Biostatistics and Biometrics
Open Access Journal
ISSN: 2573-2633

Juniper
PUBLISHERS
key to the Researchers

Review Article
Volume 6 Issue 2 - April 2018
DOI: 10.19080/BBOAJ.2018.06.555683

Biostat Biometrics Open Acc J

Biometrics Technologies for Secured Identification and Personal Verification

Eludire AA* and Adio EO

Department of Computer Science, Joseph Ayo Babalola University, Nigeria

Submission: January 29, 2018; **Published:** April 18, 2018

***Corresponding author:** Eludire AA, Department of Computer Science, Joseph Ayo Babalola University, Ikeji Arakeji, Osun State, Nigeria, Email: aaeludire@jabu.edu.ng

Abstract

Biometrics technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solution. It is an automated method of recognizing an individual based on physiological or behavioural characteristics such as fingerprints, distinctiveness in terms of characteristics, persistence characteristics, collectability characteristics and the ability of the method to deliver accurate results under varied environmental circumstances, acceptability, and circumvention. Biometrics technology is useful in the securing of electronic banking, financial and investment transactions, retail sales, social and health services, law enforcement. This paper examines a number of technologies for highly secured identification and personal verification.

Abbreviations: RFID: Radio Frequency Identification Devices; PIN: Personal Identification Number

Introduction

The applications of biometric technology have attracted increasing attention over the past years because of advances in computations and imaging, the identification of criminals reduced identity theft or forgery and enhanced security in electronic transaction and so forth. A number of technologies that are jointly used with automatic data capture to help machines identify objects or individuals for the purpose of increasing efficiency, reducing data entry errors are broadly referred to as Automatic identification or Auto ID. Biometrics is the use of Auto ID capability to recognize a person using different traits that can be captured or presented as data. In technical terms Biometrics is the automated technique of measuring the physical characteristics or personal trait of an individual 2 and comparing that characteristics or trait to a database for the purpose of recognizing that individual. In other words, biometrics can be used for verification as well as for identification. The verification is referred to as «one to one» matching while identification is known as «one-to-many» matching [1].

In using biometric verification two main individual features are employed: unique physiological trait or behavioural characteristics Physiological traits are stable physical characteristics with measurement that is essentially unalterable. Examples of physiological traits include individual's physical features such as fingerprint, retina, palm prints and iris patterns. Typical examples of behavioural characteristic include individual's voice, signature, or keystroke dynamics. It can be stated behavioural characteristics are easily influenced by both regulated actions and less regulated psychological factors. Because behavioural characteristics can change over time, the enrolled biometric reference template must be updated each time it is used. From the point of measurement reliability, greater accuracy and security is provided by biometrics based on physiological traits while behaviour-based biometrics can be less costly and less threatening to users. In any case, both techniques provide a significantly higher level of identification than passwords or cards alone. Biometric traits are unique to each individual; they can be used to prevent theft or fraud. Unlike a password or Personal Identification Number (PIN), a biometric trait cannot be forgotten, lost, or stolen. Today there are over 10,000 computer rooms, vaults, research labs, day care centres, blood banks, ATMs and military installations to which access is controlled using devices that scan an individual's unique physiological or behavioural characteristics. Biometric authentication technologies currently available commercially or under development include fingerprint, face recognition, keystroke dynamics, palm print, retinal scan, iris pattern, signature, and voice pattern [2].

Mode of operation

Biometrics has been used throughout the human history. Kings of Babylon have used handprints to identify different things such as engraving and the like of their own. Depending on the context, a biometric system may operate either in verification mode or identification mode [3]. Evangelista Purkinije from Czech had realized from had realized fingerprint to be unique form of identification in 1823. Fingerprint was first begun to be taken in ink on dactlograms by a by Scotland Yard and the concept of fingerprinting has been unique identifier to catch criminals that took off from the Scotland Yard. In 1970's electronic reader was being developed that led to today's technologies, Sandia National Laboratories has developed hand geometry readers in 1985 and the US government has purchased the readers.

Types of biometrics

The common biometrics based on physiological or behavioural characteristic that a normal person have are:

a. Face

b. Iris

c. Retina

d. Voice

e. Handprint

f. Fingerprint

g. Signature

h. DNA pattern

i. Sweat pores

Basically, the biometric method of identifying a person is preferred over traditional methods. As the use of computer in information technology areas is rapidly increasing, a secure restricted access to privacy or personal data must be obtained. The biometric technique can be used in many application area in order to prevent unauthorized access to use the privacy data such as ATMs, smart card, computer networks, time & attendance system, desktop PCs and workstation. Nowadays, there are several types of system developed with biometrics techniques for real-time identification. The face recognition and fingerprint matching are the most popular biometric techniques used to develop the system followed by hand geometric, iris, retina, and speech. The oldest biometric technique is the electronic fingerprint recognition which has undergone researches and development to extend its applications since its applications by law enforcement. There are two related matching techniques, which are minutiae-based, and correlation- based. What makes a fingerprint unique includes three main patterns; the loop the whorl and the arc using these patterns to match a fingerprint will generally locate a positive identification [4].

The finger print biometric machine is an automated digital version of the old ink and-paper method used for more than a century for identification, primarily by law enforcement agencies. The digital version involves electronically reading users finger print when placed on a platen where the details are mined by the biometric machine algorithm and a finger print pattern analysis is performed. A fingerprint is an impression of the friction ridges on all parts of the finger and pattern recognition algorithms rely on the features found in the impression. These are sometimes known as «epidermal ridges» which caused by the underlying interface between the dermal papillae of the dermis. Gorman identified three major areas where finger print biometrics are used to include: Law enforcement purposes, fraud prevention in entitlement programs, and physical and computer access generally referred to as large-scale Automated Finger Print Imaging Systems (AFIS). It is believed that no two people have identical fingerprint in world, so the fingerprint verification and identification is most popular way to verify the authenticity or identity of a person wherever the security is a problematic question. The reason for popularity of fingerprint technique is the uniqueness of a person arising from his behaviour and personal characteristics which indicates that each and every fingerprint is unique, different from one other.

Finger print recognition is probably the most widely used and well-known biometric that is very less vulnerable to errors in harsh errors environments. Though fingerprint biometrics is applicable in all fields of human endeavour, the finger print of some individuals working in certain industries such as chemical and agricultural are often badly affected making fingerprint mode of authentication problematic. However, to overcome this problem multimodal biometrics system can be applied and fingerprint recognition systems are still considered as the right applications under the right circumstances. Phillips and Martin concluded that finger print biometrics is one of the efficient, secure, cost effective, ease to use technologies for user authentication and according to their survey almost all drawbacks are addressed in fingerprint biometric system.

Verification and identification

Biometric systems operate in two basic modes: verification and identification [5,6]. Verification mode is used to validate a person against whom they claim to be and use one to one matches by comparing biometric data taken from an individual to a biometric template stored in a database. Verification relies on individuals enrolling on the system and registering their identity prior to providing biometric samples which is a massive administrative task when applied to international border control. Identification mode uses a one to many match and searches all the templates in a database to identify an individual therefore the system does not need the compliance of the data subject. The accuracy of biometric technology depends on the accuracy and number of records within the databases.

In the verification mode, the system validates a person's identity by comparing the captured biometric data with her own biometric template(s) stored system database. In such a system, an individual who desires to be recognized claims an identity, usually via a Personal Identification Number (PIN), a user name, a smart card, etc., and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., "Does this biometric data belong to Janet?"). Identity

How to cite this article: Eludire AA, Adio EO. Biometrics Technologies for Secured Identification and Personal Verification. Biostat Biometrics Open Acc J. 2018; 6(2): 555683. DOI: 10.19080/BBOAJ.2018.06.555683.

verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

Identification mode involves establishing a person's identity based only on biometric measurements. The comparator equivalent they obtained biometric with the ones stored in the database bank using a 1: N matching algorithm for recognition. In the identification mode, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., "Whose biometric data is this?"). Identification is a critical component in negative recognition applications where the system establishes whether the person is who she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may work for positive recognition, negative recognition can only be established through biometrics [3].

Identified application areas

Staff Attendance Management is an area that has been carried out using attendance software that relies on passwords for users' authentication. However, this type of system allows for impersonation since the passwords can be shared or tampered with. Passwords could also be forgotten at times thereby preventing the user from accessing the system [7]. Oloyede et al. [8] carried out extensive research on applicability of biometric technology to solve the problem of staff attendance. However, the researchers did not write any software to address the problems of attendance [9-12]. Marijana carried out a critical review of the extent to which biometric technology has assisted in controlling illegal entry of travelers into specific country through the integration of biometric passport. The issue regarding how the false acceptance rate can be measured in a border control setting was also looked into. The researcher concludes that the problems associated with biometric technologies such as error rates, spoofing attacks, non-universality and interoperability can be reduced through an overall security process that involves people, technology and procedures. Previously a very few work has been done relating to the academic attendance monitoring problem like radio frequency identification devices (RFID) based systems. Furthermore idea of attendance tracking systems using facial recognition techniques have also been proposed but it requires expensive apparatus still not getting the required accuracy [13-15].

Conclusion

This work presents the biometric technologies that can be used for personal identification and verification. An important area for the application of biometric technologies is implementation of an effective and efficient fingerprint-based Staff Attendance Management System aimed to address the shortcomings in recording staff attendance. This also allow attendance register system generate positive results in the process of gathering, processing and storing attendance information, and making it available for on-line consultation and generation of reports. Having this system enable staff to take their attendance at work serious.

References

1. Brunelli R (2009) Template Matching technique in computer Vision: theory and practice.
2. Dileep K, Yeonseung R, Dongseop K (2008) A Survey on Biometric Fingerprints: The Cardless Payment System, IEEE ISBAST.
3. Alex H (2006) Biometrics: Payments at Your Fingertips.
4. Ashbourn (2000) An introduction to the Implementation of Biometrics Systems.
5. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition, Circuits and Systems for Video Technology. IEEE Transactions 14(1): 4-20.
6. Jain AK, Ross A, Prabhakar S (2004) An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics 14.
7. Shoewu O, Olaniyi OM, Lawson A (2011) Embedded Computer-Based Lecture Attendance Management System. Afr J of Comp & ICT 4(3): 27-36.
8. Oloyede MO, Adedoyin AO, Adewole KS (2013) Fingerprint Biometric Authentication for Enhancing Staff Attendance System. International Journal of Applied Information Systems (IJAIS) 5(3): 19-24.
9. Jain AK, Feng J (2011) Latent Fingerprint Matching, IEEE Transactions Circuits and Systems for Video Technology. Special Issue on Image- and Video-Based Biometrics 33: 88-100.
10. Connell JH, Ratha NK, Bolle RM (2001) An analysis of minutiae matching Strength, London, UK.
11. Kumar (2003) Electronic voting machine- A review, IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME), pp. 44-48.
12. Maltoni D (2010) A tutorial on fingerprint Recognition, Biometric Systems Laboratory-DEIS -University of Bologna, Italy.
13. Prabhakar S, Maltoni D, Maio D, Jain AK (2013) Handbook of fingerprint recognition, Springer, Verlag, New York, USA.
14. Pankanti SI, Prabhakar S, Jain AK (2002) On the Individuality of Fingerprints. IEEE Trans PAMI 24: 1010-1025.
15. Yash M, Aishwary V, Prachi A, Kapil M, Mittal VK (2016) Fingerprint biometric based Access Control and Classroom Attendance Management System.

How to cite this article: Eludire AA, Adio EO. Biometrics Technologies for Secured Identification and Personal Verification. Biostat Biometrics Open Acc J. 2018; 6(2): 555683. DOI: 10.19080/BBOAJ.2018.06.555683.

DOI: 10.19080/BBOAJ.2018.06.555683