Biometric System and its trends for today's era for Uniquely Identifying, Authentication and authorization

[1]Sachin Singh , [2]Namit Gupta, Mohan Vishal Gupta
[1]Assistant Professor CCSIT, TMU Moradabad
[2]Assistant Professor CCSIT, TMU Moradabad
[1]singh.sachin1986@gmail.com [2]namit.k.gupta@gmail.com,

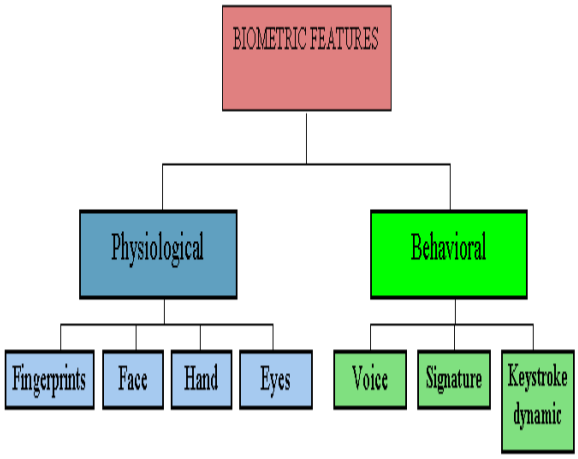
[3]Mohan.computers@tmu.ac.in

Abstract-A biometric system is a recent technological system that looks for metadata about a person (or other biological organism) to identify that person uniquely. Biometric systems rely on precise data about inimitable natal character in command to labour efficiently. A biometric scheme will engage consecutively data during algorithms for a meticulous outcome, regularly connected to a activist recognition of a consumer or other human being. The exact nature of today's biometric systems is linked with a precise use of the term "biometrics." In broad, biometrics is a few use of biological data in technology. Biometric systems focusing totally on the recognition of humans have become the major kind of biometric system in today's IT world.

Keywords- metadata, inimitable, meticulous.

Introduction

Biometric Systems are computerized methods of verifying or identifying the identity of a living being on the basis of some physiological or behaviroul characteristics, like a fingerprint or face pattern, or some aspects of behavior, like handwriting or keystroke patterns. Some of the most used biometric characteristics are shown in the picture below. A biometric system based on **physiological** characteristics is more reliable than one which adopts **behavioral** features, even if the latter may be easier to integrate within certain specific applications.

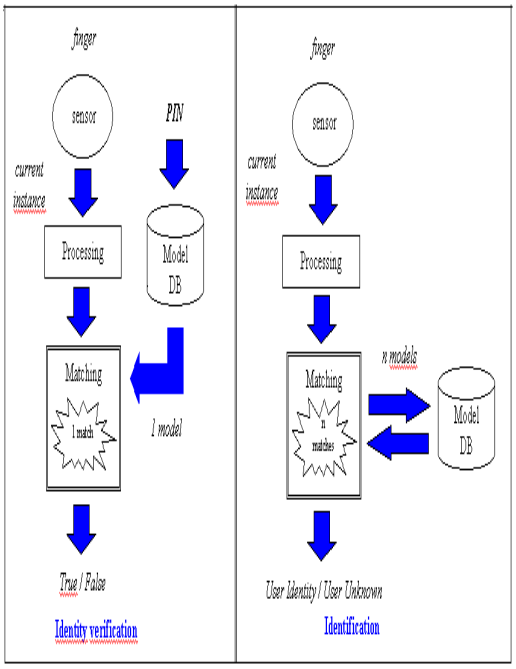


Using biometric characteristics is the only way to guarantee the presence of the owner when a transaction is made. In particular fingerprint-based systems have been proven to be effective in protecting information and resources in a large area of applications. At present, the amount of applications employing biometric systems to secure transactions is quite limited. On one side, some barriers are determined by the lack of familiarity (and in some cases, of acceptability) of the people, but, probably, the most important reasons of the underdevelopment of biometrics in the past were the cost of the required hardware/software and the insufficient performance. Nowadays technology leads to design low-cost systems whose performance makes them well-suited for a broad range of applications.

Generally, in the field of biometric systems, two different problems can be considered:

- **Identity verification** (or simply verification) requires the person to declare his/her identity, for instance by means of a PIN (personal identification number); the system directly matches (1:1) the person's current biometric characteristic with a previously acquired one which is retrieved through the PIN.

- **Identification** requires the system to scan a set of candidates, and decide whether one of them matches the person to be identified. Obviously, this is a more difficult task since it requires a (1:N) match which can be computationally very expensive on large database.



Before a biometric system can be used for verification/identification, all the users must be enrolled. **Enrollment** involves the individual giving a sample of his/her biometric characteristic which is used by the system to generate a compact model (or template) summarizing the discriminant features. Depending on the specific application, models can be stored into a centralized database, can be distributed over a network or can be stored in badges released to the users. Each time an individual requires a verification/identification, he/she provides a new sample of his/her fingerprint and the system matches this current instance with the stored model(s).

Biometric system performance

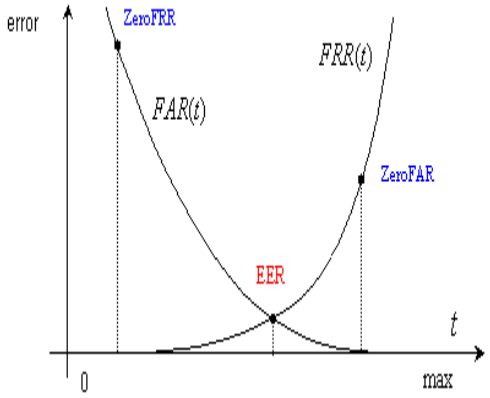
Due to different positioning on the acquiring sensor, to environmental changes, to deformations and noise, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide; for this reason the matching is performed by an algorithm which computes a similarity score and compares it with an acceptance threshold: in case the similarity is greater than the threshold the system claims that the two samples coincide. Differently from a password matching, sometimes the output of a biometric system may be incorrect: the main system errors are usually measured in terms of:

- **FRR** (**False Rejection Rate**) the frequency of rejections relative to people who should be correctly verified. When an authorized user is rejected he/she must represent his/her biometric characteristic to the system. Note that a false rejection does not mean necessarily an error of the system; for example, in the case of a fingerprint-based system, an incorrect positioning of the finger on the sensor or dirtiness can produce false rejections.

- **FAR** (**False Acceptance Rate**) the frequency of fraudulent accesses due to impostors claiming a false identity.

Generally, FAR and FRR depend on the **acceptance threshold *t***, which is used to set the desired security level, and are

strictly related to each other. More specifically, FRR(t) is an increasing function and FAR(t) is a decreasing function, so if the threshold setting is increased to make the access harder for impostors, some authorized people may find it harder to gain access.



False acceptance rate (FAR) and false rejection rate (FRR) as functions of the threshold t

Other performance indexes are commonly used to evaluate biometric systems:

- ***EER (Equal Error Rate):*** *denotes the system error when FRR=FAR*
- ***ZeroFAR:*** *denotes FRR when FAR=0*
- ***ZeroFRR:*** *denotes FAR when FRR=0*

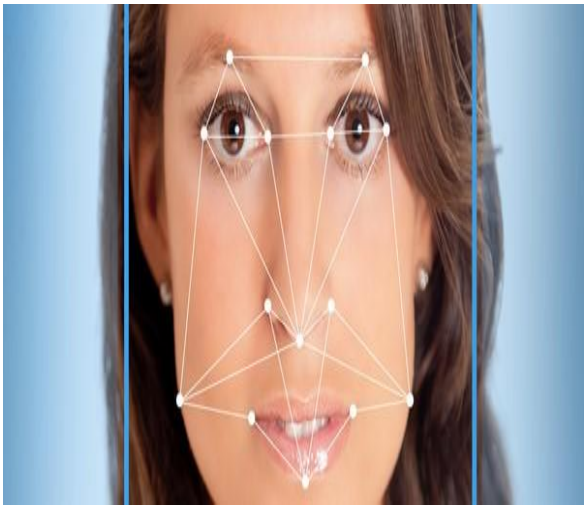
Various Biometric Means That are itroduced or will be introduced for upcoming era

1. Fingerprint recognition

An identification system based on fingerprint recognition looks for specific characteristics in the line pattern on the surface of the finger. The bifurcations, ridge endings and islands that make up this line pattern are stored in the form of an image.

The disadvantage of capturing an image of an external characteristic is that this image can be replicated – even if it is stored in encoded form. An image is still an image, after all, and can therefore be compared. In principle, you can then generate the same code. Fingerprints can already be spoofed***** using relatively accessible technology. Another, by no means insignificant, point to consider is that a finger presented for recognition does not necessarily still need to be attached to a body

2. Facial recognition



A facial recognition system analyses the shape and position of different parts of the face to determine a match. Surface features, such as the skin, are also sometimes taken into account.

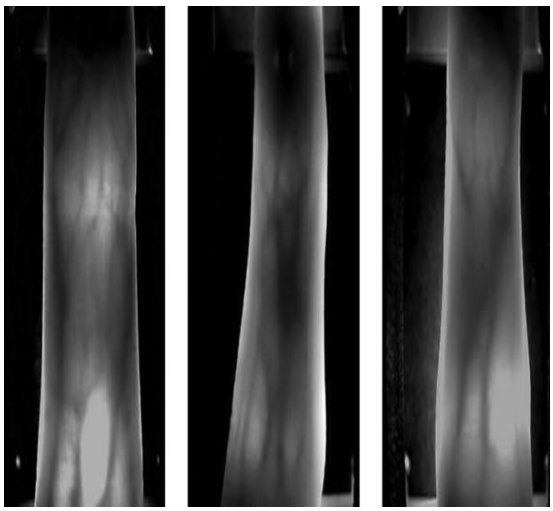
Facial recognition for security purposes is an offshoot of face detection technology, which is used to identify faces in complex images in which a number of faces may be present. This technology has developed rapidly in recent years and is therefore an excellent candidate if a system is needed for remote recognition. Another plus is that the technology allows 'negative identification', or the exclusion of faces, making it a good deal easier to scan a crowd for suspicious individuals.

3. Iris recognition

When an iris scan is performed a scanner reads out the unique characteristics of an iris, which are then converted into an encrypted (bar)code. Iris scanning is known to be an excellent security technique, especially if it is performed using infrared light.

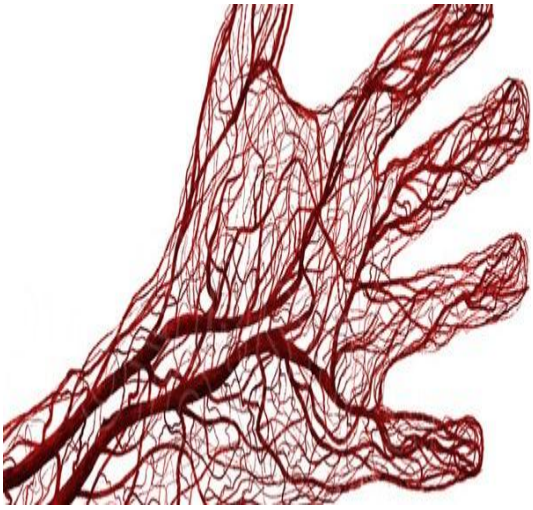
However, one problem frequently encountered when the technology is introduced is resistance from users. Quite a few people find having their eyes scanned a rather unpleasant experience. You also have to adopt a certain position so the scanner can read your iris, which can cause discomfort. Hygiene is another frequently cited drawback, as many systems require users to place their chin on a chin rest that has been used by countless people before them.

4. Finger vein pattern recognition



In the case of vein pattern recognition the ending points and bifurcations of the veins in the finger are captured in the form of an image, digitised and converted into an encrypted code. This method, combined with the fact that veins are found beneath rather than on the surface of the skin, makes this technology considerably more secure than fingerprint-based identification, as well as faster and more convenient for the user. It is a more expensive method, however.

5. Palm vein pattern recognition



This technique is also based on the recognition of unique vein patterns. However, as more reference points are used than in the case of finger vein pattern recognition, this is an even simpler and more secure identification method.

The technology, which cannot be copied (or only with extreme difficulty), is currently regarded as the best available method in the area of biometric security, alongside iris scanning. Palm scanning is fast and accurate and offers a high level of user convenience.

Access control systems based on palm vein pattern recognition are relatively expensive. For that reason such systems are mainly used within sectors that have exacting demands when it comes to security, such as government, the justice system and the banking sector.

Application Of Biometrics

- **Airport Security**

In many airports, the top biometric modality choice for immigration control is iris recognition. In order to use iris recognition, travelers are first enrolled by having a photo of their iris and face captured by a camera. Then, their unique details are stored in an international database for fast, accurate identification at ports of entry and exit that use iris recognition for traveler identity verification. When travelling, instead of waiting in long queues to be processed, passengers simply walk into a booth and look into an iris camera. The camera then photographs the iris and a software program then matches the details with the information stored on the database.

- **Time and Attendance**

A biometric time and attendance system is the automated method of recognizing an employee based on a physiological or behavioral characteristic. The most common biometric features used for employee identification are faces, fingerprints, finger veins, palm veins, irises, and voice patterns. When an employee attempts identification by their biological traits, a biometric hardware device compares the new scan to all available templates in order to find an exact match. Even government organizations now rely on **biometrics for ensuring timely attendance** of staff and accurate payroll calculations.

- **Law Enforcement**

Biometrics is also widely used for jail and prison management. Biometrics provides a modern solution by which the Jail Authority, Public Safety Departments, and Governments can safely and securely manage prisoner identities

- **.Access Control & Single Sign On (SSO)**

The primary reason behind more and more organizations and personnel across the globe adopting biometric technology for

access control and Single Sign On (SSO) is because traditional authentication tactics like **passwords are insufficient for personal identification**. Passwords only provide evidence or proof of knowledge whereas biometrics provides unique advantages because it relies on identifying someone by "who they are" compared to "what you know "or "what you have."
Today, biometrics is widely used around the world for **home access control**, **mobile phone access**, **vehicle access authentication** and **Single Sign On (SSO)**.

- **Banking – Transaction Authentication**

Biometrics in banking has increased a great deal in the last few years and is being implemented by banks throughout the world. As global financial entities become more digitally-based, banks are implementing biometric technology to improve customer and employee identity management in an effort to combat fraud, **increase transaction security**, and enhance customer convenience. Customers are also fed-up with identity theft and the inconveniences associated with constantly having to prove their identities. As a result, more and more **customers are looking for banks** that have biometric authentication in place prompting banks to more closely research the technology for implementation.

Conclusion-

The recent and future global attitude towards terrorism has influenced people and their governments to take action and be more proactive in security issues.. Presently, there are several biometric security systems that use different human biometric characteristics for recognition. Examples include fingerprint, signature, face, hand, voice, iris, etc. Out of these, fingerprint is more frequently used because of its high uniqueness and ease of capturing.

References-

[1] "A study on new biometric approaches" **Shally Gupta" ; Lakshmi Singh**

[2] "A Study of Biometric Approach Using Fingerprint Recognition" **Ravi Subban and Dattatreya P. Mankame**

[3] "Weakness Of Biometric authentication" **Boy, Jacobsen & Lidén**, Societal Ethics of Biometric Technologies

[4] "A Survey of Biometric Recognition Methods" **Kresimir Delac, Mislav Grgic** International Symposium Electronics in Marine, ELMAR

[5] "Emerging Biometric Developments: Identifying The Missing Pieces For Industry" **Dr. Edward S.** Dunstone International Conf. on Signal Processing and Its Applications August 2001

[6] "Biometric Identification",**Anil K. Jain, Lin Hong,** Sharath Pankanti Conference onCommunications of the ACM Volume 43 February 2000

[7] "Biometric Recognition: Securiy and Privacy Concerns" **Salil Prabhakar, Sharath Pankanti, Anil K. Jain** Conference on IEEE Security and Privacy April 2003

[8] "Practical Implementation of Biometrics based on Hand-Geometry" **Julian Ashbourm** Conference on IEEE Colloquium on Image Processing for Biometric Measurement April 1994