

A Review on Biometric Authentication Techniques



Subhash Basishtha¹, Saptarshi Boruah²

¹Department of Information Technology, Assam University Silchar, India, subhash.cse08@gmail.com

²Department of Information Technology, Assam University Silchar, India, baruah.ss@gmail.com

Abstract: Advancement in the Information Technology field also makes the security of the information an important part of it. Therefore, security becomes a major issue and the need for authentication even become more important. The prevailing methods of human identification such as identification of documents and PIN are not able to meet the growing needs of security; as a result biometrics comes into existence which is based on physiological and behavioral characteristics of a person. It is increasingly adopted by everyone and used in most of the person identification application. Unlike the prevailing technology, biometric traits (e.g., fingerprint, face etc) cannot be lost, stolen, or easily forged. This paper represents a review of the overview of Biometric, some of emerging Biometric authentication techniques and some performance metrics associated with Biometric technology.

Keywords : biometric, Authentication, fingerprint, IRIS, security.

INTRODUCTION

We the humans distinguish each other according to their various characteristics for ages. We recognize others by their face when we meet them and by their voice when we talk to them. In traditional digital system identity verification (authentication) is done by something that one has (key) or one knows (pin, password). However, things like keys or cards tend to get stolen or lost and passwords are often forgotten or disclosed. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

To overcome this problem and to achieve more reliable verification or identification we should use something that really characterizes the given person. Biometrics offer automated methods of identity verification or identification on the principle of measurable physiological or behavioral characteristics such as a fingerprint or a voice sample. [8]. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance.

Biometric Authentication is one of the most exciting technical improvements of recent history. It is the most emerging technology for people identification and authentication. It is strictly based on personal traits, which is much more difficult to be forgotten, lost, stolen, copied or forged than traditional data [1].

OVERVIEW

Biometrics means Identifying things by their biological traits. Simply it means the methods which are used to identify a person or verifying the identity of a person based on his physiological or behavioral characteristic is known as biometric. The most popular applications which most people associate with biometrics is security. Examples of physiological characteristics include fingerprint images, facial character, iris recognition etc. Behavioral characteristics are traits that are learned or acquired. Examples of Behavioral characteristics are Dynamic signature verification, speaker verification, and keystroke dynamics [2].

Generally, physical and behavioral characteristics used by biometrics include the following taxonomy: [3]

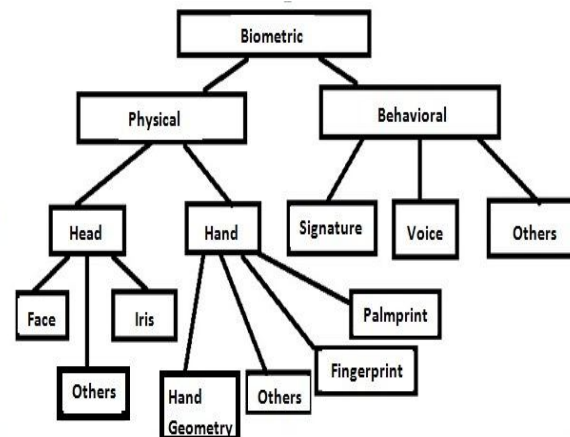


Fig: 1 Physical and behavioral characteristics used by biometrics [3]

Enrollment and authentication are the two stages of biometric authentication systems.

In the enrollment subsystem the biometric data are captured from a subject and checked for their quality. Then relevant information, typically indicated as biometric features, are extracted and eventually stored in a database [1].

Biometric authentication requires comparing a registered or enrolled biometric sample against a newly captured biometric sample (for example, a fingerprint captured during a login). During Enrollment, as shown in the picture below, a sample of the biometric trait is captured, processed by a computer, and stored for later comparison [2].

Advantages of Biometric Technology [11]:

- Biometric identifiers are difficult to be lost or forgotten, because it is always present in human body itself. It is also difficult to be copied/shared, and It require the person to be authenticated to be present at the time and point of authentication (a user cannot claim his/her password was stolen)
- Instead of passwords, biometric systems could be used to protect the strong cryptographic keys.
- In case of Biometric Identifier all users have relatively equal security level, One user's biometrics is no easier to break than another's. –There cannot be many users who have “easy to guess” biometrics like in case of password that can be used to mount an attack against them.

A. BASIC BLOCK OF BIOMETRICSYSTEM

The below Fig: 2 show the basic block diagram of biometrics.

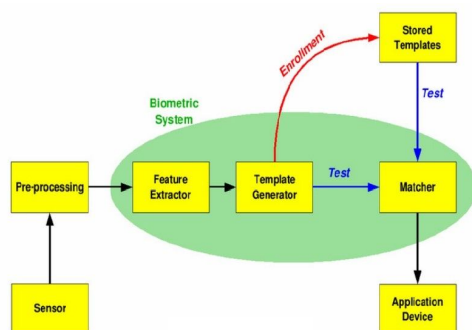


Fig: 2 Biometric block diagram

Description of the blocks:

- Sensor: The sensor is an interface between the real world and the system. It is used to acquire all the necessary data, depending on the characteristic in consideration.
- Pre-Processing: This block is needed to enhance the input (i.e., remove all the background noise and unnecessary artifacts during data collection) and also to use some kind of normalization, if needed.
- Feature Extractor: This block is responsible to extract the necessary features from the pre-processed input in the correct and in the optimal way.
- Template Generator: The template is typically a vector of numbers or an image with particular properties, and is generally a synthesis of the relevant characteristics extracted from the source.
- Enrollment: If an enrollment is performed, the template is typically stored in a central database.
- Matcher: If a matching is being performed, the obtained template is passed to a matcher that compares it with other relevant templates in the database and estimates the distance between them using any specific algorithm (e.g., the Hamming Distance metric).

Application Device: The matcher then returns the result of the evaluation to the application device, which will then decide how to handle the user being evaluated.

BIOMETRICS TECHNOLOGIES

Biometric Technologies for Biometric Authentication are based on a physiological or behavioral characteristic of an individual. Some of the emerging and popular Biometric technologies are listed as below:

1. *Fingerprint Technology*: Fingerprint-based recognition has been the longest serving, most successful and popular method for person identification [5]. It is the oldest of all the biometric techniques. A fingerprint is an impression of the friction ridges of all or any part of the finger. A friction ridge is a raised portion of the on the palmar(palm) or digits (fingers and toes) or plantar (sole) skin, consisting of one or more connected ridge units of friction ridge skin [6].

A block diagram of how a fingerprint identification system operates is given in the below Fig: 3. A single finger or multiple fingers are imaged using a live-scan fingerprint capture device. Generally that image is transmitted unencrypted to a local client workstation. After compression, the client software usually packages the biometric data with other demographic or identifying data (such as that contained on a driver's license or other credential), encrypts it, and sends it to a central server for further processing. Quite often, the central server is referred to as an AFIS or Automatic Fingerprint Identification System, which is responsible for matching one fingerprint to another.

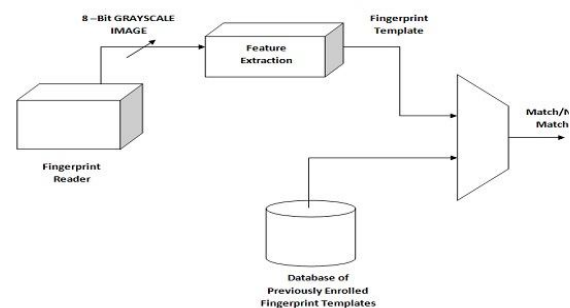


Fig: 3 Fingerprint [7]

The first step in AFIS processing consists of creating a biometric template through a process known as “feature extraction”. Specifically, the image of a biometric sample such as a fingerprint is not used in comparing one fingerprint to another. Rather, a significantly smaller “feature map” or template of the fingerprint, containing only the unique identifying minutiae points on the finger, is used. Matching one template to another is a secondary function of the AFIS and a process known simply as “matching”. The template created from processing the live biometric sample is referred to as the Inquiry template. The Reference template that the Inquiry template is matched against can be contained on the secured identification document, or reside internal to the AFIS as a result of a prior enrolment process [7].

Thus, at the most fundamental level, the processing involved in fingerprint identification consists of three steps: [7]

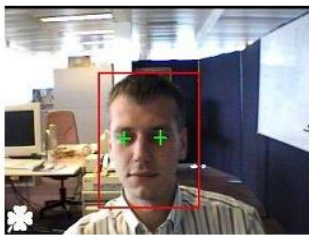
- a) Biometric Sample Acquisition
- b) Feature Extraction/Template Generation and
- c) Matching.

2. *Facial Recognition Technology*: Facial recognition is the most natural means of biometric identification. The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission.

Most of facial recognition systems require the user to stand a specific distance away from the camera and look straight at the camera. This ensures that the captured image of the face is within a specific size tolerance and keeps the features (e.g., the eyes) in as similar position each time as possible.

The first task of the processing software is to locate the face (or faces) within the image. Then the facial characteristics are extracted. Facial recognition technology has recently developed into two areas: facial metrics and eigen faces. [8]

Facial metric technology relies on the manufacture of the specific facial features (the system usually look for the positioning of eyes, nose and mouth and distances between these features), shown in below Fig: 4 [6].



After locating the face in the image the system locates eyes within the face region.

Fig: 4 Facial Recognition Technology

The face region is rescaled to a fixed pre-defined size (e.g. 150-100 points). This normalized face image (Fig: 5 shows a Normalized face) is called the canonical image. Then the facial metrics are computed and stored in a face template. [6]



Fig: 5 Normalized Face

The Eigen Face method (below Fig: 6) is based on categorizing faces according to the degree of it with a fixed set of 100 to 150 eigen faces. The eigen faces that are created will appear as light and dark areas that are arranged in a specific pattern. This pattern shows how different features of a face are singled out [6].



Fig: 6 Eigen Face

The image processing and facial similarity decision process is done by the computer software at the moment, this processing requires quite a lot of computing power and so it is not easy to assemble a stand-alone device for face recognition. There are some efforts (by companies like Siemens) to create a special-purpose chip with embedded face recognition instruction set.

3. *Iris Recognition Technique*:

This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are unique and obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Fig: 7 shows an image of Iris. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities [2].

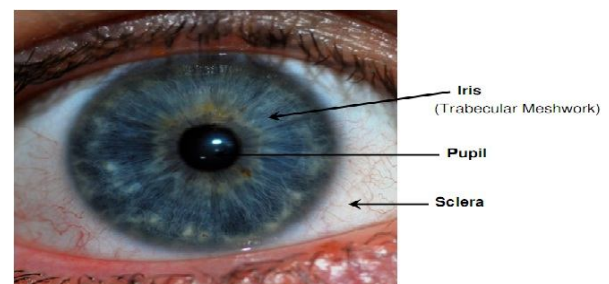


Fig: 7 Iris Technology [4]

The iris pattern is taken by a special gray scale camera in the distance of 10- 40 cm of camera. Once the gray scale image of the eye is obtained then the software tries to locate the iris within the image. If an iris is found then the software creates a net of curves covering the iris. Based on the darkness of the points along the lines the software creates the iris code.

Here, two influences have to take into account. First, the overall darkness of image is influenced by the lighting condition so the darkness threshold used to decide whether a given point is dark or bright cannot be static, it must be dynamically computed according to the overall picture

darkness. Secondly, the size of the iris changes as the size of the pupil changes. Before computing the iris code, a proper transformation must be done.

In decision process, the matching software takes two iris codes and compute the hamming distance based on the number of different bits. The hamming distances score (within the range 0 means the same iris codes), which is then compared with the security threshold to make the final decision. Computing the hamming distance of two iris codes is very fast (it is the fact only counting the number of bits in the exclusive OR of two iris codes). We can also implement the concept of template matching in this technique. In template matching, some statistical calculation is done between a stored iris template and a produced. Depending on the result decision is taken [6].

4. *Speaker Recognition Technology*: Voice is a natural choice to authenticate a user (for a mobile phone or even a computer). The generation of human voice involves a combination of behavioral and physiological features. The physiological component of voice generation depends on the shape and size of vocal tracts, lips, nasal cavities, and mouth. The movement of lips, jaws, tongue, velum, and larynx constitute the behavioral component of voice which can vary over time due to person's age and medical condition (e.g., common cold). The spectral content of the voice is analyzed to extract its intensity, duration, quality, and pitch information, which is used to build a model (typically the Hidden Markov Model) for speaker recognition. Speaker recognition is highly suitable for applications like tele-banking but it is quite sensitive to background noise and playback spoofing. Again, voice biometric is primarily used in verification mode.

5. *Hand Geometry Technology*: Hand geometry [9] is based on the fact that nearly every person's hand is shaped differently and that the shape of a person's hand does not change after certain age. Hand geometry systems produce estimates of certain measurements of the hand such as the length and the width of fingers. Various methods are used to measure the hand [8].

Person identification using hand geometry utilizes low resolution (~20 ppi) hand images to extract a number of geometrical features such as finger length, width, thickness, perimeter, and finger area. The discriminatory power of these features is quite limited, and therefore hand geometry systems are employed only for verification applications (1:1 matching) in low security access control and time-and-attendance applications [5].

The following Fig: 7 briefly compare five biometric techniques according to seven parameters: [3]






BIOMETRIC	FINGERPRINT	FACE	HAND GEOMETRY	IRIS	VOICE
					
Barriers to universality	Worn ridges; hand or finger implementation	None	Hand Implementation	Visual impairment	Speech impairment
Distinctiveness	High	Low	Medium	High	Low
Performance	High	Medium	Medium	High	Low
Collectivity	Medium	High	High	Medium	Medium
Performance	High	Low	Medium	High	Low

Fig: 7 Comparisons of Biometric Techniques

PERFORMANCE METRICS FOR BIOMETRIC SYSTEMS

There are various parameters by which we can measure the performance of any biometric Techniques. Some of such factors are discuss below.

FMR (False Match or Acceptance Rate): FMR means the rate at which the biometric measurement from two different individuals is mistaken to be from the same individual [3] [4]. Simply it is a measure of the percent of invalid inputs that are incorrectly accepted. The lower the biometric identification system's FMR, the better the security [3].

FNMR (False Non-Match or Rejection Rate): FNMR means mistaking two biometric measurements from the same individual to be from two different individuals [3]. Simply it is a measure of the percent of valid inputs that are incorrectly rejected [4]. The lower the biometric identification system's FNMR, the easier the system is to use [3].

Relative Operating Characteristic: It is a curve drawn between the False Accept Rate vs. the False Reject Rate.

- The shape of the curve depends on the threshold value set for acceptance. If the threshold value (for the difference or the distance between the templates) is too small, the FAR would be low, but the FRR would also be high. If the threshold value is too high, the FAR would be high, but the FRR would be low [4].

Crossover Error Rate (CER): The rate at which both the accept and reject errors are equal [4].

Failure to Enroll Rate (FER): The rate at which attempts to create a template from an input is not successful.

- This is most commonly caused by low quality inputs that are insufficiently distinctive biometric samples or from a system design that makes it difficult to provide consistent biometric data.
- Larger the FER, lower the FAR and FRR; and vice-versa [4].

Failure to Capture Rate (FCR): Applicable for automated systems, the probability that the system fails to detect a biometric input when presented correctly [4] [10].

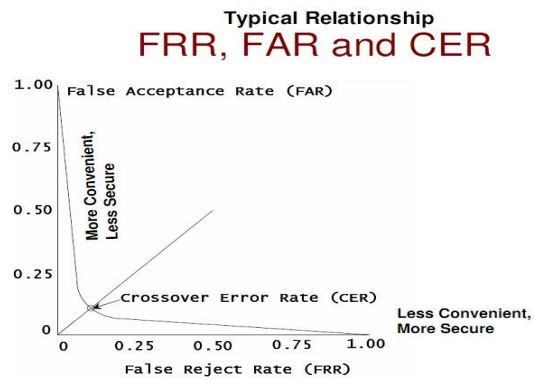


Fig: 8 Relationship of EAR, FAR, CER

Table 1 shows the evaluation of six biometric techniques based on the above discussed factors.

Table 1: Evaluation of Biometric Techniques [10]

Biometric	EER	FAR	FRR	Subjects	Comments
Face	NA	1%	10%	37437	Varied light, Indoor/Outdoor
Finger print	2%	2%	2%	25000	Rotation and Exaggerated Skin distortion
Hand geometry	1%	2%	2%	129	With rings and improper placement
Iris	0.1%	.94%	.99%	1224	Indoor Environment
Key strokes	1.8%	7%	.1%	15	During 6 Months period
Voice	6%	2%	10%	30	Text dependent and multilingual

CONCLUSION

Biometric authentication is highly reliable, because physical human characteristics are much more difficult to forge than security codes, passwords and hardware keys. Proper design and implementation of the biometric system can increase the overall security. But the accuracy of the Biometric System is not perfect yet. In future we will study on advanced biometric technology such as DNA, Palm prints, Odor etc and try to implement them for modern information security.

REFERENCES

- [1] (Emanuele Maiorana, Chiara Ercole, Secure Biometric Authentication System Architecture using Error Correcting Codes and Distributed Cryptography.
- [2] Fernando L. Podio and Jeffrey S. Dunn. Biometric Authentication Technology: From the Movies to Your Desktop.
- [3] Fahad Al-harby, Rami Qahwaji, and Mumtaz Kamala. Secure Biometrics Authentication: A brief review of the Literature.
- [4] Dr. Natarajan Meghanathan. Biometrics for Information Security.
- [5] Anil K. Jain, Ajay Kumar, Biometrics of Next Generation: An Overview. SPRINGER, 2010.
- [6] Debnath Bhattacharyya, Rahul Ranjan, Farkhod Alisherov A., and Minkyu Choi. Biometric Authentication: A Review, International Journal of u- and e- Service, Science and Technology, Vol. 2, No. 3, September, 2009.
- [7] Dr. JK Schneider. BIOMETRICS, SMARTPHONES AND THE E-WALLET. 2011.

- [8] Zdenek Ríha, Václav Matyáš. Biometric Authentication Systems. FIMU Report Series.
- [9] Phalguni Gupta, Ajita Rattani, Hunny Mehrotra, Anil Kumar Kaushik. Multimodal Biometrics System for Efficient Human Recognition.
- [10] Debnath Bhattacharyya, Rahul Ranjan, Poulami Das, Tai Hoon Kim, Samir Kumar Bandyopadhyay, Biometric Authentication Technique and Its Future probabilities. IEEE Trans Int. conf. On Computer and Electrical Engineering, pp. 652-655, 2009.
- [11] A. K. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security," IEEE Transactions on Information Forensics and Security, vol. 1, no. 2, pp. 125-143, June 2006.