Model of Hybrid Biometric System

Priyanka Deore[1], Tushar Chaudhari[2]
1 Lecturer, pursing ME (Computer Engineering) YTCEM, Mumbai, India
2Lecturer,S.H.Jondhale Polytechnic, Mumbai, India

Abstract— Biometrics refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. Biometric technologies are used to provide high security by using personal physical and behavioral characteristics. This technology acts as a entry pass to a system that requires identification before it can be accessed or used. Utilizing biometrics for personal authentication is becoming more accurate and secure than current methods (such as the utilization of passwords or Personal Identification Number - PINs) and more convenient (nothing to carry or remember). Thus, Biometrics is not just provides *security,* it's also about *convenience.* The need for biometrics can be found in a wide range of commercial and military applications where high level of security is required.

Most biometric systems deployed in real-world applications are unimodal, such as they use a single source of information for authentication (e.g., single fingerprint, face, voice etc.). Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. If we use combination of this biometrics it will provide extra level of security. It overcomes the limitations of the previous methods and gives extra level of security. It also reduces FAR (False Acceptance Rate), FRR (False Rejection Rate).

Keywords—*Introduction, Biometric system, Biometric system errors, Limitations of biometric system, Multimodal biometric system, Conclusion, References.*

*****

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics and traits. It uses person's physical and behavioral characteristics for securing any system. Biometric identification (or biometric authentication) is used in computer science as a form of identification and access control. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Biometric technologies are automated methods of verifying or recognizing the identity of a living person based on a physiological or behavioral characteristics. In a biometric identification system, the identity corresponding to the input data (probe/investigation) is typically determined by comparing it against Physiological characteristics are related to the shape of the body. For Examples fingerprint, palm print, face recognition, DNA, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the pattern of behavior of a person, including but not limited to typing rhythm, gait, and voice.

- *<u>Fingerprint Recognitions</u>:*

Human fingerprints unique one. They are detailed, difficult to alter, and durable over the life of an individual making them suitable as long-term markers of human identity. Fingerprints, as shown in Fig. (a) are unique and consistent over time and hence being used since a long time. A fingerprint is a pattern of ridges and valleys on the surface of a fingertip. It contains shapes like crossover, core island, delta, poreetc. The fingerprint recognition is important in forensic science for detecting crime scene. Ridges are the upper skin layer segments of the finger and valleys are the lower segments. The various kinds of discontinuities in ridges (minutiae) have sufficient discriminatory information to recognize fingerprints. Ridge bifurcation (where the ridge splits) and ridge ending (where the ridge ends) are the important minutiae points. Minutiae-based fingerprint recognition usually represents fingerprint by these two ridge characteristics called as minutiae. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Availability of multiple fingerprints of a person makes fingerprint recognition suitable for use in large-scale identification involving millions of identities. However, the problem with the large scale fingerprint recognition system is the requirement of huge amount of computational resources, especially in the identification mode.

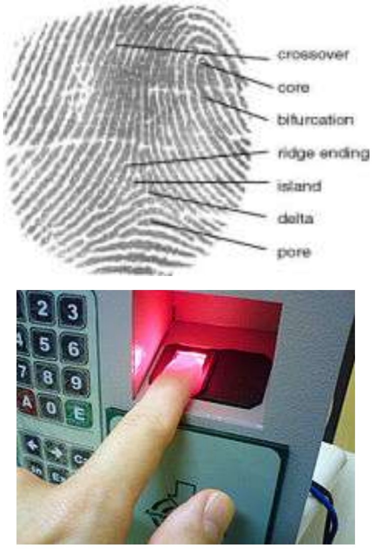

Fig. (a) Fingerprint Recognition

- *Face Recognition:*

Face recognition as shown in Fig (b) is a computer application for automatically identifying or verifying a person from a digital image or a video frame from a video source. One of the ways to do this is by comparing selected facial features from the image and a facial database. The dimensions, proportions and physical attributes of a person's face are unique. The Fig. (b) Shows that application scans person face by using sensor and plot grid on it to locate facial features. That plotted grids are stored in data base with unique ID for further use. Next time when person need access to the system, the application first persons face using sensor, again plot the grid and then compared that grids with the facial templates stored in the database. If match is found then person get access to the system. One popular approach to face recognition is based on the location, dimensions and proportions of facial attributes such as eyes, eyebrows, nose, lips, and chin and their spatial relationships. Another approach being widely used is based on the overall analysis of the face image that represents face as a weighted combination of a number of canonical faces. Face recognition involves two major tasks: i) face location and ii) face recognition. Face location is determining the location of face in the input image. For recognizing the located face, the Eigen face approach is one of the very popular methods. The Eigen face-based recognition method consists of two stages: i) training stage and ii) operational stage. In the training stage, training set of face images are acquired. The acquired face images are projected into lower dimensional subspace using Principle Component Analysis (PCA). A set of images that best describe the distribution of training images in a lower dimensional face space (the Eigen space) is computed. Then the training facial images are projected into this Eigen space to generate representation of the training images in the Eigen space. In the operational stage, the input face image is projected into the same Eigen space that the training samples were projected into. Then, recognition can be performed by a classifier operating in the Eigen space.

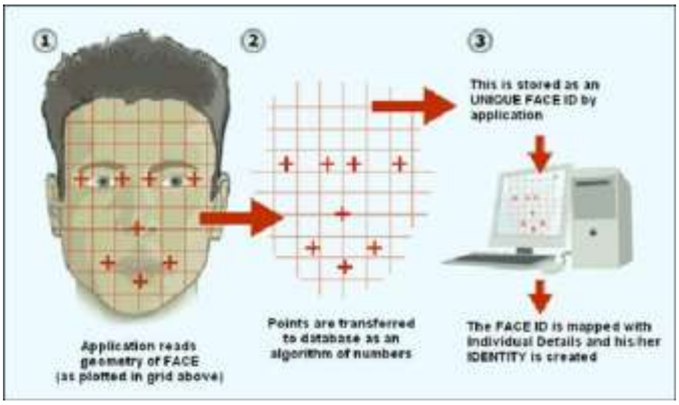
1
2
3
This is stored as an UNIQUE FACE ID by application
Application reads geometry of FACE (as plotted in grid above)
Points are transferred to database as an algorithm of numbers
The FACE ID is mapped with Individual Details and his/her IDENTITY is created

Fig (b) Face Recognition

- *Iris Scan:*

The iris shown in Fig (c). The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. Iris of the each personisunique. The accuracy and speed iris scan system is good. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost-effective.

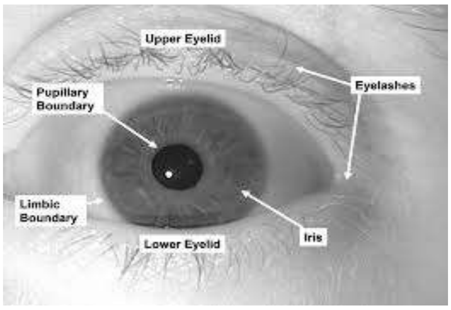

Fig (c) Iris Scan

- *Hand Geometry:*

Hand geometry is a biometric that identifies users by the shape of their hands. Hand geometry recognition systems, as shown in the Fig (d) are based on the different measurements such as shape of the hand, size of palm, lengths and widths of the fingers, space between fingers and thickness of hand. Hand features are not very distinctive. They are suitable for verification but not for identification. In certain situations such as immigration and border control, biometrics such as fingerprints may not be suitable because they infringe on privacy. Hand geometry is less secured because size and shape on the hand may be changed over time. In such situations hand geometry can be used for verification as hand geometry is not very distinctive. Hand geometry features may not be invariant during the growth period of children. The size of such recognition systems is large and hence it is difficult to embed the systems in other devices such as laptops. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry based systems.

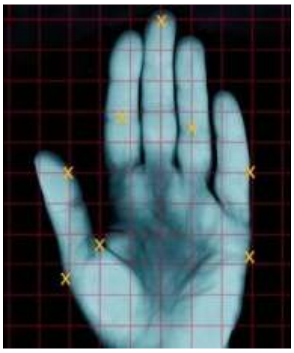

Fig. (d) Hand Geometry

II. BIOMETRIC SYSTEM

Biometrics is assuming a noteworthy part in everywhere throughout the world in robotized individual distinguishing proof frameworks sent to improve security. Fig (e) demonstrates the biometric framework. The qualities of individuals may shift starting with one individual then onto the next. Numerous qualities of the human are interesting which are utilized for remarkable recognizable proof. This interesting property is utilized by the Biometric innovation to unmistakably distinguish every individual. Biometric framework is basically an example acknowledgment framework which perceives a client by deciding the legitimacy of a particular physiological or behavioral trademark controlled by the client. A few critical issues must be considered in outlining a useful biometric framework. Initial a client must be selected in the framework so that his biometric layout can be caught. This layout is safely put away in a focal database or a brilliant card issued to the client. The format is recovered when an individual should be distinguished. Contingent upon the connection, a biometric framework can work either in check (confirmation) or a recognizable proof mode.

A biometric system is pattern recognition system that scan the biometric feature, extract features and that with templates stored in database. This system is works either in verification mode or identification mode. In verification mode, person's identity like ID, PIN or username is compared with the captured templates. In the identification mode, all the templates in database is compared with the scaned features.

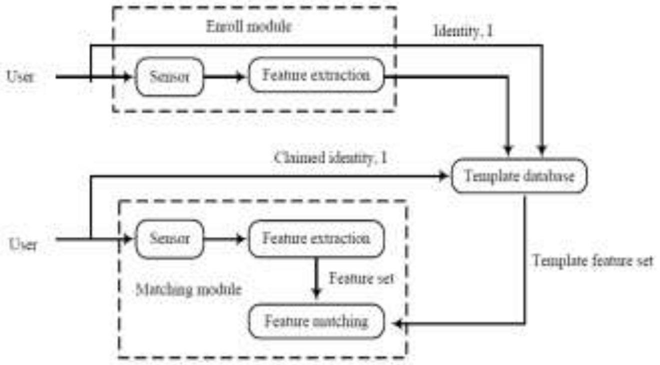

Fig (e) Block Diagram of Biometric System

III. BIOMETRIC SYSTEM ERRORS

A biometric verification system makes two types of errors:
1. Mistake occasionally made by biometric security systems is False Acceptance. In an instance of false acceptance, an unauthorized person is identified as an authorized person.

2. Second Mistake occasionally made by biometric security systems is False Rejection. In an instance of false rejection, the system fails to recognize an authorized person and rejects that person as an impostor.

IV. LIMITATIONS OF (UNIMODEL) BIOMETRIC SYSTEMS

The successful installation of biometric systems in various civilian applications does not imply that biometrics is a fully solved problem. Biometric systems that operate using any single biometric characteristic have the following limitations.

1) *Noisy data*. The sensed data might be noisy or distorted. Fingerprints with a scar or a voice altered by cold are examples of noisy data. Noisy data could also be the result of 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). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

2) *Intra-class variations*. The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor or when sensor characteristics are modified (e.g., by changing sensors—the sensor interoperability problem) during the verification phase.

3) *Non-universality*. While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users to not possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges. Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait.

4) *Spoof attacks Problem*. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demonstrated that it is possible (although difficult and requires the help of a legitimate user) to construct artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system.

V. MULTIMODAL BIOMETRIC SYSTEMS

A percentage of the impediments forced by unimodal biometric frameworks can be overcome by utilizing numerous biometric modalities, (for example, face and unique finger impression of a man or various fingers of a man). Such frameworks, known as multimodal biometric frameworks or Hybrid Biometric System, are required to be more dependable because of the nearness of different, free bits of proof. These systems are additionally ready to meet the stringent execution requirements imposed by different applications. Multimodal biometric systems address the issue of non-all-inclusiveness, since multiple qualities guarantee adequate populace scope. Further, multimodal biometric frameworks give against satirizing measures by making it troublesome for a gatecrasher to at the same time parody the multiple biometric attributes of a honest to goodness client. By asking the user to present an irregular subset of biometric characteristics (e.g., right index and right center fingers, in a specific order), the framework guarantees that a "live" client is undoubtedly present at the purpose of information obtaining. Fig (f) demonstrates characterization of multimodal biometric framework were we can utilize fingerprints of two fingers or blend of unique mark and iris filter and so forth.

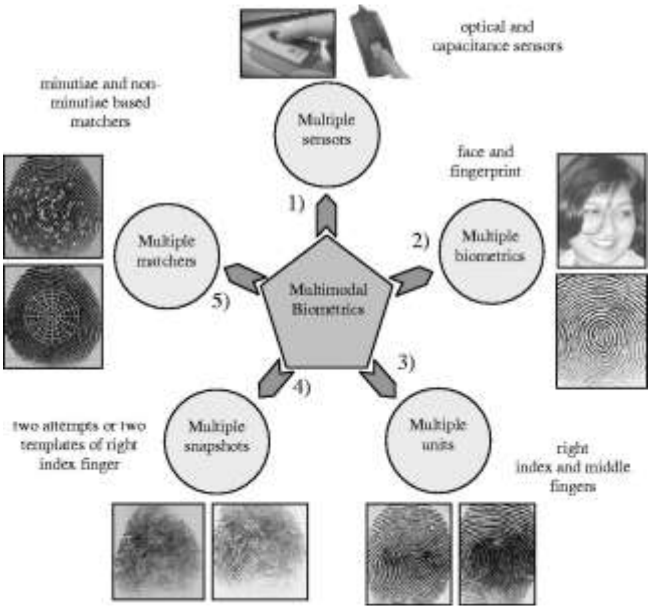
optical and capacitance sensors
minutiae and non-minutiae based matchers
Multiple sensors
face and fingerprint
1)
2)
Multiple matchers
Multiple biometrics
Multimodal Biometrics
5)
3)
4)
two attempts or two templates of right index finger
Multiple snapshots
Multiple units
right index and middle fingers

Fig. (f) Hybrid Biometric System

Multi-biometric systems can remove some of the drawbacks of the uni-biometric systems by grouping the multiple sources of information. Multimodal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example, a system combining face and iris characteristics for biometric recognition would be considered a “multimodal” system regardless of whether face and iris images were captured by different or same imaging devices.

Although a multimodal biometrics system helps us to reduce:

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

It also increases:

- Sensor cost
- Enrollment time
- Transit times
- Need for a prior knowledge/data
- System development and complexity

VI. PROPOSED SYSTEM

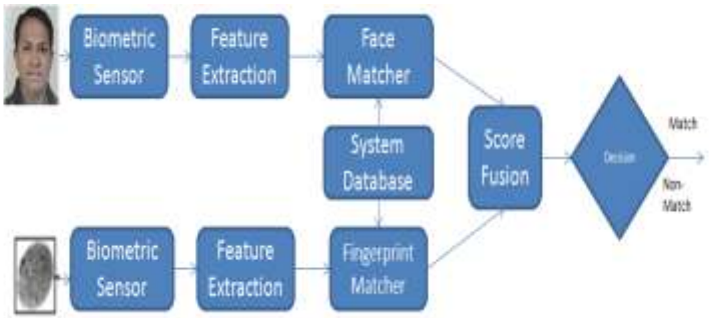

Fig.(g) Block Diagram of Proposed Hybrid Biometric System

The proposed system uses face recognition and fingerprint recognition for biometric system. This system will use two sensors. One for extracting the features of the face and other is for extracting fingerprint features then match with already stored templates are done. On all combinations the score fusion is applied on it and on the value of score fusion decision is made whether that person is authenticate person or not. In detailed we can say that sensor takes biometric image and compare it to stored templates. The result is a match score, which is used for decision making. It decides whether person is authenticated person or not.

Fig. (h) Shows the improvement with hybrid biometric system. Graph shows that True acceptance rate in hybrid biometric system is more than fingerprint recognition and face recognition because of combination. Were false rejection rate of hybrid biometric system is less that fingerprint recognition but somewhat more than face recognition. Face recognition system is less accurate than Hybrid biometric system and fingerprint recognition. Hybrid biometric system is more secured and accurate than unimodel biometric system.

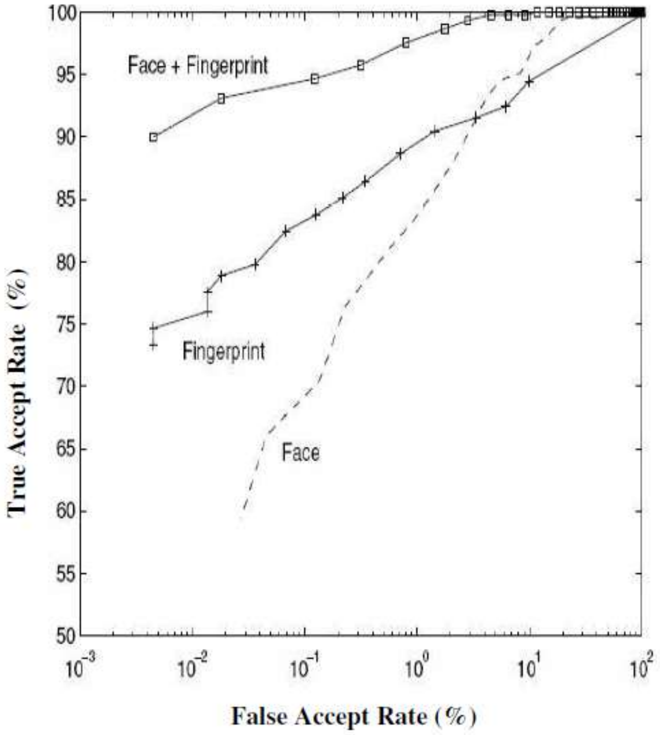

Fig. (h) Improvement with Hybrid Biometric System

VII. CONCLUSION

Unimodel or single model biometric system has many limitations and low security because it uses only one biometric feature. False acceptance rate and false rejection rate is more in unimodel biometric system. To overcome this problem multimodel biometric system is useful. A multimodal biometric system uses multiple biometric features of the person for recognition it provides high range of security. Because of multiple biometric features this system becomes slow and complex.

REFERANCES

[1] "Index Codes for Multibiometric Pattern Retrieval" AglikaGyaourova and Arun Ross, IEEE transactions on information forensics and security, vol. 7, no. 2, April 2012

[2] "Multimodal Biometric Identification for Large User Population Using Fingerprint, Face and Iris Recognition", Teddy Ko, 0-7695-2479-6/05 $20.00 © 2005 IEEE

[3] "Towords efficient privacy preserving two stage identification for fingerprint based biometric cryptosystems" Benjamin Tams ;Biometrics (IJCB), 2014 IEEE International Joint Conference on [::Biometrics::] Compendium, IEEE

[4] A. Gyaourova and A. Ross, "A coding scheme for indexing multimodal biometric databases," in Proc. IEEE Computer Society Workshop on Biometrics at the Computer Vision and Pattern Recognition (CVPR) Conf., Miami, FL, Jun. 2009.

[5] "Hybrid Multi-Biometric Person Authentication System" Tran Binh Long and Le Hoang Thai, Proceedings of the World Congress on Engineering and Computer Science 2012 Vol I WCECS 2012, October 24-26, 2012, San Francisco, USA

[6] A. Ross and A.K. Jain, "Information Fusion in Biometrics", *Pattern Recognition Letter* 24, pp.2115-2125, 2003.

[7] ISO/IEC JTC 1/SC 37 Biometrics, *Working Draft Technical Report on Multi-Modal and Other Multi-Biometric Fusion*, August 2005.

[8] "Summary of NIST Standards for Biometric Accuracy, Tamper Resistance, and Interoperability," November 13, 2002.

[9] "Bimodal biometric verification mechanism using fingerprint and face images", manjunathswamyb e ; d2015 ieee 10th international conference on industrial and information systems (iciis)

[10] "Biometrics and Face Recognition Techniques", Renu Bhatia, 2013, IJARCSSE

[11] "Multimodal Biometric System",TarunaPanchal Dr. Ajit Singh,2013, IJARCSSE.

[12] A. Jain, R. Bolle, and S. Pankanti, editors, *Biometrics: Personal Identification in Networked Society*, KluwerAcademic Publishers, 1999

[13] S. Prabhakar and A.K. Jain, "Decision-level fusion in fingerprint verification", *Pattern Recognition*, Vol. 35, No. 4, pp. 861-874, 2002.

[14] H. Korves, L. Nadel, B. Ulery, and D. Masi, "Multibiometric Fusion: From Research to Operations", *Sigma*, Mitretek Systems, Summer 2005.

[15] A. Mhatre, S. Palla, S. Chikkerur, and V. Govindaraju, "Efficient search and retrieval in biometric databases," Biometric Technol.Human Identification II, vol. 5779, no. 1, pp. 265–273, 2005

[16] "Multimodel Biometric Person Authentication System using Speech and Signature Features", P. Kartik ; S. R. MahadevaPrasanna ; R. V. S. S. Vara Prasad, TENCON 2008 - 2008 IEEE Region 10 Conference