IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Model of Hybrid Biometric System

Vinayak Khavanekar[1], Aishwarya Shinde[2], Shambu Rai[3]
Student[1,2] and Mentor[3]
Bharati Vidyapeeth' Institute of Management and Information Technology, University of Mumbai, India

Abstract: *Biometrics refers to the automatic recognition of people based on their physical and / or behavioral characteristics. Biometric technology is used to provide maximum security through personal and physical features. This technology serves as a gateway to a system that needs to be identified before it can be accessed or used. Using biometrics for personal verification is very accurate and is safer than current methods (such as passwords or Personal Identification Numbers - PINs) and very simple (none to carry or to remember). So, Biometrics not only provides security, but also is about flexibility. The need for biometrics can be found in a wide range a list of commercial and military applications where a high level of security is required. Many of the biometric systems used in real-world systems have not changed, such as using a single source of information authentication (e.g., single fingerprint, face, voice etc.). Some of the limitations imposed by unimodal biometric systems can be overcome which includes many sources of identity- building information. If we use a combination of these biometrics it will provide an additional level security. It overcomes the limitations of the previous methods and provides an additional level of security. It also lowers FAR (False Acceptance Level), FRR (False Rejection Level).*

Keywords: Introduction, Biometric system, Biometric system errors, Limitations of biometric system, Multimodal biometric system

I. INTRODUCTION

Biometrics refers to metrics related to human characteristics and features. It uses the human body and behavior security features of any system. Biometric detection (or biometric validation) is used in computer science as type of identification and access control. Biometric identifiers they are often classified as anti- behavioral features. Biometric technology automated methods to verify or identify the identity of the living person on physical or moral aspects. In biometric identification system, input-related identity data (investigation / investigation) are usually determined by comparison it versus Physiological features related to the condition of the body. For Examples Fingerprints, palm stamps, face recognition, DNA, hand geometry, iris recognition, retina and smell / smell. Behavioral factors are related to pattern by human behavior, which includes but is not limited to typing rhythm, movement, and voice.

1.1 Fingerprint Recognitions

Unique human fingerprints. They have a lot of details, it's hard transform them, and last a long time in the life of the person who makes them suitable as long-term signs of personality. Fingerprints, as shown in Fig. (a) are different and do not change over time as well therefore used for a long time. Fingerprint is a pattern of hills and valleys in place of the finger. Contains Situations such as crossover, core island, delta, pore etc. I Finger recognition is important in forensic science for finding a crime scene. The ridges are above the skin the finger sections and grooves are the lower parts. I different types of non-continuation in the ridge (minutiae) be sufficient discriminatory information to detect fingerprints. Ridge bifurcation (where the ridge separates) and the end of the ridge (where the limit ends) important points minutiae. Minutiae-based fingerprint recognition often stands out fingerprints on these two ridge elements are called minutiae. Variations of fingerprints can be determined with a pattern of ridges and ditches and minutiae points. Availability of multiple human fingerprints fingerprint recognition is ready for use on a large scale identification involving millions of identities. However, problem with large fingerprint recognition system the need for a large amount of accounting resources, especially in the detection mode.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Fig. (a) Fingerprint Recognition

1.2 Face Recognition

Face detection as shown in Fig (b) is a computer program automatically identify or verify a person from digital image or video frame from a video source. One of the ways to do this is to compare selected facial features from photo and face website. Dimensions, dimensions and the physical features of the human face are different. The fig tree. (b) Indicates that the app detects a person's face using a sensor and edit the grid on it to get face features. That grids are organized stored in a database with a unique identifier for reuse. Next the time when a person needs access to a system, a request the first people deal with it using a sensor, rearrange the grid and then compare those grids with face templates stored in database. When a match is found, the person gets access to system. One popular method of facial recognition is based on it location, size and dimensions of facial features such as eyes, eyebrows, nose, lips, chin and their location relationships. Another widely used method is based on a complete analysis of the face image representing the face as a combination of a conical number of centrical faces. Face recognition involves two main functions: i) facial area and ii) face recognition. The surface area determines the location of face in image input. By seeing the existing face, i Eigen face approach is one of the most popular methods. I Eigen's facial recognition method has two stages: i) training phase and ii) working phase. In the training phase, a set of facial training is available. Found face images are displayed in a low-resolution substrate using Principle Component Analysis (PCA). A collection of pictures that better describe the distribution of training images at a lower level dimensional surface space (Eigen space) is calculated. Then training facial images are arranged in this space by Eigen to produce a representation of training images in Eigen space. In the application phase, the image of the input face included in the same Eigen training samples filed on. Then, the recognition can be made by a section operating in the Eigen area.

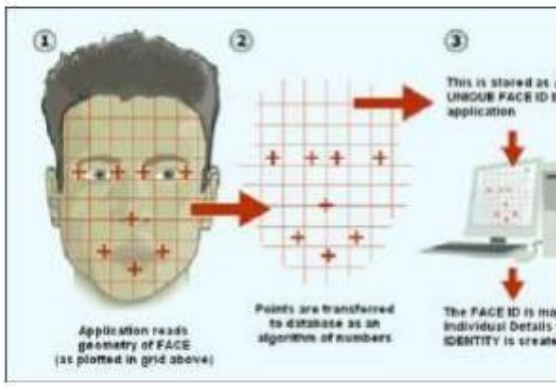

Fig (b) Face Recognition

1.3 Iris Scan

The iris shown in Fig (c). The iris is a year round the eye is bound by the pupil and the sclera (white of the eye) on both sides. The visible texture of the iris is formed during the fetus development and sustainability within the first two years

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

of life. The intricate iris texture holds very different information is useful for personal recognition. The individual Iris is different. The accuracy and speed of the iris scan system is it's good. Each iris is different and, like fingerprints, even irises of identical twin twins. It is very difficult to do surgically to disrupt the texture of the iris. Moreover, rather it is easy to see artificial irises (e.g., designer contact lenses). However, iris-based monitoring systems are required great user engagement and costly, new systems that are easier to use and less expensive.

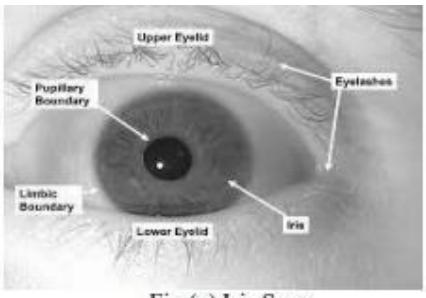

Fig (c) Iris Scan

1.4 Hand Geometry

Hand geometry is a biometric that identifies users by status of their hands. Hand geometry recognition systems, as shown in Fig. (d) are based on various similar measurements hand shape, palm size, length and width of fingers, space between fingers and hand stiffness. Hand features are not very divisive. They deserve it confirmation but not identification. In some such cases such as arrival and border control, biometrics are similar Fingerprints may be inappropriate because they violate the law privacy. Hand geometry is less secure due to its size and shape hand may change over time. In such cases the hand geometry can be used for validation as hand geometry is not available very different. Hand geometric features may not change during adolescence. Such a size awareness systems are large and therefore difficult to embed systems on other devices such as laptops. The hand of trade Verification systems based on geometry are included hundreds of places around the world. The process is very important simple, easy to use, and inexpensive. Environment factors such as dry weather or individual anomalies such as dry skin does not appear to have any adverse effects on the accuracy of verification of hand-based geometry systems

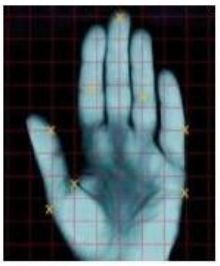

Fig. (d) Hand Geometry

II. BIOMETRIC SYSTEM

Biometrics plays a significant role in it everywhere in the world by man made of robots to distinguish the frameworks of evidence submitted to improve security. Fig (e) reflects the biometric framework. Qualifications for people can change from one person to another Next. Many interesting human qualities they are used for visual evidence. This is interesting The structure is used by Biometric innovation to divide everyone unequivocally. Biometric the framework is basically an example of consent a framework that recognizes the client by deciding on legitimacy a particular physical or behavioral mark client management. A few serious problems should be considered in presenting a useful biometric framework. First a the client must be selected by frame for his biometric the structure can be captured. The building is securely located in the focus area database or smart card provided to the client. The format says recovered when one had to be separated. Depending on the connection, the biometric framework may be correct work with a check (confirmation) or physical proof mode.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

A biometric system is a pattern recognition system scan biometric feature, remove features and so on templates stored on a website. This program works either internally verification mode or identification mode. In verification mode, personal identity such as ID, PIN or username in comparison captive captions. In diagnostic mode, all entries Web-based templates compared to scanned features.

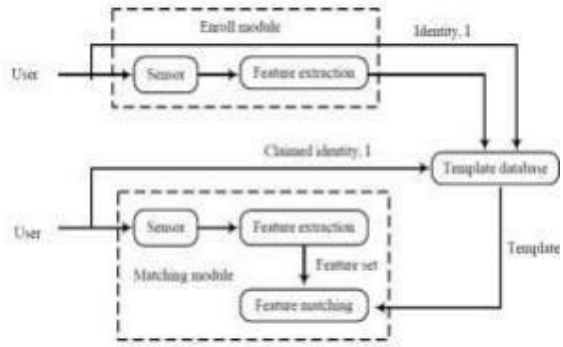

Fig (e) Block Diagram of Biometric System

III. BIOMETRIC SYSTEM ERRORS

The biometric authentication system makes two types of errors:

1. Occasional error biometric security systems False Acceptance. In the case of false acceptance, i an unauthorized person is identified as an authorized person.
2. The second mistake is made from time to time by biometric security False Rejection programs. In the case of false condemnation, the system fails to detect the authorized person and refuses that person as a deceiver.

IV. LIMITATIONS OF (UNIMODEL) BIOMETRIC SYSTEMS

Successful installation of biometric systems in Different social applications do not mean that biometrics is a problem completely solved. Biometric systems operate using any biometric element has the following limitations

1. Noisy data. Hearing data may be noise or distorted. Fingerprints with a scar or cold- changed voice examples of noisy data. Noisy data can also be the result of defective or poorly maintained sensors (e.g., accumulation contamination of the fingerprint sensor) or incorrect ambient conditions (e.g., blurring of the user's face recognition system). Noisy biometric data may be incorrect matched to templates that lead to a user-led website unjustified rejection.
2. Internal classroom changes. Biometric data obtained from each person at the time of proving authenticity may be very different data used to create a template in the middle registration, thus disrupting the matching process. These discrepancies are often caused by an error user sensory interaction or where sensory features are present fixed (e.g., by sensor-sensor switching interaction problem) during the verification phase.
3. Non-university. While every user is expected to have biometric element obtained, in fact possibly a small set of users that they do not have a particular biometric. A the fingerprint biometric system, for example, may not be able to remove features from personal fingerprints, due to the low level of ridge. So, there is a failure registration rate (FTE) related to the use of a single biometric feature.
4. Spoof Attack Problem. This type of attack in particular are important when behavioral features such as signature and voice are present used. However, physical features are also easily compromised by spoof to attack. For example, it has been shown to be true it is possible (although difficult and requires the help of a official user) to create artificial fingerprints / fingerprints on enough time to avoid fingerprints verification system.

V. MULTIMODAL BIOMETRIC SYSTEMS

Percentage of unimodal enforced barriers biometric structures can be overcome through multiple applications biometric methods, (e.g., unique face and finger human vision or various fingers of a man). Such frameworks, known as multimodal biometric frameworks or Hybrid Biometric System, is required to be very reliable because of the proximity of various,

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

liberal evidence. These the systems are moreover ready to face a solid execution requirements set by different applications. Multimodal biometric systems deal with the problem of omissions, as many attributes ensure a sufficient human population. In addition, multimodal biometric frames provide resistance satisfactory steps by making it difficult for the gatecrasher at the same time parody many biometric attributes of loyal client for beauty. By asking the user to submit an unusual subset of biometric features (e.g., right- hand indicator and fingers in the middle right, in a certain order), outline confirms that the "live" client is undoubtedly present at the purpose of obtaining information. Figure (f) shows multimodal biometric simulation model was may use two fingerprints or a combination of different symbols and iris filter and more.

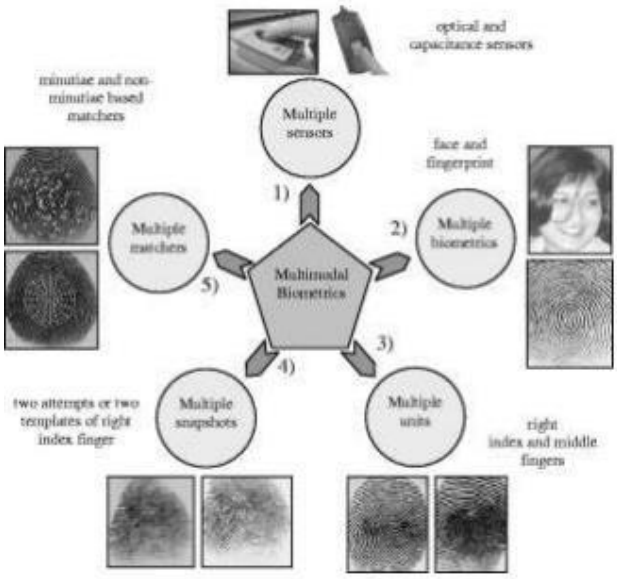

Fig. (f) Hybrid Biometric System

Multi-biometric systems can remove some of the barriers uni-biometric systems by combining multiple sources of information. Many biometric systems take input one or more sensors of two or more different scales biometric signal processes. For example, a program combining facial features with biometric iris recognition will be considered multimodal ‖ whether facial and iris photos were taken by different or similar image devices. Although the multimodal biometrics system helps us 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

The proposed system uses face recognition and fingerprints biometric system recognition. This program will use two senses. One for removing facial features and the other for to extract the features of fingerprints and match already Saved templates created. In all combinations of points the fusion is applied to it as well as the sum of the points it is decided that the person is a real person or no. In detail we can say that the sensor takes a biometric image and compare it with saved templates. The result is game points, used to make decisions. It determines who the person is you are a certified person or not. Fig. (h) Indicates improvements in hybrid biometric system. The graph shows that the level of acceptance of truth

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

in biometric hybrids the system is more than just fingerprint recognition and facial recognition recognition for integration. It was a level of false rejection of the biometric system is subject to the detection of fingerprints but somehow more than face recognition. Face recognition the system is slightly more accurate than the Hybrid biometric system as well recognition of fingerprints. Hybrid biometric system is above is safer and more accurate than the unimodel biometric system.

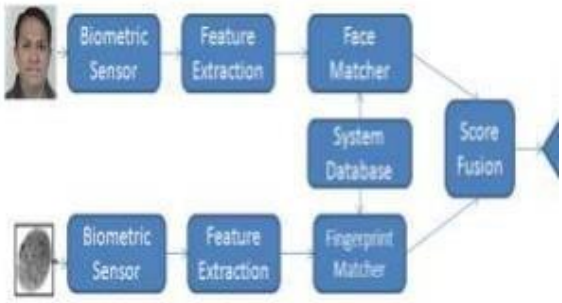

Fig.(g) Block Diagram of Proposed Hybrid Biometric

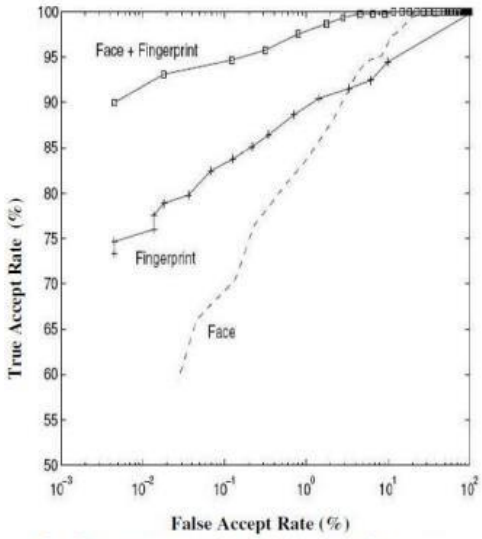

Fig. (h) Improvement with Hybrid Biometric System

VII. CONCLUSION

A unimodel or single biometric system has many limitations and low security because it uses only one biometric feature. The level of false acceptance and the level of false rejection is higher in the unimodel biometric system. Overcoming this problem a multimodel biometric system is helpful. Multimodal The biometric system uses many biometric features of a person for recognition provides a high level of security. Due to many biometric features this program becomes slow and complex.

REFERENCES

[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 crypto systems Benjamin Tams ;Biometrics (IJCB), 2014 IEEE International Joint Conference on [::Biometrics::]

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

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, Kluwer Academic 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.