Innovation
2020; 1(1): 1-5
http://www.sciencepublishinggroup.com/j/innov
doi: 10.11648/j.innov.20200101.11

Overview of Technologies and Fingerprint Scanner Used for Biometric Capturing

Ezeonyi Nnaemeka Uchenna[1], Okonkwo Obikwelu Raphael[1], Alumona Theophilus Leonard[2]

[1]Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria

[2]Department of Electronic and Computer Engineering, Nnamdi Azikiwe University, Awka, Nigeria

Email address:
nu.ezeonyi@gmail.com (E. N. Uchenna), ro.okonkwo@unizik.edu.ng (O. O. Raphael), tl.alumona@unizik.edu.ng (A. T. Leonard)

To cite this article:
Ezeonyi Nnaemeka Uchenna, Okonkwo Obikwelu Raphael, Alumona Theophilus Leonard. Overview of Technologies and Fingerprint Scanner Used for Biometric Capturing. *Innovation*. Vol. 1, No. 1, 2020, pp. 1-5. doi: 10.11648/j.innov.20200101.11

Received: September 12, 2020; **Accepted**: October 16, 2020; **Published**: October 21, 2020

Abstract: Human beings recognize each other in various characteristics for ages. This research is based on general overview of biometrics system and the technology behind using fingerprint scanner used for biometric capturing. Biometrics is the automated methods of verifying the identity of a person based on physiological or behavioral characteristics. In this study, its development as well as its basic structure is discussed in details. This study also talks about fingerprint scanner and how it can be used for capturing information for easy verification and identification of humans to promote security in our society. Also, stages involved in fingerprint scanner detection are well elaborated in this research and various applications of fingerprint scanner in our society. In general, the characteristics of each person differs from one another, and that is why fingerprint scanner which is one of the medium of capturing data in biometric system makes verification and identification of individuals more reliable and accurate than the traditional methods of verifying and identifying information.

Keywords: Biometric, Fingerprint, Scanner, Verification and Identification

1. Background of the work

Biometrics is the technical term or body measurements and calculations. It refers to metrics related to human characteristics. Biometrics is automated methods of identifying a person based on behavioral characteristics. Biometrics authentication is used as a form of identification or access control. [1]. It is also used to verify and identify individuals in groups that under surveillance. [3] Biometrics identifiers are the distinctive, measurable characteristics used to label and describe individuals. [4]

Information security in individuals is based to ensure the integrity, confidentiality and availability of information. Biometric system goes a very long way to achieve information nowadays. Biometric data is personal private information which uniquely and permanently associated with a person and cannot be replaced with any sort of keys or passwords. One problem of biometric data of a user is that when the data is lost, the information will be lost forever, leading to a huge financial loss or problem. This is the reason why one needs to protect the biometric data of one collected to any form of losses.

2. Brief Historical Development of Biometrics

One of the oldest and most basic examples of a characteristic that is used for recognition by humans is the face. Since the beginning of civilization, humans have used faces to identify known (familiar) and unknown (unfamiliar) individuals. This simple task became increasingly more challenging as populations increased and as more convenient methods of travel introduced many new individuals into- once small communities. The concept of human-to-human recognition is also seen in behavioral-predominant biometrics such as speaker and gait recognition. Individuals use these characteristics, somewhat unconsciously, to recognize known individuals on a day-to-day basis [2]. By the mid-1800s, with the rapid growth of cities due to the industrial revolution and more productive farming, there was a formally recognized need to identify people. Merchants and authorities were faced with increasingly larger and more mobile populations and could no longer rely solely on their own experiences and local

knowledge. Influenced by the writings of Jeremy Bentham and other Utilitarian thinkers, the courts of this period began to codify concepts of justice that endure with us to this day. Most notably, justice systems sought to treat first time offenders more leniently and repeat offenders more harshly. This created a need for a formal system that recorded offenses along with measured identity traits of the offender. The first of two approaches was the Bertillon system of measuring various body dimensions, which originated in France. These measurements were written on cards that could be sorted by height, arm length or any other parameter. This field was called anthropometries.

Recently, most phones come with fingerprint to be able to verify and identify the owner of the item. Even with the increasing rate of development, the possibilities of biometric identification and authentication are far from being exhausted or extinct. As biometrics research continues to progress, we can see it clearly being merged with artificial intelligence. Therefore, with time, biometrics can be made or created in a seamless and frictionless identification and authentication experience. [2]

3. Basic Structure of a Biometric System

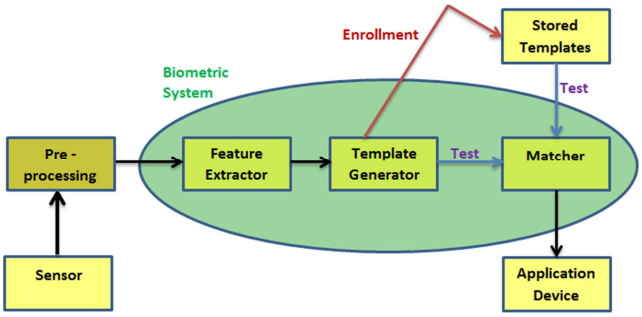

Figure 1. *Basic Structure of a Biometric System [1].*

The above diagram illustrates the basic structure of a biometric system. The bock diagram shows that there are modes of a biometric system which are verification/authentication and identification.

In the first case which is the verification component, the system performs a one-to-one comparison of a captured data against the specific data already stored in a biometric system or database in order to verify the information of the individual stored in the system for proper checking and matching. [5] There are steps involved under this category. They include:

a) Here, the users' data are collected and stored in the database of the system.
b) The data collected are checked and matched with reference to the original one collected, as to check the genuine owners or impostors.
c) This step involves testing the data collected.

In the second case which is the identification component where the system performs a one-to-many comparison of the captured data against the biometric data already stored in the database of a biometric system in an attempt to establish the identity of an unknown individual. The system will complete a given task if the comparison of the biometric sample collected matches with the sample already stored in the database of a biometric system. [5]

4. Types of Biometrics

There are different types of biometrics. [8] They include:

1) Fingerprints Biometrics: This is a type of biometrics where patterns of friction ridges and valleys on an individual's finger tips are unique to that individual. For many years now, law enforcement agencies having been identifying and tracking criminals through this medium of biometrics which makes their work easier and safer. Fingerprints are unique for each finger of a person in the entire universe including that of identical twins. One can purchase fingerprint detecting devices in any part of the word and at a minimal cost.
2) Face Recognition Biometrics: this is a type of biometrics where verification and identification of a person is through their facial image which can be done in a different ways. Using a wide assortment of cameras, the visible light systems extract features from the captured images that do not change over time while avoiding superficial features such as facial expressions or hair.
3) Speaker Recognition: this is a type of biometrics that uses features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and earned behavioral patterns. There are many various technologies used to process and store voice prints which include: hidden Markova models, pattern matching algorithms, neural networks, matrix representation and decision trees.
4) Signature Verification Biometrics: this is a type of biometrics that uses the dynamic analysis of a signature to authenticate a person. This technology is based on measuring speed, pressure and angle used by the person when a signature is produced.
5) Hand and Finger Geometry Biometrics: This is a type of biometrics where to achieve persona authentication, a system may measure either physical characteristics of hands or fingers. These characteristics or features include length, width, thickness, and surface area of the hand.
6) Iris Recognition Biometrics: this is another type of biometrics that uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought and are obtained through a video-based image acquisition system. This technology works very well in verification and identification modes of biometric system.

From the above analysis, this study has been given the analysis of a biometric system. Further study will be on fingerprint scanner as a means of verification and identification of a person with regards to biometric system.

4.1. Fingerprint Scanner as a Means of Biometric Capturing

A fingerprint scanner is a type of technology that identifies and authenticates the fingerprints of an individual in order to grant or deny access to a computer system or a physical facility. [9] It is a type of biometric system that uses the combination of hardware and software techniques to identify and very the fingerprints of an individual. They are used in paramilitary, law enforcement agencies, industries, schools, etc. for the purpose of efficient security system. This research made us understand that every individual has a unique pattern of finger which cannot be changed or removed; and these marks are called the fingerprint. As the computer become the subject rapid development, the fingerprint system also evolved and an automated research and the use of computers.

4.2. Types of Fingerprint Scanner Used for Biometric Capturing

Fingerprint scanner works by capturing the pattern of ridges and valleys on a finger. [9] The information captured is the processed by the matching software to compare and determine whether the information collected matches with the data in the database of the system. A successful match means that the information has been verified and identified. This can now lead us to various ways by which fingerprint of different individuals can be captured in a biometric system and that depends on the type of scanner being used. They include:

1) Optical sensor: this is type of scanner that basically makes a photocopy of the finger to produce a digital image. Many PC-connected fingerprint scanners use optical sensors.
2) Capacitive Sensor: this is a type of scanner that uses electricity to determine the fingerprint patterns this works by if a finger rest on the touch-capacitive surface, the device measures the charge; ridges exhibit a change in capacitance, while valleys produce no change. Then the sensor uses the data collected to accurately map out the prints. Most smart phones with finger print scanners uses this type of scanner.
3) Ultrasonic Sensor: this is a type of scanner that uses echolocation to find and identify objects. Ultrasonic scanners works through sound waves. They are currently being prototyped and tested for use in many mobile devices.

4.3. Stages Involved in Fingerprint Scanner Detection

Fingerprints are made of series of ridges and furrows on the surface of the finger and have a core around which patterns like arches which is curved, to ensure that each print is unique. [6] An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc; and then exit the other side of the finger. The ridges and furrows are characterized by irregularities known as “minutiae”, the distinctive characteristic upon which finger scanning technologies are based.

Minutiae points are local ridge characteristics that occur at either a ridge ending or bifurcation. The ridge ending is the point at which a ridge terminates, while ridge bifurcations are pints where a single ridge spits into two. Minutiae and patterns are very important in the analysis of fingerprints, since no two fingers have been shown to be identical.

There are five stages involved in finger-scan verification and identification of information in a biometric system. They include:

1) Fingerprint image acquisition.
2) Image processing.
3) Locating distinctive features.
4) Template creation.
5) Template matching.

A fingerprint sensor takes a snap shot of the user’s unique pattern of finger, which is then saved I fingerprint database system. A fingerprint enhancement algorithm is included in the minutiae extraction module to ensure that the performance of the system is not affected by the variations in the quality of fingerprint images.

4.4. Applications of Fingerprint Scanner Used for Biometric Capturing

There are various ways in which fingerprint scanner used for biometric capturing can be applied. [3] They include:

1) Fingerprint scanner can be integrated into a smartphone device without any challenges or deformity to the area concerned. Since the features of fingerprint sensors comprise of ultra-thinness, robustness and conformability, they offer alternative integration approaches. This is done by pacing the flexible fingerprint sensor under the display to enable more elegant mobile phone designs, thereby making it more intuitive for the user to authenticate them with a single hand while holding the phone.
2) With the rapid growth in the use of wearable devices, fingerprint scanners can be incorporated in these electronic devices that can easily be conformed with the device to reduce the case of theft and improve the security aspect.
3) One of the criteria when selecting a fingerprint authentication system for border control is the speed of acquisition of the Person’s fingerprints. So fingerprint scanner helps law enforcement agencies in terms of border control for efficient security against criminal activities. This is achieved by having the ten fingerprints of every individual in case of any problem.
4) Fingerprint scanner can be incorporated into smartcard during the design to help in the ease verification and identification of the genuine owners in case of any loss or problem. It is used in banking industry for more security purposes and to promote private transactions for every single customer banking with them.
5) Integrating biometric fingerprint readers into POS

devices allows firms to efficiently manage their retail system by implementing biometrics on the staff login for more time-efficient in the business and security for unaccounted transactions.

5. Sources of Uncertainty and Variations in Fingerprint-Scanned Biometrics

There are numerous levels of uncertainty and variation in fingerprint-scanned biometric systems [12], including the following:

1) Age: People in the 18-25 age range give consistently good prints, while older individuals have more borderline print quality.
2) Gender: Men give higher quality print than women.
3) Height of the Sensor: The placement of scanner with respect to counter height effects fingerprints image quality. Capturing individual thumbs yields higher quality images than capturing simultaneous thumbs irrespective of height. The thumbs are more sensitive to height than the slaps. The left slap is more sensitive than the right slap. The right index finger is the only finger that is not sensitive to height.

6. Security and Accuracy of Fingerprint-Based Biometrics

In [13] 2019, Yang gives a comprehensive review of security and recognition accuracy in Fingerprint-Based Biometrics. In regards to security, he analyzed two categories of attacks:

1) Attacks to User Interface
2) Attacks to Template Database

6.1. Attacks on User Interface and Countermeasures

The User Interface (the sensor module) can be attacked by 'spoofing'. Since biometric traits are not secret, an adversary can intrude a fake trait into the system (e.g., artificial fingerprint, face mask) to spoof the biometric system if the system is unable to differentiate between a fake biometric trait and a genuine one. The countermeasure for spoofing is a term known as 'Liveliness Detection' [13].

Among these approaches mentioned below, there are many approaches for Fingerprint Liveliness Detection:

1) Tan & Suckers Approach [14]
   a. Uses a Wavelength Transform technique
   b. Uses Capacitive DC, Optical and Electro-optical sensors
2) Galbally et al Approach [15]
   a. Uses Fingerprint Parameterization Technique
   b. Uses Optical sensors

6.2. Attacks on Template Database and Countermeasures

Biometric traits are irrevocable or cannot be reset. Therefore security concerns could arise if database contains raw, unprotected template data [13]. An adversary can hack the template data in the database, thus gaining unauthorized access to a biometric system. To protect raw template data, two techniques may be employed:

1) Cancelable Biometrics

The concept of cancelable biometrics is that at the enrollment stage, the original template data is transformed into a different version by using a non-invertible transformation function. In the verification stage, query data are applied the same non-invertible transformation. In the transformed domain, using the transformed template and query data, matching is conducted [16].

2) Biometric Cryptosystems

A biometric cryptosystem combines biometrics with a cryptographic key and merges the advantages of both biometrics and cryptosystems [13].

7. Conclusion

In conclusion, there are different kinds of biometric system available these days. Proper design and implementation of any kind of biometric system will help to promote and increase security. There are also many conditions one needs to take into consideration when designing any secured biometric. Firstly, one should know that biometric is not in any form of secret affair. This implies that one needs to be extremely careful when designing the system so as to not generate any form of keys. Secondly, one should make sure that the input devices are perfectly working and the communication link should be well established and properly secured. Thirdly, the input devices and output devices should be properly checked and verified to ensure that they are in good working condition.

Fingerprint verification is one of the most reliable means of biometric authentication due to its universality, permanence, accuracy, readiness and distinctiveness. It has much number of benefits when compared with the rest of biometric system. They enjoy good acceptance rates in the general public, and have a positive image.

In T. Caldwell's research [10] 2013, Countries around the world employed biometric systems at the border. The said biometric system seeks to tighten up security at borders. We propose the Development of fingerprint biometrics verification and vetting management system to secure sensitive organization.

In the research of Adewole et al [11] 2014, Adewale proposed the development of fingerprint biometrics attendance systems for non- academic staff in tertiary institution. The system was developed to manage attendance record in an organization using the available computer development tools. The proposed application captures attendance electronically with the help of fingerprint recognition system. In Adawawe's work the emphasis was to reduce labour intensiveness associated with manual attendance record system.

References

[1] Jain, Anil K.; Ross, Arun (2008). "Introduction to Biometrics". In Jain, AK; Flynn; Ross, A (eds.). Handbook of Biometrics. Springer. pp. 1–22. ISBN 978-0-387-71040-2.

[2] Stephen M. (2018). History of Biometrics. Retrieved June, 2020 from https://www.biometricupdate.com/201802/history-of-biometrics.

[3] Flex Enable Ltd (2019). Biometrics: Flexible fingerprint sensors can be seamlessly integrated into products, bringing game-changing capabilities to biometric applications. Retrieved October 02, 2019 from https://www.flexenable.com/applications/biometrics/.

[4] Jain, A.; Hong, L.; Pankanti, S. (2000). Biometric Identification. Communications of the ACM, February 2000, Vol. 43 No. 2, Pages 90-98. 10.1145/328236.328110.

[5] Jain, A. K.; Ross, A. (2008). Introduction to Biometrics: in Jain, A. K.; Flynn; Ross, A. (eds). Handbook of Biometrics, Springer. Pp. 1-22. Retrieved August 30, 2019 from https://en.wikipedia.org/wiki/Biometrics.

[6] Matoni, D.; Jain, A. K.; Maio, D.; Prabhakar, S. (2004). Handbook of Fingerprints Recognition, Springer. Retrieved September 23, 2019 from https://www.ijcee.org/papers/239-E576.pdf.

[7] Mary, L. R.; Dushyant, K. (2010). Fingerprint Identification in Biometric Security Systems. International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, 173-8163.

[8] Sayani, Mondal (2019). A Seminar Report on Biometric Authentication. Department of ICT. Retrieved September 24, 2019 from https://pdfs.semantic scholar.org.

[9] Staney, Goodner (2019). Finger Scanners: what they are and why they are gaining in popularity. Retrieved September 24, 2019 from https://www.lifewire.com/understanding-finger-scanners-4150464.

[10] T. Caldwell, "Market report: border biometrics," *Biometric Technol. Today*, vol. 2015, no. 5, pp. 5–11, 2015.

[11] K. S. Adewole, S. O. Abdulsalam, R. S. Babatunde, T. M. Shittu, and M. O. Oloyede, "Development of Fingerprint Biometric Attendance System for Non-Academic Staff in a Tertiary Institution," vol. 5, no. 2, pp. 62–70, 2014.

[12] M. Theofanos, R. Micheals, J. Scholtz, E. Morse, & P. May, "Does Habituation Affect Fingerprint Quality?" Proceedings of ACM SIGCHI Annual Conference, Montreal, Quebec, Canada, 2006.

[13] W. Yang, S. Wang, J. Hu, G. Zheng and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review", *Symmetry*, vol. 11, no. 2, pp. 141, 2019.

[14] Tan, B.; Schuckers, S. Liveness detection for fingerprint scanners based on the statistics of wavelet signal processing. In Proceedings of the Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06), New York, NY, USA, 17–22 June 2006; p. 26.

[15] Galbally, J.; Alonso-Fernandez, F.; Fierrez, J.; Ortega-Garcia, J. A high performance fingerprint liveness detection method based on quality related features. Future Gener. Comput. Syst. 2012, 28, 311–321.

[16] Ratha, N. K.; Connell, J. H.; Bolle, R. M. Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. 2001, 40, 614–634.