Available online at www.ijapie.org

INTERNATIONAL JOURNAL OF ADVANCED PRODUCTION AND INDUSTRIAL ENGINEERING

IJAPIE-2018-04-223, Vol 3 (2), 13-17

IJAPIE
Connecting
Science & Technology
with Management.

A Journal for all
Products & Processes.

Biometrics in Healthcare

Himanshi, Trisha Gulati, Yasha Hasija*
(Department of Biotechnology, Delhi Technological University, Delhi, India)
Email: yashahasija@dtu.ac.in

Abstract : Biometrics is the discipline to measure physical human characteristics for identification and authentication of an individual. Since ancient times, people have used voice, face and other characteristics for identification of an individual. With evolution, we take the individual characteristics like fingerprint scans, retina and iris image, etc., as inputs to the computer systems and then store or verify them with existing records.This report discusses about biometrics and its recent role found in the field of healthcare, medicine, genetics and biotechnology. It includes the concept of biometrics, the system used for biometric recognition and its working, types of biometric systems, the different system algorithms applied along with system modules.Biometry has enabled the proper organization and storage of the health records of individuals in medical institutes. Biometric authentication is also finding a distinct role in foiling medical claims fraud highlighting the advantages of it. Even after processing via a very accurate biometric system there is a chance of a false result due to some disease or injury to the body part subjected to biometry or faulty system leading to some error. In addition, the biometric records need really tight system security to prevent any kind of misuse. In future, biometrics can be used to detect potential disease and risks by using methods like adiposity measurement and Gas Discharge Visualization (GDV).

Keywords: Authentication, Biometrics, FAR, FRR, Verification

1. INTRODUCTION

Biometrics (derived from bio i.e., life and metrics i.e., measurement) is the technology to measure characteristics of an individual for identification and authentication [1]. A highly secure and convenient authentication can be provided by biometrics for an individual as no one can steal and forge it [2]. Unique **physiological** or **behavioral** characteristics are the basis for identifying and authenticating the existence of a living being using biometric technologies.

Physiological characteristics categorize those physical characteristics which are relatively stable in body, such as fingerprints, iris pattern of an individual, hand form or blood vessel stencil at the eyes' back. Such types of biometric measurements generally do not change and are unalterable without significant damage to the body part of the individual [3]. A behavioral characteristic reflects an individual's psychological makeup. It is not a body part of an individual but the way one's body behaves such as signature.

2. WORKING OF BIOMETRIC SYSTEMS

The biometric system process involves the following two stages –

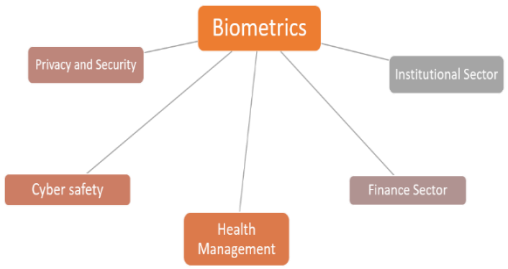

Fig. 1 Flowchart showing role of biometrics in healthcare

2.1.1 Enrollment:

The biometric image of the individual is scanned by using a scanner for fingerprint, camera for face detection, scanner for retina or iris scan etc. midst the stage of enrollment. This data is then extracted from the format in which the information of biometric is scanned or captured to form the biometric template of the user. A database or a machine-decipherable identity card is used for the storage of biometric template which can be used later for other stage, that is, identity verification process.

2.1.2 Verification:
Following figure depicts the identity verification process. The biometric characteristic is reiteratively taken as an input to the system. The unique data is culled from the input biometric format to form the new biometric template of the user. A comparison between the new template, which is received "live" and the template which is already maintained in database is performed. As an observation, calculation of a numeric matching score built on the proportion of match between the live and stored templates is performed. A threshold value is determined by the system designers for this identity verification score according to the safety concerns at the moment.

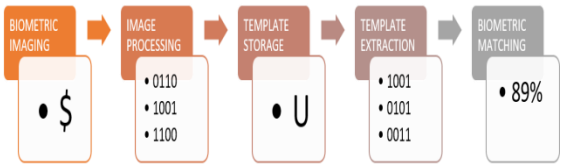

Fig. 2 Working of a Biometric System

I**dentification** process is used to confirm that the biometric data of an individual does not exist in the database with another identity and is not on a list of individuals who are forbidden by law. Identification requires a secured database that contains all the users and their respective biometrics data. The biometrics of the person being enrolled would be tested against the maintained biometrics of all the individuals. Generally, the process of identification is used only once for an individual, that is, at the instant of enrollment to ensure that his/her biometrics are not already existing in the database.

The credentials presented by an individual are confirmed whether they belong to him/her or not by using the process of **authentication** (also known as one-to-one comparison process because the biometric data received from an individual are cross-checked with the stored data of his/her account only). The system that takes the biometric input of the user must have ingress only to his/her enrolled biometric template, with the storage being local or central [4].

A multimodal system can be a combination of any types of biometrics. For example, Indian Aadhar system is a multimodal biometric system which uses fingerprints, irises scan and face recognition. It is estimated that approximately 5% of the world population do not have readable fingerprints due to some serious damage or mutation such as adermatoglyphia. The multimodal biometrics utilizes the proficiency of each single biometric and overcomes such limitations of single biometric systems.

2.2 Biometric Accuracy
Biometric accuracy aids the biometric system in separating the genuine matches from imposters. A matching score which helps to decide confirmation or denial of the user's identity is generated when the newly enrolled biometric template is subjected to comparison with a stored biometric template. Designers of the biometric system assign this numeric score to decide the suitable level of accuracy for the system. This biometric system accuracy is measured by the probabilities - False Rejection Rate (FRR) and False Acceptance Rate (FAR).

• The statistical probability that the biometric system will reject the genuine adduced identity of an enrolled person or will not detect an enrolled person is termed as **False Rejection Rate** (FRR).

• The statistical probability of acceptance of false biometric data or verification of incorrect biometrics is termed as **False Acceptance Rate** (FAR).

Both False Rejection and False Acceptance are hazardous to biometric security.

• When the decision threshold matching score is adjusted so that the false-acceptance rate becomes equal to the false-rejection rate, the case is termed as **Equal-Error Rate.**

A false accept happens when an unmatched or mismatched pair of biometrics is regarded as a match. On the other hand, a false reject happens if a couple biometric, which has a match score over threshold, is not accepted by the system. The rate of errors depends on the threshold decided by the system designer as shown in the plot. Generally, the intersection of the area of two errors is displayed by plotting False Acceptance Rate against False Rejection Rate keeping the threshold as the independent variable. The plot depicted in the figure is known as the ROC (Receiver Operating Characteristic) curve. The two errors are contingent on each other because when the rate of one error is reduced with the shift of threshold axis towards it, the rate of other error is increases automatically as the threshold axis moves away from it. Vice versa also holds true for this statement. By choosing a particular point of operation for the system (i.e., a detection threshold), the relative false acceptance and false rejection rates can be determined in a biometric authentication process. It is not possible to have very low (negligible) value of error rates for both the errors (FAR and FRR) at the concomitant instant of time. The FAR error can be reduced to almost zero by setting a high threshold for the system, and similarly the FRR rate can be approximated to zero by setting the threshold at a quite low value. The decision for an appropriate functioning point for the threshold is made according to the requisites of the application of the system, and the FAR versus FRR error rates at that functioning point may vary. Generally, the threshold point is set at equal error rate (EER) functioning point (where FAR=FRR). But, for high security purposes, biometric systems function at a very low FAR (so as to decrease the risk of false acceptance) [5].

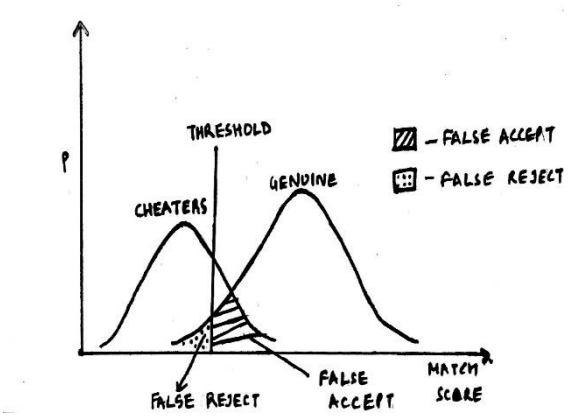

Fig. 2 Error trade-off in a biometric system

2.3 Types

There are many options available for biometric analysis and the respective methods employed to take them as inputs by the biometric system. This includes: DNA Matching, Ear**,** Iris Recognition, Retina Recognition, Face Recognition, Fingerprint Recognition, Vein Recognition, and etc.

Several function-specific factors, such as, the environment in which the process of verification takes place, the profile of user, the requisites for testament accuracy and throughput, the total system expenditure (space and time of program), and ethical issues determine the choice of biometric system [4]. Some of the frequently used biometrics are explained here.

2.3.1 Fingerprint Recognition

For authentication process, the first step is to acquire a fingerprint impression by using a scanner. There are many scanning technologies available for this task like optical, thermal or pressure sensitive scanner. The digital input of the fingerprint impression taken by an archetype fingerprint scanner is at 500 dots per inch (dpi) with 256 gray levels per pixel [5]. There are several unique features in the digitalized image of the fingerprint known as *minutiae*. These minutiae are the patterns obtained due to ridge bifurcations and ridge endings. The three basic fingerprint patterns are Loops, Arches and Whorls [6]. A loop can be classified as a left loop or a right loop depending on which side it is tilted. An arch can also be classified into a subcategory of trenched arch if it is very steep. Every fingerprint falls into one of these patterns. Within these patterns, we find some specific turning and twisting points known as minutia points. These minutiae points are of about thirty types. These minutiae points make the fingerprints unique because no two people have the minutiae of same types, in the same number and at the same position on their fingertips.

After taking the fingerprint scan, minutiae are located in the fingerprint image employing an automated feature extraction algorithm. The two attributes of each feature are its location *(x,y)* and the direction of ridge at that location *(θ)*. But, because of disturbances in sensor and more volatility in the course of fingerprint imaging, some minutiae may be missed during the feature extraction stage and spurious minutiae may be generated. Sometimes, the elasticity of human skin can cause distortions in the impressions of similarity between minutiae. During the final stage, the matcher subsystem analyses degree of analogy between the two sets of minutiae after bringing down the two images to comparable angle of rotation, translation, and scale. This similarity expressed in terms of match score and based on this score, it is decided that the two fingerprints match or not. Generally, the sum total of the number of the minutiae that are in conformity is taken as score.

2.3.2 Iris Recognition

Iris is the dark pupil area of the human eye which is pigmented or constitutes of colored circles, rings. It is the visible (via regular and/or infrared light) appearance of the iris on which Iris recognition is based. A primary visible characteristic of iris is a tissue that elicits an appearance of radial lines separating the iris called the trabecular meshwork. This meshwork tissue is completely formed by the 8th month of gestation. Rings, furrows, freckles, and the corona are some other visible features of iris. The technology used for iris recognition transforms such discernible characteristics into a 512-byte template which can be maintained in database. This information density is such that each iris can be said to have 266 unique points of identification while other biometric technologies have 13-60. First of all, the eye (to be scanned) is located within the range of 3 feet from a high-definition camera. After the camera locates the eye, the system algorithm oscillates between the ends of the iris to find the location of its outer edge. Such horizontal approach is employed to avoid the obstruction caused by the eyelids and lashes. We can also locate the inner edge of the iris using this approach [7].

Both visible and infrared light are used by monochrome camera. The latter one lies in the range of 700-900 nm (lower range of IR). After locating the iris, 2-D Gabor wavelets is used by the algorithm to sieve and map the sectors of the iris into numerous vectors (called phasors). These varied length and amplitude wavelets impute values extracted from the orientation/pattern and spatial arrangement of select are onward with the location of these areas. The orientation and position are utilized to establish the Iris Code (template). A top portion, as well as 45 degree of the bottom, is not used for iris recognition to account for the hindrances like eyelids and camera-light reflections.

Iris recognition can account for its ability to determine fraudulent samples in several ways: the detection of changes in pupil; detection of contact lenses over the cornea; light reflected from the cornea and infrared rays being used to establish the status of the scanned eye tissue.

2.3.3 Face Recognition

One of the latest biometric technologies is face recognition. These systems recognize people's faces with the help of specialized recognition software coupled with video camera. Facial scan technology recognizes faces of peoples by various methods. Emphasizing less alterable sections of the

face, comprising the upper outlines of the eye sockets (bone cavity and muscles containing the eye), the areas which surround one's cheekbones and the sides of the mouth are some common aspects of all face recognition methods. Sample capture, template analogy, feature derivation and matching are the gradations of facial scan process. One to one verification process involves clicking several photos of one's face with each sample having a 20-30 second enrollment process. Each picture in the series is taken with slight difference in angles and facial expressions, so that more precise searches can be allowed. After enrollment a template is created by extraction of distinctive features. The templates require much smaller than the image for storage.

In the process of authentication, a user takes an identity like a user name or a PIN, gets his/her face recognized by the camera for a few seconds, and the claim is either detected or declined. The decision is made by comparing the live template with the stored template or templates on file. The threshold is pliant for different people, systems, time etc. Facial scan technology is also used in forensics and hospitals. Large databases are used to store biometric templates obtained from stationary photographs of known criminals.

2.4 System Algorithm

Following are the modes of operation for a biometric system contingent on application context:

- Midst the verification mode, the system confirms identity of a person by keeping the live biometric data in juxtaposition with its already stored biometric template(s) maintained in the database of the system. In this mode of system, an identity is claimed by an individual who wishes to be recognized, generally via a PIN (Personal Identification Number), smart card, a username etc. [8]. For this, a one-to-one comparison is conducted by the system to determine whether the claim made by that person is true or not. When we want to avert many people from employing the same identity, verification is used.
- Midst the identification mode, the system searches the templates of all the enrolled users in the database to look for a match in order to recognize an individual. Therefore, a one-to-many comparison is conducted by the system to form identity of an individual (or becomes redundant if the biometric is not stored in the system database) without the need of claiming an identity. Identification mode of biometrics is the only way for negative recognition i.e., the system establishes whether the individual is who he/she disapproves to be.

The term **recognition** can be employed for both verification and identification.

The verification problem can be explained as follows:

Let us consider PQ is an input feature vector (obtained in digitized form from the biometric data) and I is a claimed identity. Now it is to be determined if (I, PQ) is a part of class C1 or C2, where C1 represents the case of true claim (a genuine user) andC2 represents the case of false claim (an impostor). Now the next step is to match PQ against PI to determine its category. PI is the biometric template akin to user I.

Thus:

$(I, PQ) \in (C1)$, if $F(PQ, PI) \geq t$

$\in (C2)$, otherwise (1)

Where F is the function defined such that it weighs the match between feature vectors PQ and PI, and the variable threshold is t. The result for the matching function F (PQ, PI), also known as matching score, is the representation of ratio of similarity betwixt the biometric measurements of the live user and the identity which is obtained from the stored database. Therefore, depending upon the variables PQ, I, PI and t, and the function F; every identity which is claimed can be classified into either of the cases C1 or C2. For an individual, biometric measurements taken at different instant of time are almost never identical because of different physical conditions in which it measured. This is why the threshold t is introduced. The problem of identification may be explained as follows:

There is an input feature in the form of vector PQ;

The identity I_k is determined, where $k \in \{1,2,...N,N+1\}$

Here $I_1, I_2, \ldots, I_N$ are the identities which have already been stored in the system and I_N+1 represent the case which is to be rejected where no appropriate identity can be established for the user.

Hence,

$PQ = I_k$, if $\max \{(PQ, PI_k)\} \geq t$, $k = 1,2,3 \ldots\ldots N$,

$= I_N+1$, otherwise, (2)

Where PI_k is the biometric template related to identity I_k, and t is the threshold defined for the system [9].

Following are the four main modules comprising the design of a biometric system:

1. Sensor module: This module grabs an individual's biometric data by sensing via optical, thermal, vibration or other physical method. For example, the ridge &valley pattern of an individual's finger scanned by a Fingerprint sensor.

2. Feature extraction module: Processing of biometric data takes place in this system module to extract unique biometric features and converting it into digitalized form. For example, the positioning and orientation of minutiae points in an image of fingerprint is a task that takes place in this module.

3. Matcher module: In this module the biometric features are analyzed with the templates of the database to create matching scores during recognition. For example, matching score is generated by comparing the new data and the stored template images in the matching module of a Fingerprint-based biometric system.

4. System database module: This module is used to cache the templates of the already enrolled users. Individuals are enrolled into the database of biometric system by the enrollment module. The biometric feature of a person is examined and then converted to a digital representation (feature values) during enrollment phase.

3. CONCLUSION

Biometry has enabled the proper organization and storage of the electronic health records of individuals in medical

institutes. The healthcare industry requires biometrics at high rates; the current estimation of overall market potential is of more than $1.9 billion. HIPAA (Health Insurance Portability and Accountability Act of 1996, USA) has imposed requisites to assure privacy and the confidentiality of patient information. As nobody can steal one's biometric identity, the risk of fraud is reduced. However, after the processing via a very accurate biometric system there is a chance of a false result due to some disease or injury to the body part subjected to biometry. There is also a possibility that the biometric system may harm our body. For example, lights/EM waves of the eye scanning system may harm eye of the user. Also when a biometric data is stored in computer, it just like any other digital data (encrypted or non-encrypted) for a determined pirate. Biometrics has a great potential to find a lot more uses in the field of healthcare. In future, biometrics can be used to detect potential disease and risks by using methods like adiposity measurement and Gas Discharge Visualization (GDV). Adiposity measurement can help to detect tumor or cancer growth in body. Biometrics of veins can be used to detect disorders related to blood flow. Medical history of a patient can also be used as a biometric in future because no two people can have same biometric history.

REFERENCES

[1] http://www.iritech.com/blog/biometric-accuracy-evaluation/
[2] Dana Marohn (2006). Biometrics in healthcare. In Biometric Technology Today 14(9): 9-11. https://doi.org/10.1016/S0969-4765(06)70592-6
[3] A Strong Pulse for Biometrics in Healthcare. (2013, September 27). Retrieved October 4, 2017, from http://www.planetbiometrics.com/article-details/i/1745/
[4] Schneider, John K. Positive Outcomes Implementing Biometrics in Multiple Healthcare Applications. (2011). Retrieved September 16, 2017, from http://www.ultrascan.com/Portals/16/PositiveOutcomes.pdf
[5] D. Peralta, I. Triguero, R. Sanchez-Reillo, F. Herrera, J.M. Benitez (2014). Fast fingerprint identification for large databases, Pattern Recognition. 47(2):588-602. https://doi.org/10.1016/j.patcog.2013.08.002
[6] Fingerprint Biometrics Help Secure Medical Data at Arizona Hospitals. (2011, August 30).Retrieved September 15, 2017, from http://www.homelandsecuritynewswire.com/fingerprint-biometrics-help-secure-medical-dataarizona-hospitals
[7] Bhattacharyya Debnath, Ranjan Rahul, Alisherov Farkhod, Minkyu Choi (2009). Biometric Authentication: A Review. International Journal of u- and e- Service, Science and Technology 2(3): 13-28. http://www.earticle.net/Article.aspx?sn=148496
[8] Yong Zhu, Tieniu Tan and Yunhong Wang (2000). Biometric personal identification based on iris patterns. Proceedings 15th International Conference on Pattern Recognition. ICPR-2000, Barcelona, 2:801-804. https://ieeexplore.ieee.org/document/906197/
[9] Abbasi Akber Asima, Khan M.N.A. and Khan Ali Sajid (2013). A Critical Survey of Iris Based Recognition Systems. Middle-East Journal of Scientific Research 15 (5): 663-668. https://www.idosi.org/mejsr/mejsr15(5)13/8.pdf .