait, the way of biometric trait presented and the user interaction with the acquisition interface. For example, due to change in pose, an appearance based on face recognition system may not match images successfully. Since different acquisitions may represent different poses of the face. Similarly hand geometry measurements may be based on different projections of hand on a planar surface. Different iris/retina acquisitions may also correspond to different non frontal projections of iris/retina on to the image planes.

b. ***Imperfect Data Acquisition:*** In practical situations the data acquisition conditions are not perfect and cause extraneous variations in the acquired biometric sample. For example, non uniform contact results in poor quality fingerprint acquisition. That is, the ridge structure of a finger would be completely captured only if ridges belonging to the part of the finger being imaged are in complete physical/optical contact with the image acquisition surface and the valleys do not make any contact with the image acquisition surface. However, the dryness of the skin, shallow/worn-out ridges (due to aging/genetics), skin disease, sweat, dirt, and humidity in the air all confound the situation resulting in a non ideal contact situation. Different illuminations may cause conspicuous differences in the facial appearance. Backlit illumination may render image acquisition virtually useless in many applications.

IV. CHALLENGES IN UNIBIOMETRIC SYSTEMS

As compared to the traditional methods of person recognition biometrics provides greater security, but there are many challenges in biometric technology. Jain etal. [JAI, 2004] discusses the following three challenges in biometric technology.

a. ***Accuracy:*** In biometric system there are two types of matching errors: false match and false non-match.

a) ***False Match (or False Accept):*** It means that the biometric system incorrectly declares a successful match between the input pattern and a non-matching pattern in the database (in the case of identification) or the pattern associated with an incorrectly claimed identity (in the case of verification). In a biometric system, it should be minimized as possible and ideally it should be zero.

b) ***False Non-match (or False Reject):*** It means that the biometric system incorrectly declares failure of match between the input pattern and a matching pattern in the database (in the case of identification) or the pattern associated with the correctly claimed identity (in the case of verification). In a biometric system, it should be minimized as possible and ideally it should be zero.

In addition to matching errors, the biometric system can make two types of acquisition errors– failure to capture and failure to enroll, which are also necessary to calculate the accuracy and performance of a biometric system.

a) ***Failure to Capture (FTC):*** It is defined as proportion of attempts for which a biometric system is unable to capture a sample of sufficient quality when the biometric characteristic is presented to it e.g., an extremely faint fingerprint or an occluded face.

b) ***Failure to Enroll (FTE):*** It is defined as proportion of the user population for which the biometric system is unable to generate reference templates of sufficient quality. This includes those who, for physical or behavioral reasons, are unable to present the required biometric feature.

b. ***Security:*** In spite of many advantages of biometrics-based personal authentication systems over traditional security systems based on token or

CONFERENCE PAPER
II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

knowledge, they are vulnerable to attacks that can decrease their security considerably. Ratha et al. [RAT, 2001A] analyzed these attacks, and grouped them into eight classes. Figure 1.3 shows these attacks along with the components of a typical biometric system that can be compromised [JAI, 2005A].

Type 1st attack on the sensor level involves presenting a fake biometric (e.g., synthetic fingerprint, iris, face etc.). Submitting a previously intercepted biometric data constitutes the second type of attack (replay). In the third type of attack, the feature extractor module is compromised to produce feature values already selected by the attacker. Genuine feature values are replaced with the ones selected by the attacker in the fourth type of attack. Matcher can be modified to output an artificially high matching score in the fifth type of attack. The attack on the template database (e.g., modifying an existing template, adding a new template, removing templates, etc.) constitutes the sixth type of attack. The transmission medium between the template database and matcher is attacked in the seventh type of attack, resulting in the alteration of the transmitted templates. Finally, in type 8th attack the matcher result (accept or reject) can be overridden by the attacker.

The main problems of biometric systems are identified as the lack of secrecy and non-replace ability. In addition to this, there are other attacks that can be launched against an application whose resources are protected using biometrics [ULU, 2004]. Maltoni et al. [MAL, 2003] describe typical threats for a generic authentication system, which includes repudiation, circumvention, covert acquisition, collusion, coercion, and Denial of Service (DoS).

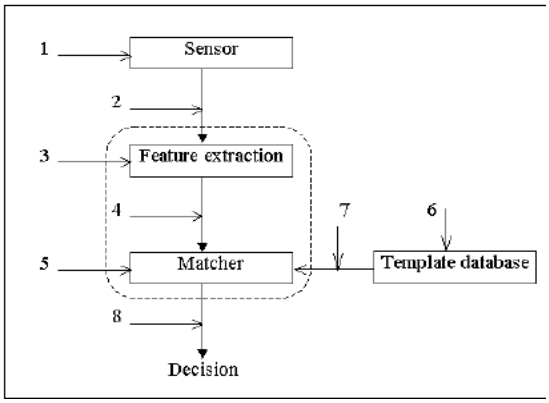


Figure 1.3: Various attacks locations in a biometric system

a) Privacy: The ability to lead one's life free of intrusions, to become autonomous, and to control access to one's personal information. As the incidence and magnitude of identity fraud cases increases, strong biometrics such as fingerprints increasingly comes into play for positively recognizing people. The conventional technologies whether knowledge based or token based cannot deliver privacy [JAI, 2004A]. On the other hand, biometrics based accesses are less reputable than other types of access control mechanisms. Therefore, biometric traits can clearly enhance the integrity of systems holding personal information [PRA, 2003].

A reliable biometric system can provides an irrefutable proof of identity of the person. However, biometrics involves various privacy concerns. Consequently, the users have multiple concerns: Will the undeniable proof of biometrics-based access be used to track the individuals that may violate an individual's right to privacy and anonymity? Will the biometric data be abused for an unintended purpose, e.g., will the fingerprints provided for access control is matched against the fingerprints in a criminal database? Will the biometric data be used to cross-link independent records from the same person, e.g., health insurance and grocery purchases? How would one ensure and assure the users that the biometric system is being used only for the intended purpose and none other?

A. Fingerprint:

The analysis of fingerprints for matching purposes generally requires the comparison of several features of the print pattern. These include patterns, which are aggregate characteristics of ridges, and minutia points, which are unique features found within the patterns. It is also necessary to know the structure and properties of human skin in order to successfully employ some of the imaging technologies. 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 $\square^{i}_{1}$ denote the minutiae pattern extracted from the input fingerprint image with claimed identity I and $\square^{i}_{1}$ the Ith fingerprint template stored in the database. The similarity function between an input fingerprint $\square^{0}_{1}$ and a template is defined as follows.

$$\mathcal{F}_1\left(\Phi^{0}_{1}, \Phi^{I}_{1}\right) = \frac{1\,0\,0\,C^{2}}{P\;Q} \qquad (2)$$

Where P and Q are the total number of minutiae in $\square^{0}_{1}$ and $\square^{i}_{1}$ respectively and C is the total number of corresponding minutiae pairs between $\square^{0}_{1}$ and $\square^{i}_{1}$ established by the minutiae matching algorithm [8].

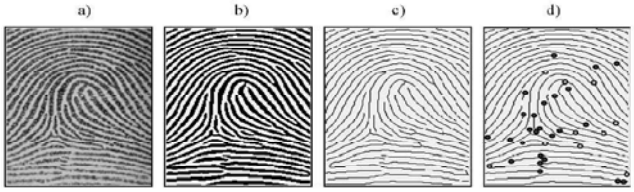


Figure1.4: Fingerprint Recognition

CONFERENCE PAPER II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

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 □02 denote the representation of the input face image with claimed identity I and □i2 denote the representation of the Ith template. The similarity function between □02 and □i1 is defined as follows:

$$\mathcal{F}_2\left(\Phi_2^0, \Phi_2^I\right) = -\left\|\Phi_2^I, \Phi_2^0\right\|, \qquad (3)$$

Where □•□ denote the L2 norm.

V. PROPOSED OBJECTIVE

This paper is about integrating Multiple Traits in Biometric System Primary Biometrics (Face, Fingerprint & Hand Geometry) with Soft Biometrics (Height, Gender) . We have developed a mathematical modal based on Bayesian decision theory for integrating primary & soft cues at Score level which play an important role for making final decision for automatic recognition of individuals.

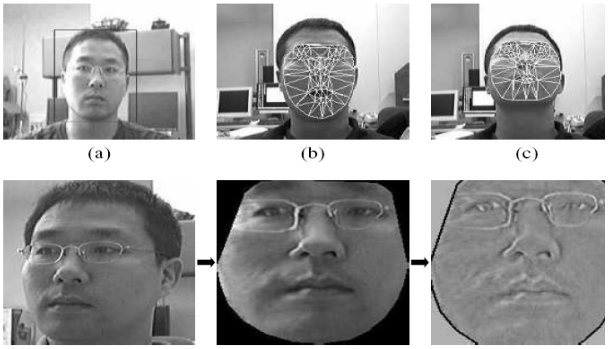
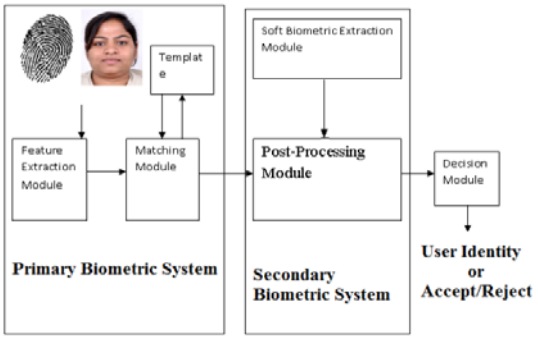


Figure1.5: Face Recognition

VI. PROPOSED METHOD FOR INTEGRATING MULTIPLE TRAITS IN BIOMETRIC SYSTEM

The method of carrying out an exhaustive search for the weights of the soft biometric identifiers is computationally inefficient and requires a large training database. Since the weights are used mainly for reducing the dynamic range of the log-likelihood values,



VII. CONCLUSION

it is possible to develop simple heuristics for computing the weights efficiently. Time-varying soft biometric identifiers such as age, height and weight cannot handle by the Bayesian framework in its current form. Therefore there is a need to investigate methods in future for the soft biometric framework to incorporate such identifiers.

VIII. 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, YatinKulkarni: 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

CONFERENCE PAPER II International Conference on
"Advance Computing and Creating Entrepreneurs (ACCE2013)"
On 19-20 Feb 2013
Organized by
2nd SIG-WNs, Div IV & Udaipur Chapter , CSI , IEEE Computer Society Chapter India Council ,
IEEE Student Chapter Geetanjali Institute of Technical Studies, Udaipur, Rajasthan, India

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.

[14]. A. K. Jain, K. Nandakumar, X. Lu, and U. Park, "Integrating faces, fingerprints, and soft biometric traits for user recognition," in NCS3087, pp. 259–269, 2004.

[15]. A. K. Jain, S. Prabhakar, and S. Pankanti, \On the similarity of identical twin fingerprints," Pattern Recognition, vol. 35, no. 8, pp. 2653-2663, 2002.