Biometrics Authentication Technologies: A further Echelon of Security

Ankhi Debnath
Department of Electronics and Communication Engineering
Techno India University, EM-4, Salt Lake City, Sector V, Kolkata, West Bengal-700091

***Abstract*: The use of biometric data for authentication and recognition is now a reality. On the other hand, there is still a very strong need for new technologies to overpass intrinsic limitations of already "established" techniques. This not only requires to implement new algorithms but to determine the real potential and limitations of existing techniques. Nowadays, in many real time applications like forensic, security and other identification purposes biometrics is widely used. With the availability of inexpensive biometric sensors, it is becoming increasingly clear that, the broader usage of biometric technologies are being stymied by our lack of understanding of three problems concerning (i) recognition of biometric patterns (ii) sensing the measurements (iii) pattern recognition for the expressed purpose. For these reasons, we see biometrics as a grand challenge - "the basic problem in science and engineering with huge economic and scientific impact".**

Keywords: Biometrics, Human Fingerprints, False Acceptance Rate, Noise in Sense Data, ID card.

1. Introduction

At the most basic, biometrics can be best explained by breaking down the word: bio, from Greek word *'bios'*, as in biological; and metric, from '*metrikos'*, as in measurement. That is to say, biometric is biological measurement. Biometrics are an emerging field of technology using unique and measurable physical, biological, or behavioural characteristics that can be used to identify a person. It is a multidisciplinary subject which assimilate engineering, statistics, mathematics, computing, policy and psychology. Using biometrics, it is possible to establish an individual's identity which is based on "who she is," rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). In this paper, we give a brief critique of the field of biometrics and summarize some of its advantages, disadvantages, strengths, limitations, and related privacy concerns.

2. Measurement Requirements

Universality	Each person should have the characteristic.
Distinctiveness	Any two persons should be sufficiently different in terms of the characteristic.
Permanence	The characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.
Collectability	The characteristic can be measured quantitatively.
Performance	Refers to an achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed.
Acceptability	This indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.
Circumvention	This reflects how easily the system can be fooled using fraudulent methods.

Table 1: Measurement Requirements of Biometric System

3. Working of the System

1. *Enrolment* - The process whereby a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system [1].

2. *Submission* - The process whereby a user provides behavioural or physiological data in the form of biometric samples to a biometric system.

3. *Acquisition device* - The hardware used to acquire biometric samples.

4. *Biometric sample* - The identifiable, unprocessed image or recording of a physiological or behavioural characteristic, acquired during submission, used to generate biometric templates.

5. *Feature extraction* -The feature extraction process may include various degrees of image or sample processing in order to locate a sufficient amount of accurate data [2].

6. *Template*- A template is created after a biometric algorithm locates features in a biometric sample.

7. *Biometric Decision-making*- is frequently misunderstood. For the vast majority of technologies and systems, there is no such thing as a 100% match, though systems can provide a very high degree of certainty [2].

8. *Matching* -A match attempt results in a score that, in most systems, is compared against a threshold. If the score exceeds the threshold, the result is a match; if the score falls below the threshold, the result is a non-match [2].

9. *Score* – A number indicating the degree of similarity or correlation of a biometric match.

10. *Threshold* - A predefined number, often controlled by a biometric system administrator, which establishes the degree of correlation necessary for a comparison to be deemed a match.

11. *Decision* – The result of the comparison between the score and the threshold.

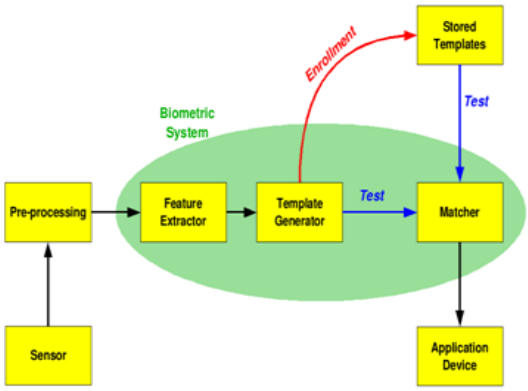


Fig.1. Block diagram of biometric system

3.1 Identification vs. Verification

Verification

The system validates a person's identity by contrasting the captured biometric data with her/his own biometric template(s) which is stored in the system database. In such system, an individual, desires to be identified claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts an one to one comparison to evaluate whether the claim is true or false (e.g."Does this biometric data belong to Mr. Y?"). Identify verification is basically used for positive recognition, where the aim is to avert multiple people from using the same identity [1].

Identification

The system identifies an individual by searching the templates of the users in the database for a match. Therefore the system conducts a one to many comparisons to confirm an individual identity (or fails if the subject is not enrolled in the database [1].

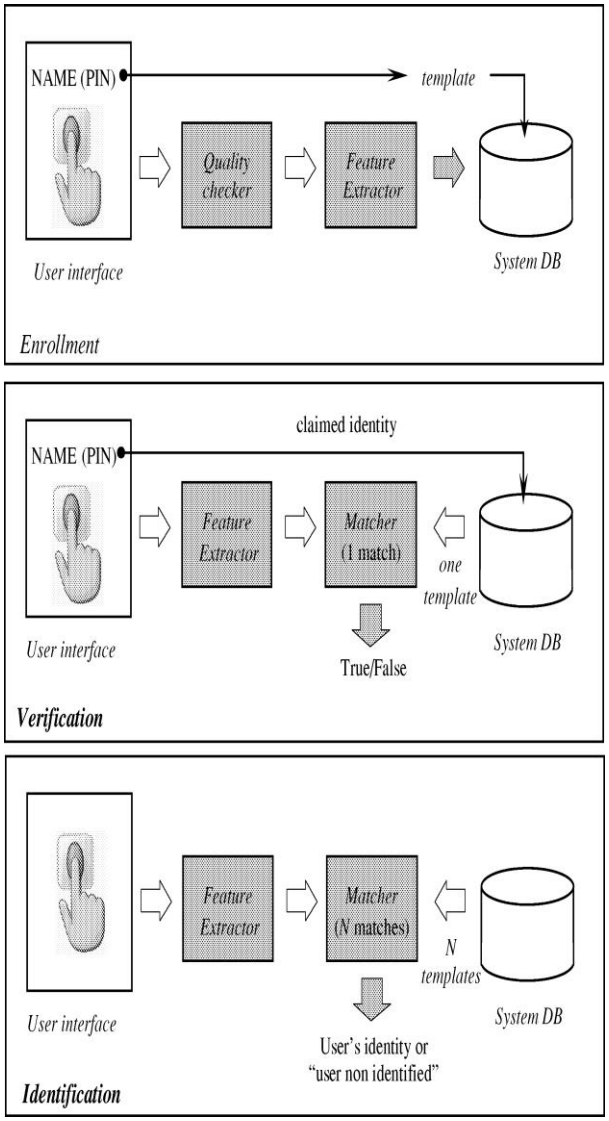


Fig.2. Block diagrams of Enrolment, Verification, and Identification using the 4 main modules of a Biometric system

3.2 Biometric System Performance and Errors

Due to various positioning on the acquiring sensor, inexact imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is not possible that two samples of the same biometric characteristics, captured in different sessions, exactly coincide.

The following are the most used performance metrics of biometric systems:

Table 2: Error Rates of Biometric System: FRR, FAR and EER

False Rejection Rate (FRR)	The probability that the system fails to detect a match between the input data and a matching template in the database. It measures the percentage of valid input patterns which are incorrectly rejected. It is sometimes referred to as **False Non-Match Rate (FNMR)**.
False Acceptance Rate (FAR)	The probability that the system incorrectly matches the inputs to a non-matching template in the database. It measures the percentage of invalid input patterns which are incorrectly accepted. It is sometimes also called **False Match Rate (FMR)**.
Equal Error Rate (EER)	The rate at which both acceptance and rejection errors are equal. The value signifies that the proportion of false acceptance is equal to the proportion of false rejection. The lower the EER value, the higher the accuracy of the biometric system.

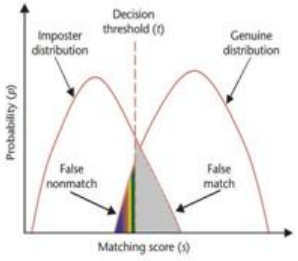


Fig.3. Biometric System Error Rates

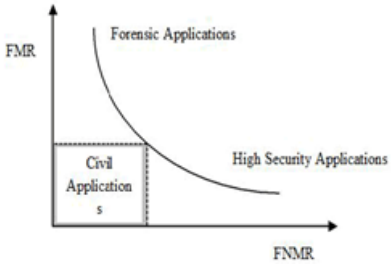


Fig.4. Receiver Operating Characteristic (ROC)

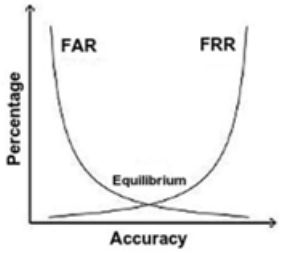


Fig.5. Equal Error Rate (EER)

3.3 Scopes and Probable Challenges

(i) Positive Identification ("Is the person truly known to the system?"): Biometrics can verify with high certainty the credibility of a claimed enrolment based on the input biometric sample.
(ii) Large Scale Identification ("Is the person in the database?"): Given an input biometric pattern, the large-scale identification evaluates if the pattern is associated with any of a large number (e.g., billions) of enrolled identities [4].
(iii) Screening ("Is he/she a wanted person?"): Screening applications covertly and discreetly determine whether a person belongs to a watch-list of identities.

4. Biometric Modalities

4.1 Physical Modalities

(A) FACE Recognition

It is probably most common biometric feature used by humans to make personal recognition. The face identification technology can be either static, controlled verification or can be dynamic that is uncontrolled face identification method. The most popular approaches to face identifications are either based on: (i) location and shape of eyes, lips, nose, eyebrows and chin or (ii) the global scrutiny of the face image that represents a face that is a combination of number of canonical faces .

Table 3: Characteristics associated with different applications

SERVICE	***STORAGE***	**DEVICE SIZE**	***DEVICE***	***ACCURACY***
1:N Large Scale Identification	Local / central Database	Millions of People	PC or smart card	Low FAR
1:1 Positive Identification/ Verification	Smart card/local database	No database Needed	PC or hard disks	Low FRR
Screening	Local / central Databases	Few hundred of people	PC or hard disks	Low FAR

(B) FINGERPRINT Recognition

Fingerprint identification technology has been undertaken by taking an image of an individual's fingertips and record the features including whorls, arches, and loops of the fingertip. It also captures the patterns of furrows, ridges, and minutiae for accurate analysis. The process can be done in the following ways:

- Minutiae based
- Correlation based
- Ridge feature based

The fingerprint is a very safe, secured, reliable and stable biometric solution. Law enforcement agencies have been using this technology for decades to recognize criminals. Currently, this technology is becoming famous in household security, banking, workforce management etc [4].

(C) IRIS Recognition

Many recognize Iris identification as the best biometric technology for. It analyzes the iris features including rings, freckles, furrows that is placed in the coloured tissue around the pupil. The iris scanner contains a video camera and works through glasses and contact lenses [12].

Generally, iris recognition is done by two methods:

- Daugman System and
- Wildes System

Iris recognition is deployed by many countries in crucial places like banking, private companies, institutes, border crossings, law enforcement agencies etc.

(D) RETINA Recognition

Retina recognition uses infrared technology to capture the unique patterns of an individual's retina blood vessels. As it is the internal organ of the eye and protected from external environments, retina recognition is recognized as a reliable biometric verification system [5].

(E) EAR Recognition

The ear recognition approach is generally based on matching the distance of salient points of the pinna from a landmark place of the ear. The characteristics of an ear are not expected to be very unique or distinctive in confirming the identity of an individual [5].

(F) Hand Geometry Recognition

Hand geometry recognition works with the shape of a person's hand features. The hand geometry reader measures an individual's hand in several dimensions. Then, it stores the data for further contrast, comparison and measurement. It is mostly famous for its comfort, easiness, and public acceptance. Nevertheless, this system is not very unique as like fingerprint or face recognition.

(G) PALM PRINT Recognition

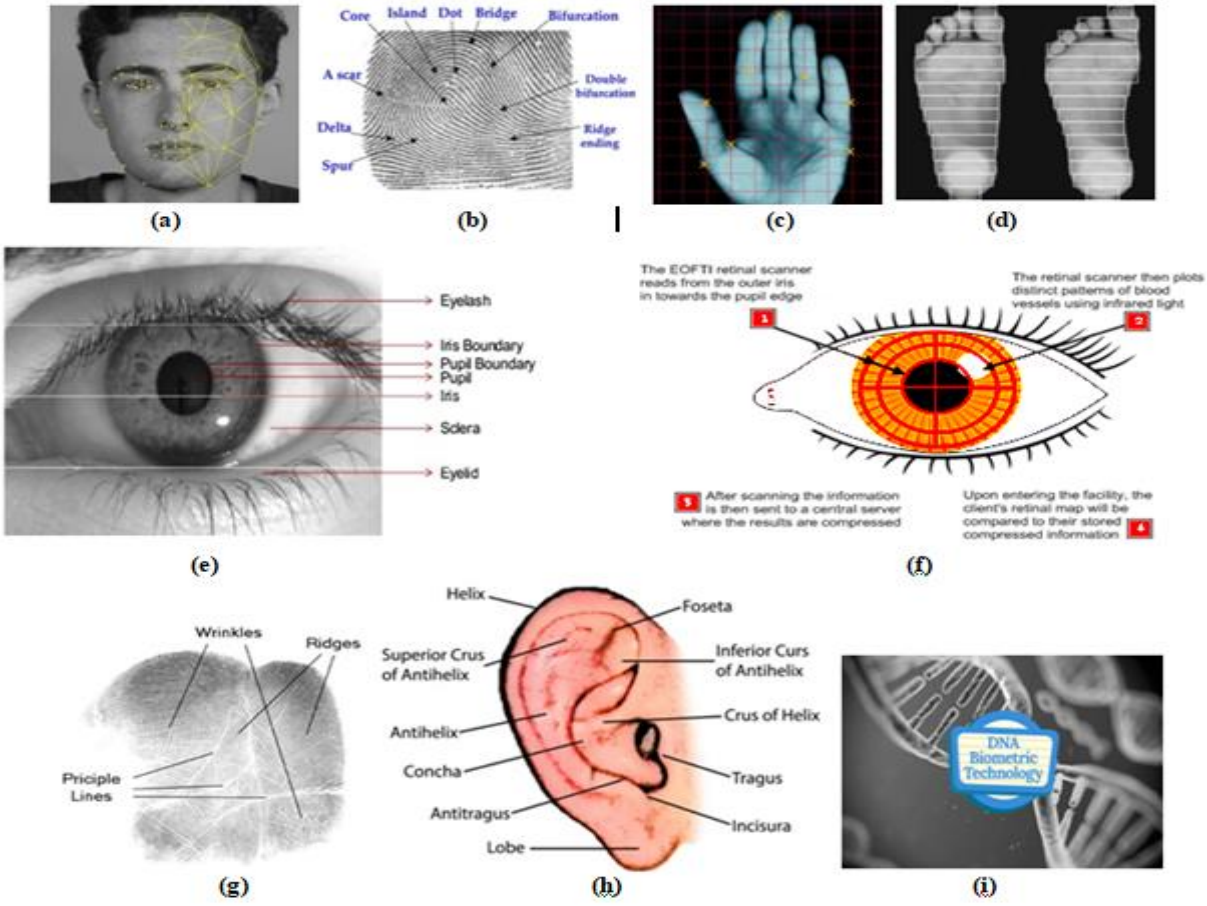
The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palm prints are expected to be even more idiosyncratic than the fingerprints. Since palm print scanners need to capture a large area, they are bulkier and more costly than the fingerprint scanners [10].

(H) DNA Recognition

DNA biometric is quite different from standard biometric modalities. It requires tangible physical template and couldn't be done in real time. It is a recognition technology with very high accuracy [4].

(I) Footprint and Foot Dynamics Recognition

As like finger vein, palm vein, fingerprint, iris and retina recognition, footprint can also be a distinctive physiological type of biometric identification. It is relatively new biometric verification system compared to other modalities. This system captures the footprint based biometric identification features of an individual.



4.2 Behavioural Modalities

(A) SIGNATURE Recognition

It is a process used to identify a person's hand written signature. It is a behavioural biometric and comes under dynamic verification technology. The technology uses the analysis of the shape, speed, stroke, and pen pressure and timing information at the time of the act of signing naturally.

(B) GAIT Recognition

It is a unique way of walking of a human and it's a spatio temporal biometric technique. It is not supposed to be very distinctive and hence used in low security application. It comes under behavioural biometric and gate based system uses video sequence footage of a person's walking to measure several different movements.

(C) VOICE/SPEECH Recognition

It works with speech patterns that capture by speech processing technology. This system analyzes the basic frequency, nasal tone, inflection, cadence etc. to identify a person's speech. It is also known as "automatic speech recognition" (ASR), "computer speech recognition", "speech to text" (STT) etc [11].

(D) TYPING/ KEYSTROKE Recognition

Typing or keystroke recognition is one of the behavioural types of biometrics. It analyzes the way a person press the keys to type something [5]. The keystroke dynamics uses the data set of the manner and the rhythm an individual types on a keyboard.

4.3 Other Modalities

(A) Odour Recognition

It is quite strange biometric method compare to fingerprint or face recognition system. It works with the body odour of an individual for verification and identification.

(B) Skin Reflection

Skin reflection biometric is quite uncommon biometric modality. In this system, several LEDs send light at different wavelengths into the human skin and photodiodes read the scattered light which is analyzed to perform the authentication.

(C) Lip motion Recognition

Lip motion technology analyzes a person's lip motions and designs a password according to the activity. Then it verifies the data pattern with previously stored data inputs with new lip motion data. Compare to other biometric modalities lip motion technology is quite a new evaluation.

(A) **(B)** **(C)** **(D)**

Fig.7. Different Behavioural Modalities: (A) Signature Recognition, (B) Gait, (C) Voice Recognition, (D) Keystroke Recognition

(D) Brain Wave Pattern Recognition

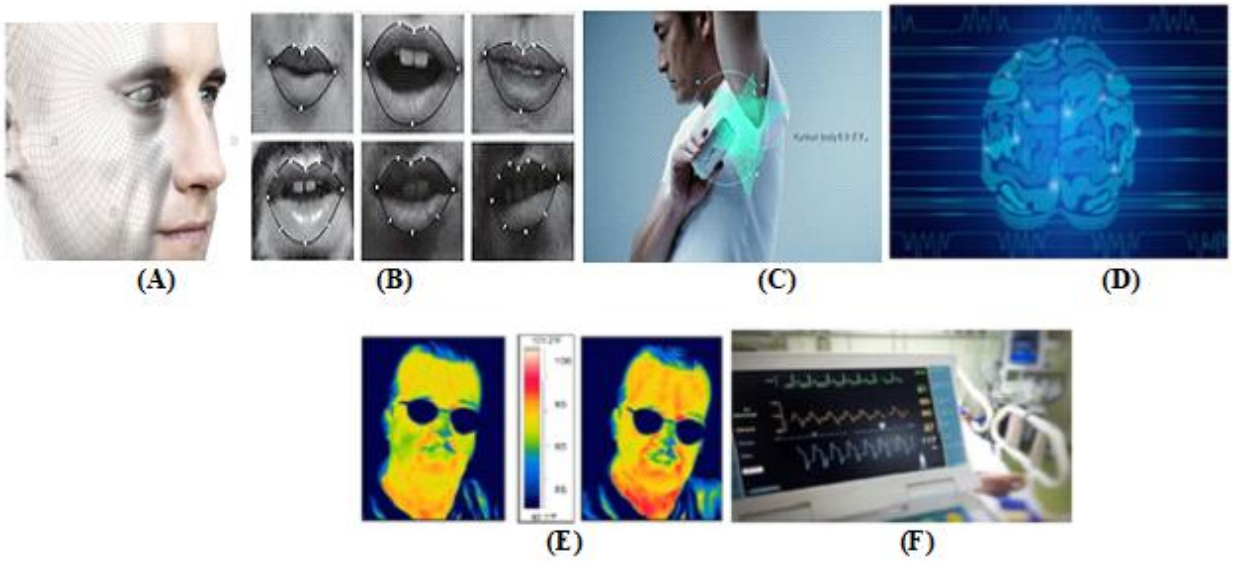
Brainwave recognition is a unique and surprising biometric modality [6]. It measures the signals given by the brain to design a unique individual characteristic set on the database. Some researchers believe that it is a hundred percent accurate biometric recognition process.

(E) Thermography Recognition

Facial thermography makes use of Infrared cameras to capture the flow of blood beneath the human skin. Then, the underlying pattern generates a robust biometric feature for positive identification. This technology may be used to test "liveness" of an individual.

(F) Heartbeat Measurement

This is one of the most critical biometric technologies so far. The growing evolvement of biometrics has already replaced the demand for passwords and PINs. Heartbeat biometric will replace the necessity of car keys, house keys, credit cards, and boarding passes too [6]. Heartbeat is a unique human characteristic, as like fingerprint, iris, palm veins, retina etc. It seems like this technology will allow us to sit in front of our laptop and unlock automatically, and when we go for a walk, it'll be locked again so that nobody can login to our pc. The same thing will happen with our car wheel, door handle etc.



(A) **(B)** **(C)** **(D)**

(E) **(F)**

Fig.8. (A) Skin Reflection, (B) Lip Motion, (C) Odour Recognition, (D) Brain Wave Patter Recognition, (E) Thermography, (F) Heart Beat Recognition

ADVANTAGES	*DRAWBACKS*
1.Security, Accuracy, Accountability 2.Convenient, Scalability 3.Flexibility 4.Save time	1.Physical rates are not changeable 2.Costly & Delay 3.Error Rate & Complexity 4.Unhygienic, Physical Disabilities 5.Scanning Difficulties 6.Environmental Usage matters

Human factors dictate the boom of a biometric-based recognition system to a large extent. The ease and comfort in interaction with a biometric system subsidize to its acceptance. For example, if a biometric system is capable to measure the features of an individual without contact, such as those using face, fingerprint, or iris, it may be perceived to be more user-friendly and hygienic. Additionally, biometric technologies needing a little cooperation or participation from the users (e.g., face and face thermograms) may be anticipated as being more convenient to users. On the other knowledge of the user, and this is anticipated as a threat to security by many individuals [9].

Privacy is the ability to lead our life free of intrusions, to stay autonomous, and to control access to our personal information. As because the incidence and magnitude of identity fraud increase, strong biometrics such as fingerprints will increasingly come into act for positively verifying people; the conventional technologies, knowledge or token based, for example-

5. Applications of Biometrics

Computer network login, Electronic data security, E-Commerce, Internet access, ATM, Credit card, Physical access control, Cellular phone, PDA, Medical records management, and Distance learning [3]. Such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children etc [4].

6. Social Acceptance and Privacy Issues

cannot deliver this functionality. However, biometrics raises three systematic privacy Concerns [9].

1. Unintended functional scope
2. Unintended application scope.
3. Convert Recognition.

7.2 Risks of stolen biometrics: Some reasons why Biometrics will have a Rocky Road

A hacker might use a specific target and represent the system with a copy of a known person's biometric template. Inter Gov reports that insiders execute about 80 percent of all cyber crimes (an estimate based only on reported security breaches). In such cases, the individual breaching the system's privacy very likely knows an authorized user personally, can capture a pattern biometric (for an example, a latent fingerprint), can make a duplicate (such as a 3D mold of the fingerprint) and represent it to the biometric system. In fact, a fictitious biometric attack on a biometric-based network access system represents a much more small risk than an attack on a password-based system. This is because a hacker might launch an attack against a password-based network access system remotely, without knowing any of the users. Also, the hacker might use the same password (for example, a dictionary word) to cast an attack against all the enrolled users at no extra cost [3].

Fig.10. Fake fingers made from consenting users. (a) Rubber stamp made from a live-scan fingerprint image. (b) Wafer-thin plastic sheet housing a three-dimensional replication of a fingerprint

1.Government Welfare	Recently, India has established a massive biometric database named Aadhaar for 1.3 billion people to enhance the government welfare programs.
2. Election	Many nations already adopted biometric technology for national elections [3].
3. Refugee Registration	Unfortunately, the global refugee crisis is increasing gravely and specially in the last few years. The countries which are providing shelters for the refugees are sensing the pressure of having a full biometric data pattern for those refugees.
4. Law Enforcement	With the advances in biometric technology to recognize a person impeccably, law enforcement agencies around the world continue to accept this technology as a means of strengthening their system.
5. National ID	Growing security concerns around the world constantly build a higher demand for biometric national verification program.
6. Border Security	Developed countries have deployed biometric technologies to tighten their border securities [4].
7. Military	While the law enforcement authority is increasingly viewing to turn popular biometric technologies like iris and face scanning to policing applications, the military market presents a whole different beast, with an craving for highly sophisticated technologies and a budget to back it up.
8. Aadhaar and Biometric ID	Administrated by the Unique Identification Authority of India, or UIDAI, Aadhaar is the world's most ambitious biometric national ID program. Over the last few years, Aadhaar has become pervasive in Indian society, with almost every citizen having enrolled their retina, iris, face, fingerprint and biographic data. Given the rapidity with which it has been evaluated – it's seen as a crucial constituent of a broader modernization program called "Digital India" – it has, at times, been a bit of a mess, with the UIDAI having frequently seen privacy and legal controversies, and periodically issuing press delivers to clarify how Aadhaar works for citizens and government officials alike [2].

Advantages and Drawbacks

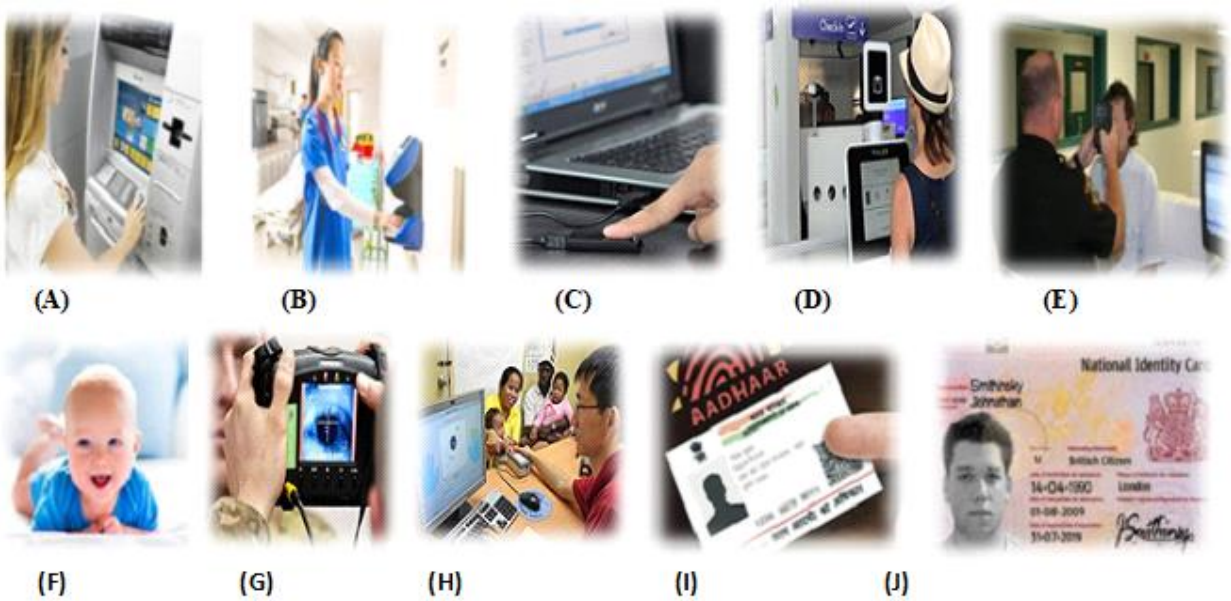


Fig.9. Applications of Biometrics: (A) ATM, (B) Hospitals, (c) PC Access, (D) Airports, (E) Prisons, (F)Child Care (G) Military, (H) Refugee Registration, (I) AADHAR & Biometric ID, (J) National ID

6.1 Limitations of Biometrics Using Any Single (UNIMODAL) Characteristics

Noise in sensed data	A fingerprint with a scare. Noisy data pattern can also result from accumulation of dirt on a sensor or from ambient conditions [6].
Intra class variations	Biometric data captured from an individual during authentication may be different from the pattern that was used to generate the template during enrolment [6].
Distinctiveness	While a biometric trait is expected to differ significantly across individuals, there may be large interclass similarities in the characteristic sets used to represent these traits [6].
Non universality	While every user is expected to possess the biometric trait being captured, in reality it is possible that a group of users do not possess the particular biometric trait[6].
Spoof attacks	An individual can try to forge the biometric trait. This is particularly easy when signature and voice are used as an identifier [6].

6.2 Risks of stolen biometrics: Some reasons why Biometrics will have a Rocky Road

A hacker might use a specific target and represent the system with a copy of a known person's biometric template. Inter Gov reports that insiders execute about 80 percent of all cyber crimes (an estimate based only on reported security breaches). In such cases, the individual breaching the system's privacy very likely knows an authorized user personally, can capture a pattern biometric (for an example, a latent fingerprint), can make a duplicate (such as a 3D mold of the fingerprint) and represent it to the biometric system. In fact, a fictitious biometric attack on a biometric-based network access system represents a much more small risk than an attack on a password-based system. This is because a hacker might launch an attack against a password-based network access system remotely, without knowing any of the users. Also, the hacker might use the same password (for example, a dictionary word) to cast an attack against all the enrolled users at no extra cost [3].

6.3 Vitality Detection and Multimodal Biometrics for Increased Security

Limitations of Unimodal biometrics can be overcome by using *Multimodal Biometric Systems* [7]. A multimodal biometric system uses multiple applications to acquire various types of biometrics. This allows the integration of two or more types of biometric identification and verification systems in order to meet stringent performance requirements. Such systems are expected to be more trustworthy due to the presence of multiple, independent sets of evidence [8].

These systems are also capable to meet the draconian performance requirements imposed by different applications. Multimodal biometric systems can be constructed to operate in five integration scenarios:
1) Multiple sensors,
2) Multiple biometrics,
3) Multiple units of the same biometric,
4) Multiple snapshots of the same biometric,
5) Multiple representations and matching algorithms for the similar biometric [6].

7. Future Prospects

There are several possible investigations on the future work that can be initiated. Feature level fusion in multimodal biometric may be extended by lots of ideas in terms of feature extraction and combination.

Selected 'Just Around the Corner' Biometric Technologies

<u>These are some of the biometric technologies which we will be discussing in the next five years</u>:

(A) Digital Tattoo from Vivalnk

(B) Motorola's patented phone on your skin

(C)Google's "Password Pill"

(D)Nymi's Heart rhythm Biometric identification device

(E) The MUSE EEG headset which can be used to read brainwaves

(F) Biowake's Touch DNA Kit

CONCLUSION

Current electronic security system which depends primarily on personal recognition to ensure that a client is an authorized user of a system, have a common vulnerability: the verification can be cloned which can be nearly eliminated using biometrics. Biometrics can be used by several organizations to increase security layers and protect their database and patents. Biometrics although interdisciplinary, it is not the consequent choice of the masses due to its high cost and legal considerations like security issues. The merit of biometrics is proven by joint venture of the G8 countries to apply it to avert forgery of passports and other travel documents as part of their fight against terrorism. Without any doubt the age of biometrics is here and the technology will directly disturb everyone over the next few years.

ACKNOWLEDGEMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Dr. Asit Baran Bhattacharya, Professor, Department of Electronics and Communication, Techno India University for his exemplary guidance, monitoring and encouragement throughout the course of this paper.

REFERENCES

[1] Wayman, J. L., "Fundamentals of Biometric authentication technologies" Int. J. Image Graphics, vol 1, pp no. 1, pp 93-113, 2001.

[2] Hong, L, Jain, A. K., "Integrating faces and fingerprints for personal identification, "*IEEE Trans. Pattern Analysis Machine Intel"*, Vol. 20, pp. 1295-1307, December 1998.

[3] Jain, A. K., Ross, A., "Multibiometric Systems", *Appeared in Communication of the ACM, Special Issue on Multimodal Interfaces*, Vol. 47, No.1, pp. 34-40, January 2004.

[4] Bolle, Ruud M., Connell, Jonathan H., Pankanti, Sharath, Ratha, Nalini K., Senior, Andrew W., "*Guide To Biometrics", 2003.*

[5] Arthi, K., Nandhitha, N.M., EmaldaRoslyn, S., "A Study and Evaluation of Different Authentication Methods and Protocols," IJCSMR, Volume 2,Issue 1 January 2013.

[6] Jain, A. K., Ross, A., Prabhakar, S., "An Introduction to Biometric Recognition", *IEEE Trans. on Circuits and Systems for Video Technology*, Vol. 14, No. 1, pp 4-19, January 2004.

[7] Hong, L., Jain, A. K., Pankanti, S., "Can multibiometrics improve performance?," in *Proc. AutoID'99, Summit*, NJ, pp. 59-64, October 1999.

[8] Kuncheva, L. I., Whitaker, C. J., Shipp, C. A., Duin, R. P. W. "Is independence good for combining classifiers?," in *Proc. Int. Conf. Pattern Recognition (ICPR)*, Vol. 2, pp. 168-171, Barcelona, Spain, 2001.

[9] Prabhakar, S, Pankanti, S, Jain, A. K., "Biometric Recognition: Security and Privacy Concerns", *IEEE Security & Privacy*, pp. 33-42, March/April 2003.

[10] Zhang, D., and Shu, W., "Two novel characteristic in palmprint verification: Datum point invariance and line feature matching," Pattern Recognition., vol. 32, no. 4, pp. 691–702, 1999.

[11] Bhatia, Renu, "Biometrics and Face recognition Techniques", IJARCSSE, vol 3, pp no. 5, may 2013.

[12] Mali, Kalyani, Bhattacharya, Samayita, "Comparative Study of Different Biometric Features", International Journal of Advanced in Computer and Communication Engineering Vol.2, Issue 7, July 2013.

[13] Jain, A. K., Bolle, R., Pankanti , S. (eds), *Biometrics: Personal Identification in Networked Society*. Kluwer Academic, December 1998.