Journal of Biometrics & Biostatistics
ISSN: 2155-6180

Kalyani, J Biom Biostat 2017, 8:5
DOI: 10.4172/2155-6180.1000371

Review Article Open Access

Various Biometric Authentication Techniques: A Review

Kalyani CH*

Department of ECE, KITS, Warangal, India

Abstract

Biometrics refers to metrics related to human characteristics. Biometrics is a realistic authentication used as a form of identification and access control. It is also used to identify individuals in groups that are under surveillance. Biometric identifiers are then measurable, distinctive characteristics used to label and describe individuals. Biometric authenticators are frequently labeled as behavioral as well as physiological characteristics. Physiological characteristics are related to the shape of the body. By utilizing biometrics a man could be distinguished in view of "who she/he is" instead of "what she/he has" (card, token, scratch) or "what she/he knows" (secret key, PIN).In this paper, the fundamental concentrate is on the different biometrics and their applications.

Keywords: Biometrics; Facial recognition; Fingerprints; Voice recognition; Retina scans; Palm prints; Keystrokes

Introduction

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic [1]. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the transaction fraud raises and level of security infringes, the requirement for highly secure identification and personal verification technologies are becoming apparent. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The necessity for biometrics can be found in, state and local governments, federal, in the military, and in commercial applications. Enterprise-wide network security infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security [2]. Trust in these electronic transactions is essential to the healthy growth of the global economy. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics is set to pervade nearly all aspects of the economy and our daily lives. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming socially acceptable and inexpensive.

Overview: Evolution of biometrics

Biometrics is a branch which is very much used since 14th century in china by collecting the fingerprints of the merchants and their offspring to identify them form others [3].

At first in the 19th century, a human identification technique named Bertillionage is developed by an Anthropologist called *Alphonse bertillion* by collecting the human body measurements to recognize them. He had realized the human physical features by placing them in two categories named as changing features like length of hair, weight, etc., and the unchanged human physical features like length of fingers. But this method is vanished quickly because of the false recognition of persons as it is eminent that more than one person may have same body measurements [4,5]. Later, Richard Edward Henry from Scotland Yard developed a novel technique named fingerprinting.

- In 1935 the proposal of retinal identification was introduced by Dr. Carleton Simon and Dr. Isadore Goldstein.
- In 1981 the first commercial retina scanning system had been made obtainable.
- In 1993 John Daugman introduced iris recognition at Cambridge University.

In 2001, Biometrics Automated Toolset (BAT) was introduced in Kosovo, which provide a tangible recognition means.

Today, biometric had developed as a self-determining field of study with accurate technologies for establishing individual identities [6].

Types of Biometrics

Biometric devices are many types, but majorly there are five types of biometrics security which are commonly used. Biometrics is basically the recognition of human being personality that are unique to each human, which includes facial recognition, fingerprints, voice recognition, retina scans, palm prints, and more has shown in Figure 1. Biometric technology are used to keep the devices safe in the best way to ensure that people stay out of their valuable assets and information, and will find that using any one of these five biometrics security, devices is a great way to keep things safe [7].

Retina scanner

A retinal scan is a biometric approach that makes use of the unique patterns on someone's retina to discover them. The human retina is a thin tissue composed of neural cells that is located within the posterior

***Corresponding author:** Kalyani CH, Assistant Professor, Department of ECE, KITS, Warangal, India, Tel: +91-0870-2564888; E-mail: kalyanichinegaram@gmail.com

Received September 04, 2017; **Accepted** September 28, 2017; **Published** October 11, 2017

Citation: Kalyani CH (2017) Various Biometric Authentication Techniques: A Review. J Biom Biostat 8: 371. doi: 10.4172/2155-6180.1000371

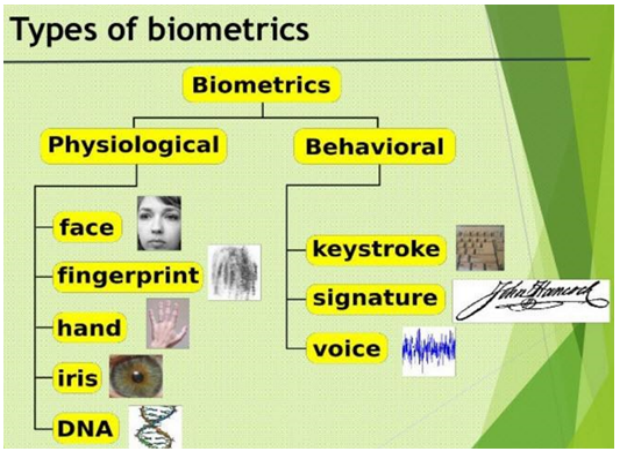

Figure 1: Types of biometrics.

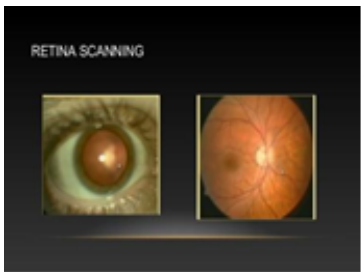

Figure 2: Retina scanning.

part of the eye as shown in Figure 2. Due to the complex shape of the capillaries that deliver the retina with blood, all and sundry's retina is unique. The network of blood vessels within the retina is so complicated that even identical twins do not proportion a comparable sample. Even though retinal styles can be altered in instance of diabetes, Glaucoma or retinal degenerative disorders, the retina typically remains unaffected from birth till dying. Due to its unique and unchanging nature, the retina seems to be the maximum precise and dependable biometric [8]. Those experiment the unique biometric pattern in every body's iris, and suit it towards a positive range of particular identifying marks that set every person apart from all people else. Advantages of using Retinal experiment consist of low prevalence of false positives, extraordinarily low (nearly 0%) fake bad charges, highly dependable because no humans have the same retinal sample, rapid results: identity of the issue is verified right away [9,10]. dangers include measurement accuracy can be stricken by a sickness such as cataracts, measurement accuracy also can be affected by severe astigmatism, canning technique is perceived by some as invasive, no longer very consumer friendly, difficulty being Scanned have to be close to the dig cam optics, high equipment cost.

Iris scanning

Iris recognition uses digital camera technology, with slight infrared illumination lowering specular reflection from the convex cornea, to create photographs of the detail-wealthy, elaborate systems of the iris as shown in Figure 3. Converted into digital templates, those snap shots offer mathematical representations of the iris that yield unambiguous wonderful identity of an individual. Iris reputation efficiency is not often impeded by using glasses or contact lenses. Iris technology has

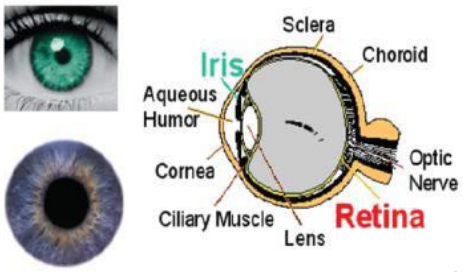

Figure 3: Iris sample.

the smallest outlier (folks that cannot use/enroll) group of all biometric technologies [11]. Because of its pace of contrast, iris reputation is the handiest biometric technology nicely-perfect for one-to-many identity. Advantage of iris reputation is its balance, or template sturdiness, a single enrollment can closing an entire life. There are few benefits of the use of iris as biometric identification: it's far an inner organ this is properly included against damage and wear by a rather obvious and touchy membrane (the cornea) [12]. This distinguishes it from fingerprints, which may be tough to recognize after years of certain styles of manual labor. The iris is normally flat, and its geometric configuration is handiest managed by complementary muscle groups that manage the diameter of the student. This makes the iris shape far greater predictable than, for example, that of the face. The iris has a pleasant texture that like fingerprints is determined randomly at some stage in embryonic gestation. Even genetically same individuals have absolutely independent iris textures, while DNA (genetic "fingerprinting") isn't unique for the about 0.2% of the human population who've a genetically same twin. An iris experiment is similar to taking a photograph and can be achieved from about 10 cm to 3 m away. There is no need for the person to be diagnosed to touch any equipment that has currently been touched by using a stranger, thereby getting rid of an objection that has been raised in some cultures in opposition to fingerprint scanners, in which a finger has to the touch a surface, or retinal scanning, where the eye can be delivered very close to a lens (like looking into a microscope lens).Even as there are a few clinical and surgical strategies that could affect the coloration and normal form of the iris, the first-rate texture stays remarkably stable over many years. Some iris identifications have succeeded over duration of approximately 30 years [13-15]. However Iris scanning is a quite new era and is incompatible with the very substantial funding that the law enforcement and immigration government of a few international locations have already made into fingerprint popularity.

Finger print scanner

Fingerprints are the graphical glide-like ridges gift on human palms. Finger ridge configurations do no longer exchange for the duration of the life of a person besides due to accidents including bruises and cuts on the fingertips. This belongings makes fingerprints a totally attractive biometric identifier. Fingerprint-based (Figure 4a) totally private identification has been used for a very long time. As a long way as fee is going, the fingerprint scanning is on the lower stop of the dimensions. The most inexpensive fingerprint scanners are those that best scan the actual print, though the dearer ones really experiment the presence of blood in the fingerprint, the scale and shape of the thumb, and plenty of different features as shown in Figure 4b. Those costlier structures in reality capture a 3D photo of the fingerprint, thereby making it a great deal more difficult for the fingerprint to be counterfeited.

Figure 4a: Finger tip.

Figure 4b: Fingerprint matching mechanism.

DNA

Not long ago Russian show business was full of rumors that one of the popular Russian singers has two fathers and each father tried his best to influence on the son. Special programmers were created and the situation was discussed but only one thing was interested to public: who was the real father of the singer. The singer himself was confused. In one of the programs the singer and both of his father's decide to take DNA test as shown in Figure 5.

Facial biometrics

Every individual around the globe has a distinctly unique face, even two twins that the human eye can't differentiate. It might be something as little as the slightly unique placing of the eyebrows, the width of the eyes, or the breadth of the nose. There are sure markers that enable these biometric acknowledgment scanners to in a split second recognize the uniqueness of every individual examining their facial elements, in this manner empowering the gadget to guarantee that lone the single individual with the right bone structure and highlight situation can obtain entrance. PCs have contributed in the programmed acknowledgment of people utilizing the incontestable facial qualities which prompted wide importance of the Face Recognition System (FRS) as shown in Figure 6.

Voice recognition

Each person in the world has a unique voice pattern as shown in Figure 7, even though the changes are slight and hardly noticeable to the human ear. On the other hand with uncommon voice recognition programming, those moment contrasts in every individual's voice can be noted, experienced and validated to enable the access to the individual that has quality pitch which is a correct one, and at the same time voice level also. Surprisingly it can be effective at differentiating two people who have almost identical voice patterns. In forensic applications, it is common to first perform a speaker identification process to create a list

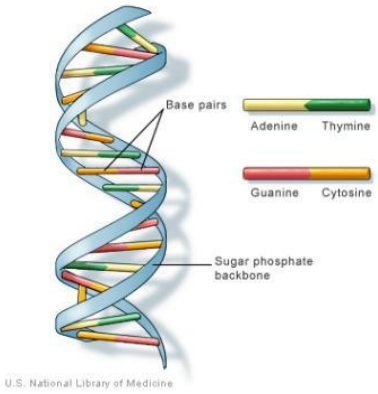

Figure 5: Structure of DNA.

Figure 6: Automatic face recognition system.

Figure 7: Sample voice clip as shown in sound editor.

of "best matches" and then perform a series of verification processes to conclude a conclusive match. Feeding the wrong voice cannot always be avoided in voice recognition as well as the voice capturing machine should be near to the user.

Key stroke

Keystroke as shown in Figure 8, it is the behavior of the human. It means to say that the different humans have the different techniques of pressing keys on such basis the identification takes place. It is 100% software-based, requiring no sensor more than a home computer.

Hand/Palm print patterns

By placing your hand on a scanner, you not only have a unique fingerprint pattern, but the size and shape of your entire hand is also very unique as shown in Figure 9. It differs to a unique finger impression in that it likewise contains other data, for example, touch, indents

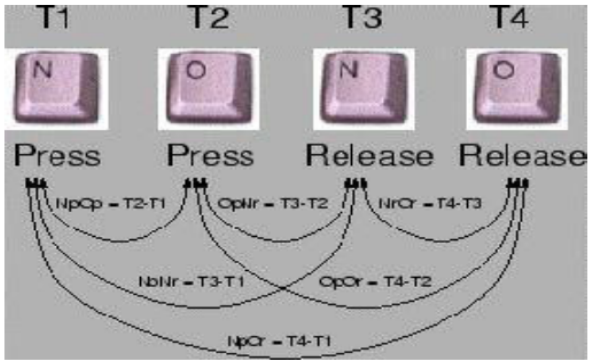

Figure 8: Keystroke.

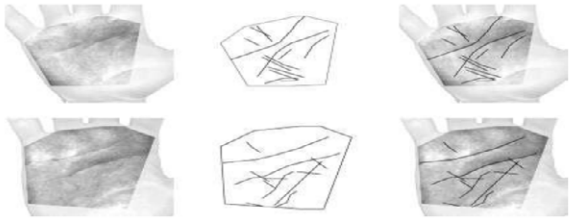

Figure 9: Hand/Palm-print and hand/palm-print features.

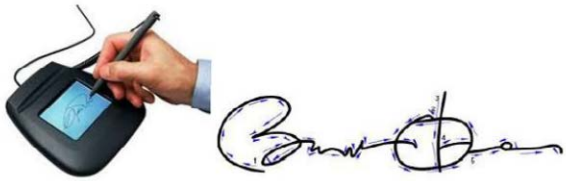

Figure 10: Signature scanning.

and symbols which can be utilized when contrasting one palm with another. Hand prints can be used for criminal, forensic or commercial applications [16]. The main difficulty of hand print is that the print changes with time depending on the type of work the person is doing for an extended duration of time.

Signature scanning

Another behavioral biometric is a signature at which the data can be extracted by the signature of that particular person as shown in Figure 10. The responsibility of a signature is exclusively not only to provide evidence of the identity of the constricting gathering but moderately to provide evidence of deliberation and educated consent signatures can be easily inaccurate With advanced signature capturing devices. Signature recognition correctly became easier and more efficient.

Comparison between Different Biometrics Used

The following table compares some of the biometric systems used lately, from the point of view of accuracy, cost, and devices required and social acceptability (Figure 11). We can see that fingerprint has a good balance about everything from Table 1.

Conclusion

A Biometric identification or else biometrics, refers to the consistent identification of an individual based on his/her physiological

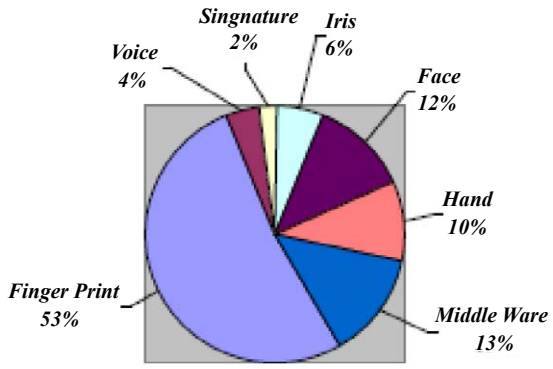

Figure 11: Biometric market report.

Biometrics	Uniqueness	performance	Measurability
Face Recognition	High	Medium	High
Iris Recognition	High	High	Medium
ECG Recognition	High	High	Medium
Voice Recognition	Low	Low	Medium
Palm Recognition	Medium	Medium	High

Table 1: Comparison between different biometrics used.

(e.g., face, fingerprint, hand, iris, DNA) or behavioral (e.g., keystroke, signature, voice) individuality. This technique of identification offers several compensations over traditional methods involving ID cards or PIN numbers for various reasons. Hence these systems are proved highly confidential computer-based security systems. Each and every biometric system is useful and selection of particular biometric device depends upon the application area, i.e. where we are going to deployed biometric technology. Mainly it depends on the quantity of people, which will perceive him or her and also conditions. In the event of restricted people, we can utilize a biometric technology as less time taken yet more secured than other biometric technology utilized where unlimited people are recognized fastly but little bit accuracy. As my comparison demonstrate various contracts in view of various perspectives so one can easily pick the biometric technology for deployment in real time.

References

1. Alsaadi IM (2015) Physiological biometric authentication systems, advantages disadvantages and future development: A review. Int J Sci Technol Res 12: 285-289.
2. Kaur G, Singh G, Kumar V (2014) A review on biometric recognition. International Journal of Bio-Science and Bio-Technology 4: 69-76.
3. Kong A, Zhang D, Kamel M (2009) A survey of palmprint recognition. Pattern Recognition 7: 1408-1418.
4. Battaglia F, Iannizzotto G, Bello L (2014) A biometric authentication system based on face recognition and rfid tags. Mondo Digitale 49: 340-346.
5. Bowyer W, Hollingsworth KP, Flynn PJ (2016) A survey of iris biometrics research: 2008-2010. Handbook of iris recognition. Springer, London.
6. Jitendra J, Singh BK, Ali MI (2014) Voice Identification Secure System by Statistical Model of Speech Signal Using Normalization Technique. International Journal of Engineering.
7. Srivastava HA (2013) Comparison Based Study on Biometrics for Human Recognition. IOSR Journal of Computer Engineering (IOSR-JCE) 15: 22-29.
8. Duarte T (2016) Biometric access control systems: A review on technologies to improve their efficiency. Power Electronics and Motion Control Conference (PEMC).

9. Debnath B (2009) Biometric authentication: A review. International Journal of u-and e-Service, Science and Technology 3: 13-28.

10. Unar JA, Chaw Seng W, Abbasi A (2014) A review of biometric technology along with trends and prospects. Pattern recognition 47: 2673-2688.

11. Bowyer, Kevin W, Hollingsworth KP, Flynn PJ (2016) A survey of iris biometrics research: 2008-2010. Handbook of iris recognition. Springer, London 23-61.

12. Surekha B, Jayant KN, ViswanadhaRaju S, Dey N (2017) Attendance Recognition Algorithm, Intelligent techniques in signal processing for multimedia security.

13. Dharavath K, Talukdar FA, Laskar RH, Dey N (2016) Face Recognition under Dry and Wet Face Conditions, Intelligent Techniques in Signal Processing for Multimedia Security. Publisher: Springer SCI series.

14. Trivedi JA (2014) Voice identification system using neuro-fuzzy approach. International Journal of Advanced Research in Computer Science and Technology (IJARCST).

15. Siddhesh A, Bhagtani R, Chheda H (2005) Biometrics: A further echelon of security. UAE International Conference on Biological and Medical Physics.

16. Shradha T, Chourasia NI, Chourasia VS (2015) A review of advancements in biometric systems. International Journal of Innovative Research in Advanced Engineering 2: 187-204.