Journal of Theoretical and Applied Information Technology
30th June 2019. Vol.97. No 12

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

COMPARATIVE AND ANALYSIS STUDY OF BIOMETRIC SYSTEMS

FAOUZIA ENNAAMA[1], KHALID BENHIDA[1], AHMED BOULAHOUAL[1]

[1]CadyAyyad University, High School of Technology, LAPSSII Laboratory, Safi-MOROCCO

E-mail: [1]faouziaennaama@gmail.com

ABSTRACT

In recent years, there has been a growing interest in the field of biometrics as a powerful identification technology. Various biometric technologies are based on behavioral and physiological analysis; therefore they must be reliable, robust, simple and cheap.
In this paper, we have investigated an analytical comparison of different biometric systems namely: fingerprint, iris, face, voice, keystroke dynamics, signature, retina, etc. and we have classified these methods based on several criteria such as: universality, uniqueness, permanency, intrusiveness, effort, cost, and reliability, as well as the most used biometric systems requested in the market and those that are of greater interest in the current research work, and for each criteria we gave synthetic discussions. Furthermore, we provided a brief overview of biometric methods, then we have described the modes used in a biometric system such as enrollment, verification and identification and we have presented the possible applications of biometrics.

Keywords: *Biometric Systems, Identification, Recognition, Biometrics, Face.*

1. INTRODUCTION

Today, determining the identity of an individual automatically is a problem that is still relevant. In a daily environment that is becoming increasingly interconnected, it is necessary to have automatic and reliable authentication systems to identify users and give them access to specific systems and applications such as: e-commerce, banking, highly secure places, etc.

Traditional systems based on the use of passwords and identity cards cannot provide guaranteed authentication functions because–they have a lot of weaknesses. In the first case, the password can be forgotten by the user or decoded by another person. In the second case, the badge (or identity card or key) may be lost or stolen. Biometric systems are an alternative solution to the two previous identification modes.

Biometrics involves identifying a person from one or more physiological characteristics (fingerprints [1], face [2], iris [3], hand geometry [4], retina [5], palmprint [6], etc.), or behavioral characteristics (signature [7], gait [8], keystroke dynamic [9], etc.). Etymologically, human biometrics is synonymous with physical anthropology [10]. Another definition of biometrics is given by Roethenbaugh [11] Biometrics are: “a measurable characteristic or trait of a human being for automatically recognizing or verifying identity”.

In general, biometric characteristics have seven factors that make them appropriate for biometric measurements and identification or authentication. These properties are [12]: (a) universality, which means that every person should have the attribute, (b) uniqueness, theoretically refers that two people cannot have exactly the same characteristic, (c) permanence, which indicates that the trait should be invariant with time, (d) collectability, which indicates that the characteristic can be measured quantitatively [12,13], (e) performance, which means the accuracy of the identification and the needed resources to achieve this accuracy must respect the constraints imposed by the application, (f) acceptability, which indicates, individuals who use the application must present their biometric features to the system, and (g) circumvention, which is about the easiest information to be collectible, measurable and usable for comparison.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Biometric systems are automatic systems essentially using various modalities to identify or / and recognize an individual [14], including fingerprint, face, hand geometry, iris, retina, signature, gait, palm print, voice model [15], ear [16], vein of the hand [17], DNA [12], etc.

In fact, a practical biometric system must have an acceptable accuracy and a reasonable recognition speed with respect the required resources, harmless for the users, accepted by the population, and robust enough against fraudulent methods [18].

This paper provides a comparative and analytical study of biometric systems. This investigation based on the review of the biometric methods, their recent developments and their statistical analysis of submitted publications rate in a scientific journal will be discussed in detail. We have chosen to organize this paper around five parts: The first section is dedicated to Biometric system and its possible modes commonly used. The second section gives a description of biometric methods; the third section is about the applications of the most requested biometric systems on the market. The comparison results will be discussedin the fourth section and the conclusion will be given in the last section.

2. BIOMETRIC SYSTEM AND ITS MODES

A biometric system is an automatic system based on the recognition of the biometric characteristics of an individual.

Generally, a biometric system can operate in three modes [19]: in enrollment mode, in verification mode or in identification mode.

- **Enrollment**: This is the first step of a biometric system. It aims to collect biometric information of the individual to identify him. Several data acquisition steps must be performed in this mode namely; data acquisition, pre-processing and feature extraction. The data acquisition is done by a biometric sensor to collect the biometric data of the individual. Then, in the pre-processing stage, these characteristics will be represented in digital form (signatures), after the suppression of the different sources of noise of the individuals collected data. Furthermore, this information is stored in a specific database. We note that the processing related to enrollment is not subject to time constraints, since it is done in "offline" mode.

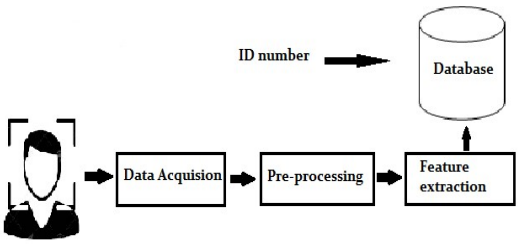

Figure 1: Block diagram of a biometric system in enrollment mode.

- Verification: This is a one-to-one comparison step (usually 1:1) [19], it consists of four main methods namely: data acquisition, pre-processing, feature extraction and matcher. This mode verifies the identity of an individual by comparing the extracted biometric signature with his or her own pre-recorded biometric template in the system database. If it is correct, he accepts it otherwise he rejects it.

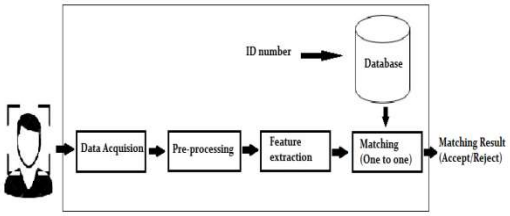

Figure 2: Block diagram of a verification system.

- **Identification:** consists of comparing the characteristic in question, often called the user's model with the equivalent models of all the users, already stored in a database. It is a comparison "1 to N" [19]. The identification is also composed of four sub-parts such as: data acquisition, pre-processing, feature extraction and matching (One to Many). These subparts work in the same way as in the case of verification, except in a matching phase. In this mode, the comparison is done as one by one while in the verification, all the data stored in the database will be compared to have a better possible correspondence with the model of the user. This mode involves associating an identity with a person.

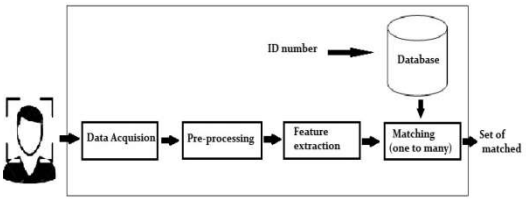

Figure 3: Block diagram of an identification system.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3. BIOMETRIC METHODS

A biometric system automatically identifies an individual based on two main biometric modalities: physiological and behavioral.

- Physiological Biometrics: This type is based on the identification of particular physical traits that for any individual are unique and permanent. This category includes: fingerprint, contour of the hand, face, retina, DNA, iris, etc.
- Behavioral biometrics: This type is based on the analysis of certain behaviors of an individual such as the tracing of his signature, his gait and his keystroke dynamic.

In this part, we present a brief introduction to some commonly used biometric modalities; figure 4 shows some example of biometric modalities.

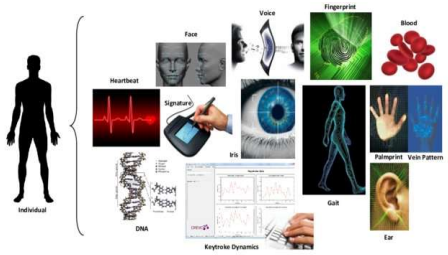

Figure 4: Some examples of biometric modalities [20].

- **Fingerprint:** is the design represented by the ridges and valleys of the epidermis. It consists of a set of locally parallel lines forming a unique and different pattern for each individual [1]. We differentiate the streaks or ridges - the lines in contact with a surface to the touch - and the valleys - the hollows between two streaks -. The streaks contain in their center a set of regularly spaced pores. Each imprint has a set of global (centers and deltas) and local (minutiae) singular points [21]. The first traces of human fingerprinting have been discovered on a large number of archaeological artifacts and historical items [1]. Although these discoveries prove that ancient peoples were aware of the individuality of fingerprints, this scientific technique was not approved and initiated until the end of the sixteenth century.At the beginning of the 20th century, fingerprint recognition was officially accepted as a valid personal identification method and became routine in forensic science [22]. Worldwide fingerprinting agencies and criminal fingerprint databases have been created. Automatic fingerprint recognition technology has evolved rapidly beyond forensic applications into civilian applications [22]. With strong recognition performance and the growing market for low-cost personal computers and acquisition devices, fingerprint biometric systems are becoming very popular and may be used in a variety of applications such as PC login, e-commerce, ATMs, physical access control, etc.The principle of each biometric fingerprint system consists first of all in capturing and recording the image of the finger by an acquisition system. This image is then transmitted to a processing system that will analyze it and compare it with those already recorded. The data acquisition is done by an electronic sensor of optical, thermal, capacitive or ultrasonic type [1].Subsequently, the captured image of the fingerprint will be initially binarized to increase the contrast, reduce the volume and increase the speed of processing. Then the system extracts the minutiae. This extraction makes it possible to establish a template of the imprint that will be compared to that already stored. The identification or recognition is performed by comparing the template of the test fingerprint with all previously saved templates.
- **Iris:** The iris is the colored part of the eye; it should not be confused with the retina [23], the back of the eye, which is also used as biometrics. It is an extremely reliable technique because it contains an infinite number of characteristic points [24].So we could call it an optical fingerprint [25]. For all these reasons, the iris makes it possible to distinguish different people, even in the case of monozygotic twins.In addition, the texture of the iris of the right and left eyes belonging to the same person are different [25]. Most of the work on iris identification and verification was done in the 1990s [26]. However, early systems have limited capacity to recognize the identity of the individual with precision and efficiency, so that much more needs to be done to improve some technologies by adding other performances from a practical point of view.The main difficulty of human iris recognition is that it is difficult to find apparent characteristic points in the image of the first sight.The acquisition of the iris is done by means of a camera to compensate for the inevitable movements of the pupil. It is very sensitive (precision, reflection ...) and relatively unpleasant for the user because the eye must remain wide open and it is

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

illuminated by a light source to ensure proper contrast.

- **Face**: This method looks at the face shape. Robust systems of facial recognition are in great demand in several applications against crimes and terrorism, as well as the access control of personnel regardless of physical or virtual space.Moreover, face recognition is a non-intrusive method, and facial attributes are the most common biometric characteristics used by human beings to recognize each other.The most popular approaches to face recognition [2] are based on: (i) the location and shape of facial attributes, such as the eyes, eyebrows, nose, lips and chin, and their relationships and spatial distances; (ii) the overall analysis of the facial image: which represents the image of the face as a linear combination of its characteristics.Although the authentication performance of commercially available facial recognition systems is reasonable [27], it imposes a number of limitations on how facial images are obtained, often requiring a fixed and simple background to controlled lighting.These systems also have difficulty matching face images captured from two different views, under different lighting conditions and at different times.For a face recognition system to function properly in practice, it must automatically (i) detect whether a face is present in the acquired image; (ii) locate the face if there is one; and (iii) recognize the face from a general point of view (i.e. any pose) under different environmental conditions.
- **Voice:** The voice is an interesting biometric feature and is extremely sought after in systems related to remote applications where the individual authenticates himself by telephone for example. Voice biometrics aims to identify the idiosyncratic characteristics of the speech signal, produced at a given moment and under specific conditions.Indeed, the production of speech is a complex process that is influenced by several factors at different levels [28]. As a single speech sample represents several types of information, both linguistic and typical features encapsulated together.The attributes of the speaker certainly include clues related to the physical properties of his vocal organs. Furthermore, many distinctive non-physiological features of the speaker mark the acoustic signal, such as information about the emotional state of the speaker. In addition, speech is influenced by diastatic (enzymatic), diatopic (depending on the region) and diaphasic (stylistic or situational) variations [29].Voice capture is relatively easy to perform using a microphone, but is sensitive to ambient noise [30]. It should be noted that this technique is nevertheless difficult to use because it is extremely subject to external conditions (illness, stress of the person, etc.) [28, 29, 30]. Because of this, it is both a physical and a behavioral characteristic. It is sometimes chosen in combination with another characteristic (voice and writing for example).On the other hand, in everyday life, identifying a person through a recording of his speech is an ordinary task that can be found in many cases. For example, a listener may know a speaker's voice easily either over the phone or in a crowd of individuals. Also, in court applications, a voice recording may be the only evidence to recognize the identity of the criminal.The main purpose of voice recognition is to extract the characteristics contained in a speech signal that is physically like a variation of the air pressure produced by the articulator system [31].This signal will be converted by sampling into an electrical signal obtained at the output of a microphone, so that it can be compared to models in digital form. Then it will be quantified in discrete values of amplitude.Then, the noise of the acoustic signal must be removed and made very clear in order to be transformed into a series of vectors typically having from 8 to 50 coefficients [31]. Subsequently, it is generally necessary to reduce the size of the acoustic vector by keeping the maximum of the characteristic information of the original signal.
- **Hand Contour (Hand geometry)**: This is a popular technology that is widely used for physical access control or clocking[32]. Historically, Jain and Duta [33] were the first to analyze a deformable shape and develop a method in which hand shapes are stored and compared according to the average misalignment.The main advantage of this modality is that it is simple and easy to capture. In addition, the biometric system is not very sensitive to the state of the hand, in other words, dirt and cuts will not prevent its operation [32].However, the geometry of the hand also has disadvantages that can make the system imprecise. Indeed, different individuals can have almost similar hand shapes. In addition, jewelry and accessories can be a challenge to extract shape information from the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

hand.Also known as hand measurements in literature, hand geometry has been the subject of much attention from hand biometrics. As its name indicates, the user positions his hand on the system to take different geometric measurements, namely the size of the palm, the length of the hand or the fingers, the width and the perimeter of the hand and the fingers, etc.In particular, Luque-Baena et al. [34] extracted 403 geometric features, including areas, perimeters, circularity measurements, compactness, etc. This is actually the highest number adopted in the literature to improve the performance of the personalrecognition system. Although geometric features are easy to extract, they are not discriminating enough to be used for high security identification or verification situations.In fact, the error rate in hand recognition is quite high, especially for people belonging to the same family because of a strong similarity. Moreover, the shape of the hand changes a lot with age [35].Therefore, some authors suggest the fusion of geometric features with other features of the hand such as palm-prints [36] or finger shapes [37].

- **Palmprint**: is one of the most commonly used biometric recognition techniques used for crime.The palm print represents the inner part of the hand (the invisible part when the hand is closed) between the wrist and the base of the fingers. The use of the characteristics of the palmprint in the identification process was originally proposed by Shu and Zhang [38]. The modality of the palmprint impression contains different types of characteristics that can be exploited for the recognition of the person [38]: (1) Determine vertical line segments, (2) Detect the secondary wrinkles or folds and (3) Determine the ridges.All these properties can characterize a person because they are stable over time. Regarding wrinkles or secondary lines, they are thinner and more irregular than the main lines. High resolution imaging is required for good extraction of minutiae. The retinal vascular system is rich in structures. It is claimed to be the safest biometric modality such as the iris.
- **Retina**: This is an old technique that uses the iris. It is based on the fact that the blood vessels of a retina are unique for each person. Even, the structures of the right and left eyes are different.The retina of a person is unique and remains unchanged throughout life [39].The retinal vascular system is rich in structures. It is claimed to be the safest biometric modality such as the iris.The acquisition of the retina is as follows: The person must place his eye in front of a capture hole located on the acquisition device [40]. A light beam passes through the eye to the capillary blood vessels of the retina. The system locates and captures about 400 reference points [40]. This technique requires close cooperation on the part of the user, as he must place his eye extremely close to the camera. This technology is very secure and reliable, which is why it is used in high-end security applications such as military installations and power plants.
- **Ear**:is a new viable biometric class because it has desirable properties such as universality, uniqueness and permanence [41]. For example, the ear is rich in features; it is a stable structure that does not change with age; thus, it does not change shape with facial expressions, cosmetics and hairstyles. The ear is largely compared with the iris, retina, and fingerprint and therefore is more easily captured at a distance [14].Although it has advantages over other biometric systems, it has not attracted attention compared to other biometric systems such as face, fingerprint and gait.
- **Gait**:indicates the way a person walks. This method is one of the few biometric features to recognize people at a distance [8].Therefore, this attribute is very appropriate in surveillance scenarios where the identity of an individual can be established confidentially. Most gait recognition algorithms extract the human silhouette in order to remove the spatio-temporal characteristics of a moving individual. It is for this reason that the choice of a good model to represent the human body is essential to the effective functioning of a gait recognition system.Gait based systems also provide the ability to follow a person for a long time. However, an individual's gait is influenced by several factors, including the choice of shoe, the type of clothing, leg support, walking surface, etc [42].
- **Signature**: is the way in which a person signs his name to be a characteristic identifying that individual [7]. This handwritten is a biometric behavioral technique that can change over time, influenced by the physical and emotional conditions of the signatories [43]. This type of biometrics is currently little used but its defenders hope to impose it quickly enough for specific applications.Although signatures require user contact with a writing tool and a

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

graphics palette, they have been accepted in government, legal, and commercial transactions as an authentication method.The signature processcontains a graphic palette with a pen. This device will measure several characteristics during the signature, such as speed, order of strikes, pressure and accelerations, total time, etc [7]. The major disadvantage of handwritten signature is that even if the signatures of the same person can change dramatically, thieves can produce the same signatures that fool the signature verification system [14].

- **Keystroke dynamics**: This technology doesn't require any special equipment since every computer has a keyboard. It is not unique to each individual but can be expected to provide sufficient discriminatory information to enable identity verification.It is a software device that calculates the amount of time a finger presses a key and the time a finger is in the air (between keystrokes) [9]. This measurement is captured about a thousand times per second. The typing sequence is predetermined in the form of a password. Initially the person must compose his password so that a template is created. This biometric device is used as a verification method for electronic commerce and as a mechanism for controlling access to databases [12].We can say that Keystroke dynamics permits "continuous verification" of an individual's identity over a session after the individual logs in using a performing biometric like fingerprint or iris [14].
- **Multimodality**: Multimodality is defined as the use of different biometric systems. The most importantmain to combine various biometric systems is to reduce the limitations of single biometric systems. In fact, the combination of different biometric systems aims to ameliorate recognition performances by increasing the quantity of discriminant data of each individual, and to have a very low failure.However, biometric systems have so far failed to achieve accurate recognition. Several challenges confronted biometric systems are presented below [14]:
  a. Noise effect: The biometric information presented to the system can be infected by noise due to imperfect acquisition conditions or subtle variations in the biometric value itself. These variations can cause bad illumination as the case of the iris and the face or the dirty surface of the sensor for the case of the fingerprint.
  b. Non universality: although biometric modalities exist in every individual, there are exceptions in which a person is not able to present his biometric trait due to pathological conditions or a working environment characterized even by erasing fingerprint data or palmprint. For example, a fingerprint system may fail to capture the friction peak structure of some individuals due to the poor quality of their fingerprints. Similarly, an iris recognition system may be unable to obtain information about a person's iris because of their long eyelashes or certain pathological conditions of the eye.
  c. Upper bound on identification accuracy: (also called Temporal variability and non uniqueness) that is when the system becomes limited by the observed variations in the set of characteristics of each subject (ie, intra-class variations) and by the variations between sets of characteristics of different subjects (that is, inter-class variations). For example, in the identical twin identity case, the main lines of their palms can lead to an inaccurate match due to incorrect data inducing a false rejection.
  d. Spoof attacks:biometric traits like voice, fingerprint and signature are easily vulnerable to spoofing attacks. For example, the voice can be imitated and fingerprints can be falsified for identity theft.

  In this regard, some of the first multimodal biometric systems reported in the literature combined the face and voice characteristics of individuals [44]. There are other works that combine several modalities such as: ear and face in [45], hand geometry and palmprint in [46], etc.

4. APPLICATIONS OF BIOMETRIC SYSTEMS

Nowadays biometric systems are increasingly integrated in several applications. These applications can be classified into three main groups [47, 48]:

• Business applications: such as computer network opening, electronic data security, e-commerce, Internet access, credit card, physical access control, cell phone, registry management medical, distance learning, etc.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

• Government applications: such as national identity card, driver's license, social security, border control, passport control, etc.
• Legal applications: such as body identification, criminal investigation, terrorist identification, etc.

5. COMPARISON RESULTS OF VARIOUS BIOMETRIC SYSTEMS

Each physiological or behavioral biometric modality has its strengths and weaknesses, and the choice depends on the targeted application. In other words, no biometric system is "optimal" and to be effective, it must have the ability to adapt to the permanent and temporary changes of the user [14, 47].

5.1 Comparison according to biometric modalities properties

In this part, we will give a comparative analysis concerning the biometric modalities based on several studies. We start with Jain et al. who made a comparison according to properties mentioned above (see Table 1).

Table 1: Comparison of the biometric modalities according to the following properties: (a) Universality, (b) Uniqueness, (c) Permanency, (d) Collectability, (e) Acceptability, (f) Performance [13].

Biometric modality	a	b	c	d	e	f
DNA	Yes	Yes	Yes	Not really	Not really	****
Blood	Yes	No	Yes	Not really	No	*
Brain signal	Yes	Yes	Yes	Not really	No	****
Heart signal	Yes	Yes	Yes	Not really	Yes	****
Signature	Yes	Yes	Not really	Yes	Yes	****
Gait	Yes	No	Not really	Yes	Yes	***
Keystroke	Yes	Yes	Not really	Yes	Yes	****
Haptic behavior	Yes	Yes	Not Really	Not Really	Yes	****
Voice	Yes	Yes	Not Really	Yes	Yes	****
Iris	Yes	Yes	Yes	Yes	Somewhat	****
Retina	Yes	Yes	Yes	Yes	Somewhat	****
Face	Yes	No	Not really	Yes	Yes	****
Hand geometry	Yes	No	Yes	Yes	Yes	****
Hand veins	Yes	Yes	Yes	Yes	Yes	****
Ear	Yes	Yes	Yes	Yes	Yes	****
Fingerprint	Yes	Yes	Yes	Yes	Yes	****

For the performance, the number of stars is related to the value of the Equal Error Rate (EER) obtained in the state of the art [13].

5.1.1 Discussion 1

According to this table, we note that no modality is perfect and therefore is not supposed to respond effectively to all the requirements (for example, permanence, acceptability, community) imposed by all applications (Digital Rights Management (DRM), access control, social protection distribution). For example, DNA is one of the most effective techniques for verifying the identity of an individual. But, it cannot be used for access control for reasons of computation time and also because the individual would not be ready to take a little blood to carry out the identification. The choice of the modality is therefore dependent on the application used.

we can also point out that the iris, fingerprint, retina, hand veins are very reliable thanks to their uniqueness and performance; but presently, they are not frequently used because they are thought to represent an intrusion into one's private life and their fabrication costs are very expensive specifically for the iris, retina and hand veins. Methods such as the face, voice, contour of the hand are very acceptable by individuals by reason of their ease of use, and their biometric systems are not expensive to manufacture.In the following part, we will give an analytic comparison according to others performances.

5.2 Analytic comparison according evaluation criteria

Several studies have been conducted to evaluate the performance of biometric systems. The American company - the International Biometric Group [IBG] [49] - for example has carried out a study based on four evaluation criteria:

- Intrusiveness: the existence of a direct contact between the sensor used and the individual to be recognized.
- Reliability: effectiveness of the method (ability to identify someone).
- Cost: cost of the technology (readers, sensors, etc ...), must be moderate.
- Effort: required by the user when entering biometric measurements. That is, techniques that don't need enough effort by the user.

The comparison results of the most used biometric methods used namely: contour of the hand, fingerprint, face, voice, retina, iris, signature and Keyboard Strike are presented as follows [46]:

✓ The least "intrusive" techniques to the most "intrusive": voice, Keyboard Strike, signature,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

contour of the hand, face, fingerprint, iris and finally retina.

- ✓ The most reliable techniques to the least reliable: iris, retina, fingerprint, face, hand, voice, and finally at an equivalent level, Keyboard Strike and signature.
- ✓ The least expensive to the most expensive techniques: Keyboard Strike, voice, signature, fingerprint, face, contour of the hand, retina and finally iris.
- ✓ The easiest techniques of use to the most difficult. Here, it is worth appreciating the degree of possible interaction with the system: face, signature, iris, Keyboard Strike, voice, fingerprint, contour of the hand and finally retina.

On the same subject, the International Biometric Group has carried out a comparative study on the most popular and most used methods in the security market. The results are presented in the form of a graph as shown in the figure 5.

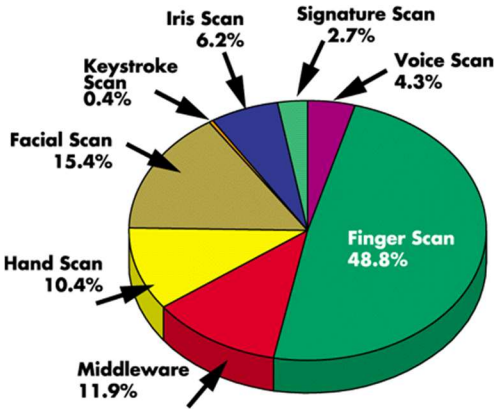

Figure5:Comparative Biometrics Market Share: 2001 [49].

5.2.1 Discussion 2

From figure 5, we can note that the most widespread technologies are fingerprints (48.8% of the market) followed by face recognition (15.4% of the market), hand geometry (10.4%), iris (6.2%), voice recognition (4.3%), retina; ear morphology and Dental radiography represent the remainder of the percentage. It should be noted that behavioral techniques (such as gait, smile, eye movement, etc.) are hard for them to overcome.

Note that fingerprints are the most used biometric characteristics. The first automatic authentication system using fingerprints was marketed in the early 1960s. In addition, several studies have shown that the iris is the most reliable feature because the structure of the iris remains stable over the course of life. However, these methods have the major disadvantage of being intrusive, which greatly limits their areas of application. In addition, a method such as the identification of the iris remains binding for the users. Conversely, identification systems based on the analysis of face images pose no difficulty for users. Face recognition is a method that can be implemented independently of other biometric modalities, and is often used in surveillance applications.

5.3 Statistical analysis of publications on biometrics

Another comparative study was carried out by Prabhakar et al. [50] about statistical analysis of publications specific to biometric techniques submitted and published in the scientific journal IEEE Transaction on PAMI. This analysis compares face, fingerprint, Iris, multimodal biometrics and the "other" category includes: ear, signature, EEG (Electroencephalography), gait, hand, dental, and speaker. Besides, it presents for each subject the percentage of Paper Distributionrelated to one of the above subjects. Table 2 shows the distribution results of submitted and accepted papers[50].

Table 2: Percentage Distribution of Submitted and Accepted Papers by Biometric Subarea [50].

Paper distribution [%]	Submitted	Accepted
Face	33%	32%
Fingerprint	17%	16%
Multimodal	16%	16%
Iris	9%	11%
Performance Evaluation	4%	5%
Other	21%	20%

This study shows that the face recognition is the most published technique at the level of the scientific journal IEEE Transaction with a percentage of 33% of the total number of publications, followed by the fingerprint (17%), multimodal systems (16%), Iris (9%) and finally other category with (22%) because there are four papers on the topics of: handwriting, ear, and two on brain waves or EEG [50].

5.3.1 Discussion 3

Face recognition made up the majority of submissions and accepted papers. There are several factors which make face recognition one of the best biometric methods. It is a task that humans do

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

habitually and naturally in their daily lives, non-intrusive, socially well accepted and easily implemented unlike most biometric modalities, which necessitate professional materiel during their implementation (sensors and scanners for fingerprints, palm prints, retina and iris), face image can be easily captured via digital cameras. Currently, 3D facial representation seems to be a promising method to deal with many of the human face variations such as illumination [51], pose changes [52] and varying facial cosmetics [53]. Moreover, it allows recognizing the individuals at a distance thanks to surveillance cameras [54] and identifying the face of the subject from a multifaceted image [55] contrary to other methods (need contact with the sensors). For these reasons and others the scientific researchers are interested in the face recognition. Fingerprint and iris recognition methods are extremely reliable technique. However, they demand much explicit effort from users. Especially, fingerprint requires that the user puts down his finger to have well physical contact with the surface of the sensor to acquire the image, while iris acquisition currently requires that the individual cooperate to careful position their eye relative to the sensor. The first problem that now arises with these two techniques is to leave the surface of the sensor clean because by dint of use it becomes dirty. The second problem is that the two techniques invade one's private life which makes it inacceptable. There is therefore a very strong demand for improved performance in face recognition systems and increasingly important in the field of research.

Although it has desirable properties such as universality, uniqueness and permanence, the ear biometric is relatively new and not yet widely studied and has not attracted attention compared to other biometric systems such as face, fingerprint and gait.

For the signature, it has the advantage over other biometric measures of being commonly used for transactions. For this reason, the signature as a means of identification is generally well accepted. The problem of signature recognition comes from the great variability that exists between two occurrences of the signature of the same individual. In addition, the signature may be affected by the health or emotional state of the individual or can be falsified by other person.

6. CONCLUSION

Biometric recognition is a powerful tool for increasing security in the private and public sectors. This paper presents an analytic comparison of the main biometric technologies. This comparison is based on several properties like: universality, uniqueness, permanency, collectability, acceptability and performance or their evaluation criteria such as: intrusiveness, effort, cost, and reliability, as well as the most used biometric systems requested in the market and those that are of greater interest in the current research work.

Fingerprint biometrics remains the most widely used technology around the world and is the most requested in the global market. It is a reliable and intrusive technique. The iris technique is one of the technologies (with the retina) that ensure a high level of security. The iris provides a very high uniqueness and extended stability, resulting in extraordinary reliability. These three methods require a great cooperation by the users because of their intrusiveness which makes them unacceptable to users compared to the other methods.

Biometry by the contour of the hand is simple to implement. However, it is not a very reliable technique. The ear biometric is relatively new and not yet widely studied and has not attracted very attention by the scientific community.

Face recognition is a non-intrusive, natural, easy for implementation and less costly method. It is also requested in the market and well accepted by users. Besides it currently acquires a greater interest to the scientific researchers. All of these factors make face recognition one of the best biometric methods.

Finally, behavioral methods such as signing and typing are still known methods but still don't have very high identification accuracy.

REFERENCES:

[1] Maltoni, Davide, Maio, Dario, Jain, Anil K., *et al. Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.

[2] Jain, Anil K. and Li, Stan Z. *Handbook of face recognition*. New York : springer, 2011.

[3] Daugman, John. How iris recognition works. In : *The essential guide to image processing*. Academic Press, 2009, pp. 715-739.

[4] Kumar, Ajay And Zhang, David. Hand-geometry recognition using entropy-based discretization. *IEEE Transactions on information forensics and security*, Vol. 2, No 2, 2007, pp. 181-187.

[5] Sukumaran, S. And Punithavalli, M. Retina recognition based on fractal dimension. *IJCSNS Int J Comput Sci and Netw Secur*, Vol. 9, No 10, 2009, pp. 66-7.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[6] Shu, Wei and Zhang, David. Palmprint verification: an implementation of biometric technology. In : *Proceedings. Fourteenth International Conference on Pattern Recognition (Cat. No. 98EX170)*. IEEE, 1998, pp. 219-221.

[7] Lee, Luan L., Berger, Toby, and Aviczer, Erez. Reliable on-line human signature verification systems. *IEEE Transactions on Pattern Analysis & Machine Intelligence*, No 6, 1996, pp. 643-647.

[8] Lee, Lily, and Grimson, W. Eric L. Gait analysis for recognition and classification. In : *Proceedings of Fifth IEEE International Conference on Automatic Face Gesture Recognition*. IEEE, 2002, pp. 155-162.

[9] Monrose, Fabian and Rubin, Aviel D. Keystroke dynamics as a biometric for authentication. *Future Generation computer systems*, Vol. 16, No 4, 2000, pp. 351-359.

[10] National Research Council, Whither Biometrics Committee, *et al. Biometric recognition: challenges and opportunities*. National Academies Press, 2010.

[11] Roethenbaugh, Gary. An Introduction to Biometrics and General History. *Biometrics Explained, Section*, Vol. 1, 1998.

[12] Jain, Anil K., Bolle, Ruud, and Pankanti, Sharath (ed.). *Biometrics: personal identification in networked society*. Springer Science & Business Media, 2006.

[13] Wayman, James, Jain, Anil, Maltoni, Davide, *et al.* An introduction to biometric authentication systems. In : *Biometric Systems*. Springer, London, 2005. pp. 1-20.

[14] Flynn, Patrick J., Jain, Anil K., and Ross, Arun A. (ed.). *Handbook of biometrics*. Springer, 2008.

[15] Campbell, Joseph P. Speaker recognition: A tutorial. *Proceedings of the IEEE*, Vol. 85, No 9, 1997, pp. 1437-1462.

[16] Chen, Hui and Bhanu, Bir. Human ear recognition in 3D. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No 4, 2007, pp. 718-737.

[17] Ding, Yuhang, Zhuang, Dayan, and Wang, Kejun. A study of hand vein recognition method. In : *IEEE International Conference Mechatronics and Automation, 2005*. IEEE, 2005, pp. 2106-2110.

[18] Wayman, James L., Jain, Anil K., Maltoni, Davide, *et al.*(ed.). *Biometric systems: Technology, design and performance evaluation*. Springer Science & Business Media, 2005.

[19] Jain, Anil K., Ross, Arun, Prabhakar, Salil, *et al.* An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, Vol. 14, No 1, 2004.

[20] Idrus, Syed Zulkarnain Syed, Cherrier, Estelle, Rosenberger, Christophe, *et al.* Soft biometrics for keystroke dynamics. In : *International Conference Image Analysis and Recognition*. Springer, Berlin, Heidelberg, 2013. pp. 11-18.

[21] Babler, W. Embryologic development of epidermal ridges and their configurations. *Birth defects original article series*, Vol. 27, No 2, 1991, pp. 95-112.

[22] Gaensslen, Robert E., Ramotowski, Robert, and Lee, Henry C. *Advances in fingerprint technology*. CRC press, 2001.

[23] Ross, Arun. Iris recognition: The path forward. *Computer*, Vol. 43, No 2, 2010, pp. 30-35.

[24] Lim, Shinyoung, Lee, Kwanyong, Byeon, Okhwan, *et al.*Efficient iris recognition through improvement of feature vector and classifier. *ETRI journal*, Vol. 23, No 2, 2001, pp. 61-70.

[25] Davson, Hugh. *Physiology of the Eye*. Macmillan International Higher Education, 1990.

[26] Daugman, John G. *Fast focus assessment system and method for imaging*. U.S. Patent No 6,753,919, 22 juin 2004.

[27] Phillips, P. Jonathon, Grother, Patrick, Micheals, Ross J., *et al.* FRVT 2002: Overview and summary, 2003.

[28] Rabiner, Lawrence R. and Schafer, Ronald W. *Digital processing of speech signals*. Englewood Cliffs, NJ : Prentice-hall, 1978.

[29] Labov, William. *Sociolinguistic patterns*. University of Pennsylvania Press, 1972.

[30] Scherer, Klaus R. Vocal Affect Expression: A review and a model for future research. *Psychological bulletin*, Vol. 99, No 2, 1986, pp. 143.

[31] Boite, René. *Traitement de la parole*. PPUR presses polytechniques, 2000.

[32] Ross, Arun, Jain, Anil, and Pankati, S. A prototype hand geometry-based verification system. In : *Proceedings of 2nd conference on audio and video based biometric person authentication*. 1999, pp. 166-171.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[33] Guo, Jing-Ming, Hsia, Chih-Hsien, Liu, Yun-Fu, *et al.* Contact-free hand geometry-based identification system. *Expert Systems with Applications*, Vol. 39, No 14, 2012, pp. 11728-11736.

[34] Luque-Baena, Rafael M., Elizondo, David, López-Rubio, Ezequiel, *et al.* Assessment of geometric features for individual identification and verification in biometric hand systems. *Expert systems with applications*, Vol. 40, No 9, 2013, pp. 3580-3594.

[35] Goldberg, David E. and Holland, John H. Genetic algorithms and machine learning. *Machine learning*, Vol. 3, No 2, 1988, pp. 95-99.

[36] Kumar, Ajay and Zhang, David. Personal recognition using hand shape and texture. *IEEE Transactions on image processing*, Vol. 15, No 8, 2006, pp. 2454-2461.

[37] Oden, Cenker, Ercil, Aytul, and Buke, Burak. Combining implicit polynomials and geometric features for hand recognition. *Pattern Recognition Letters*, Vol. 24, No 13, 2003, pp. 2145-2152.

[38] Shu, Wei and Zhang, David. Palmprint verification: an implementation of biometric technology. In : *Proceedings. Fourteenth International Conference on Pattern Recognition (Cat. No. 98EX170)*. IEEE, 1998. pp. 219-221.

[39] Hill, Robert B. *Apparatus and method for identifying individuals through their retinal vasculature patterns*. U.S. Patent No 4,109,237, 22 août 1978.

[40] Li, Stan Z. *Encyclopedia of Biometrics: I-Z*. Springer Science & Business Media, 2009.

[41] Kumar, Ajay and Wu, Chenye. Automated human identification using ear imaging. *Pattern Recognition*, Vol. 45, No 3, 2012, pp. 956-968.

[42] Wang, Liang, Tan, Tieniu, Hu, Weiming, *et al.* Automatic gait recognition based on statistical shape analysis. *IEEE transactions on image processing*, Vol. 12, No 9, 2003, pp. 1120-1131.

[43] Nalwa, Vishvjit S. Automatic on-line signature verification. *Proceedings of the IEEE*, Vol. 85, No 2, 1997, pp. 215-239.

[44] Chibelushi, Claude C., Mason, John S., and Deravi, R. Integration of acoustic and visual speech for speaker recognition. In : *Third European Conference on Speech Communication and Technology*, 1993.

[45] Chang, Kyong, Bowyer, Kevin W., Sarkar, Sudeep, *et al.* Comparison and combination of ear and face images in appearance-based biometrics. *IEEE Transactions on pattern analysis and machine intelligence*, Vol. 25, No 9, 2003, pp. 1160-1165.

[46] Kumar, Ajay, Wong, David Cm, Shen, Helen C., *et al.* Personal verification using palmprint and hand geometry biometric. In : *International Conference on Audio-and Video-Based Biometric Person Authentication*. Springer, Berlin, Heidelberg, 2003, pp. 668-678.

[47] Uludag, Umut, Pankanti, Sharath, Prabhakar, Salil, *et al.* Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE*, Vol. 92, No 6, 2004, pp. 948-960.

[48] Jain, Anil K., Flynn, Patrick, and Ross, Arun A. (ed.). *Handbook of biometrics*. Springer Science & Business Media, 2007.

[49] International Biometric Group (Ibg), Findbiometrics, Global Identity Management, https://findbiometrics.com/

[50] Prabhakar, Salil, Kittler, Josef, Maltoni, Davide, *et al.* Introduction to the special issue on biometrics: Progress and directions. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 29, No 4, 2007, pp. 513-516.

[51] Zou, Xuan, Kittler, Josef, and Messer, Kieron. Illumination invariant face recognition: A survey. In : *2007 first IEEE international conference on biometrics: theory, applications, and systems*. IEEE, 2007, pp. 1-8.

[52] Cao, Kaidi, Rong, Yu, Li, Cheng, *et al.* Pose-robust face recognition via deep residual equivariant mapping. In : *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*. 2018. pp. 5187-5196.

[53] Stern, Guillaume, Fu, Zehua, and Ardabilian, Mohsen. 3D Face Analysis for Healthcare. In : *Biometrics under Biomedical Considerations*. Springer, Singapore, 2019, pp. 147-160.

[54] Alqahtani, Faleh, Banks, Jasmine, Chandran, Vinod, *et al.* Detection and tracking of faces in 3D using a stereo camera arrangements. *International Journal of Machine Learning and Computing*, Vol. 9, No 1, 2019, pp. 35-43.

Nguyen, Anh, Yosinski, Jason, Et Clune, Jeff. Multifaceted feature visualization: Uncovering the different types of features learned by each neuron in deep neural networks. *arXiv preprint arXiv:1602.03616*, 2016.