INTERNATIONAL JOURNAL OF ADVANCED INNOVATIVE TECHNOLOGY IN ENGINEERING

Published by Global Advanced Research Publication House Journal

Home page: www.ijaite.co.in

Study of Biometric Authentication Techniques and Its Application

[1]Vishal Yuvraj Mulmule, [2]Prof. C. S. Patil

[1,2]Department of Electronics & Telecommunication, Shri Gulabrao Deokar College of Engineering, Jalgaon, Maharashtra, India

[1]vishalmulmule2017@gmail.com, [2]cspatil915@gmail.com

Article History

Received on: 14 Aug. 2022

Revised on: 05 Sept 2022

Accepted on: 30 Sept. 2022

Keywords: Fingerprint Recognition, Biometric Authentication, Cryptography Authentication, Face Recognition

e-ISSN: 2455-6491

DOI: 10.5281/zenodo.7185697

Production and hosted by
www.garph.org

ABSTRACT

One of the best and most sophisticated biometrics is fingerprint recognition. Fingerprints have been used for recognised proof for over a decade because of their novelty and constancy through time; more recently, though, they have begun to be computerised because to advancements in reasoning abilities. According to the inherent simplicity in security, the multiple sources available for collection, and their setup use and collection by legal requirement and mobility, fingerprint recognition is widely used. In this essay, we looked at the value and various applications of fingerprint recognition. Additionally, we talk about the uses for fingerprint recognition. This essay outlines the basic FPR structure, various FPR systems, and challenges. In this paper we studied about the importance and different areas of fingerprint identification. We also discuss about the applications of fingerprint identifications. This paper presents outline of a fundamental FPR framework, different FPR systems and difficulties.

1. INTRODUCTION

Biometric Authentication is any process that validates the identity of a user who wishes to sign into a system by measuring some intrinsic characteristic of that user. The traditional methods involving passwords and PIN numbers do not require the candidate to be present there at the time of authentication, while biometrics techniques do not require password, PIN numbers or any RFID cards. It prevents fraud usage of ATMs, mobiles, PCs, smart cards etc. The characteristics are measurable and unique. Identity verification occurs when the user claims to be already enrolled in the system (presents an ID card or login name); in this case the verification biometric data obtained from the user is compared to the user's data already stored in the database. Identification (also called search) identification occurs when the identity of the user is a priori unknown. In this case the user's biometric data is matched against all the records in the database as the user can be anywhere in the database or he/she actually does not have to be there at all. In biometric-based authentication, a legitimate user does not need to remember or carry anything and it is known to be more reliable than traditional authentication schemes. Biometric authentication offers a convenient, accurate, irreplaceable and high secure alternative for an individual, which makes it has advantages over traditional cryptography-based authentication schemes [1].

There are basically two kinds of biometric systems:

1. Automated identification systems operated by professionals (e.g., police Automated Fingerprint Identification Systems – AFIS). The purpose of such systems is to identify an individual in question or to find an offender of a crime according to trails left at the crime scene. Enrolled users do not typically have any access to such systems and operators of such systems do not have many reasons to cheat.

2. Biometric authentication systems used for access control. These systems are used by ordinary users to gain a privilege or an access right. Securing such a system is a much more complicated task.

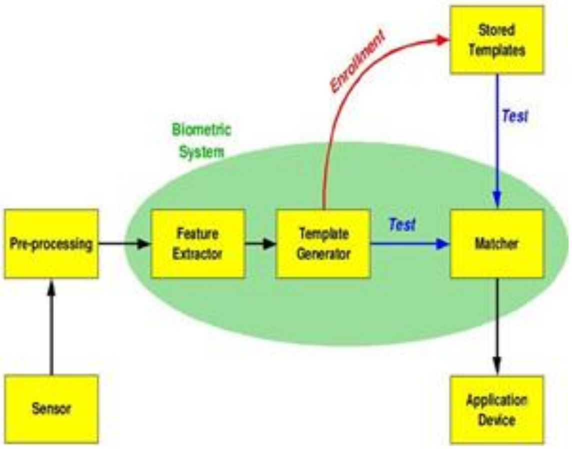

Figure 1: The model of Biometric System

Figure 1 gives the basic model of biometrics system [11]. Typical biometric system comprises of sensor like transducer to convert data to digital form. Biological templates have generated through digital image processing algorithms. Then with the use of database these templates are compared with other saved templates; these are performed by matching algorithms. Finally, decision process will determine the correct authentication.

The purpose of this paper is to give a look at the use of biometrics technology to determine how secure it might be in authenticating users, and how the users job function or role would impact the authentication. The advantages of biometric authentication definitely look very attractive, there are also many problems with biometric authentication that one should be aware of. We will be exploring many of the technologies and applications that make up the field of "biometric authentication" – what unites them and what differentiates them from each other.

2. Related Work

Normally Identification or authentication can be implemented by following methods as shown in figure 2.

1. Token can be produced from a multitude of different physical objects. Human intervention requires for identification process for manual based tokens such as paper passport and identity cards. Automated tokens do not require human intervention in the identification process; the identity is verified by a system/computer such as magnetic-stripe cards, memory cards, or smart cards.

2. By means of passwords, PIN numbers sometimes authentication have processed.

3. Biological physical or behavioural characteristics such as IRIS, Finger-paint, Palm vain, LIP motion, audio and signature analysis-based authentication have been developed now days.

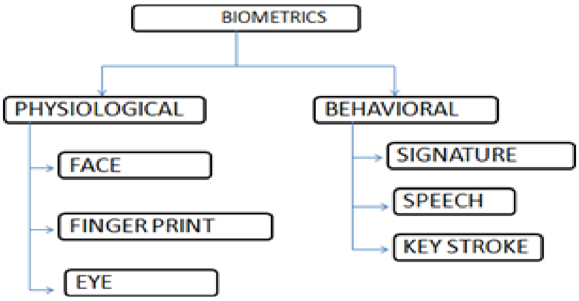

Figure 2: Classification of biometrics

Having identified the required qualities and measures for each quality, it would seem a straightforward problem to simply run some experiments, determine the measures, and set a weighting value for the importance of each, thereby determining the "best" biometric characteristic.

Different biometrics authentication methods have reviewed as follows:

A. *Fingerprints Identification*

This is the oldest biometric authentication approach. It analyzes finger characteristics. The first is by scanning optically the finger. The other method is by using electrical charges that determines which parts of the finger are directly in contact with the sensor. Each fingerprint has some characteristics, such as curves, bifurcations, deltas. One set of these characteristics is unique for each person.

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based. Minutiae-based techniques find the minutiae points first and then map their relative placement on the finger. Minutiae are individual unique characteristics within the fingerprint pattern such as ridge endings, bifurcations, divergences, dots or islands. In the recent years automated fingerprint comparisons have been most often based on minutiae. The problem with minutiae is that it is difficult to extract the minutiae points accurately when the fingerprint is of low quality. This method also does not take into account the global pattern of ridges and furrows. The correlation-based method is able to correlation overcome some of the difficulties of the minutiae-based approach. Based However, it has some of its own shortcomings. Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation.

Figure 3: Basic Fingerprint

B. Eyes Feature Recognition

There are two methods using the eyes characteristics for authentication. The first is based on the retinal recognition. The user has to look in a device that performs a laser-scanning of his retina. The device analyzes the blood vessels configuration of the acquired retinal picture. This blood vessels configuration is unique for each eye. The device is not friendly, because you have to fix a point while a laser is analyzing your eye.

The second method is based on the iris recognition. The scan is done by a camera. Unlike the retinal method, you don't need to be close to the device to be authenticated. The acquired picture is analyzed by the device, and contains 266 different spots. Moreover, iris is stable through the whole life. The 266 spots are based on characteristics of the iris, such as furrows and rings [9]. The iris patterns are obtained through a video-based image acquisition system. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes. The main drawback of the retina scan is its intrusiveness. The method of obtaining a retina scan is personally invasive. A laser light must be directed through the cornea of the eye. Also the operation of the retina scanner is not easy.

C. Face Recognition

A simple camera or a web cam with good resolution use in face recognition, after capturing face image the device computes a digital representation based on some features of the face. The representation is compared with one which is stored in a database, and if there is a match, the user is authenticated. It is easy to implement and cheap authentication method with unique recognition. Facial recognition in visible light typically models key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. The accuracy of the face recognition systems improves with time, but it has not been very satisfying so far.

D. Voice Recognition

The user speaks in a microphone, and voice is recorded and computed. It is done by using some frequency analysis of the voice. It can be useful to authenticate someone through a telephone, and it allows users to work on a remote location. It is less accurate than other biometrics authentication methods, and some errors can occur [9].

Speaker verification focuses on the vocal characteristics that produce speech and not on the sound or the pronunciation of the speech itself. The vocal characteristics depend on the dimensions of the vocal tract, mouth, nasal cavities and the other speech processing mechanisms of the human body. The system typically asks the user to pronounce a phrase during the enrolment; the voice is then processed and stored in a template (voiceprint). Later the system asks for the same phrase and compares the voiceprints. Currently there are three major international projects in the field of voice technology: PICASSO, CASCADE and Cost 250.

E. Signature Analysis

The signature analysis is a biometrical authentication solution. The device is a tactile screen. The parameters that are computed for the authentication are the shape of the signature, the time taken to do it, the stroke order and the pen pressure. With the computation of these parameters, the system provides to you a unique authentication method. It is virtually impossible to reproduce in the same way somebody else's signature. It is easy to implement and quite cheap. This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications. The accuracy of the signature dynamics biometric systems is not high; the crossover rate published by manufacturers is around 2%.

F. Handprints Recognition

This method is based on the recognition of the handprints. The device is a scanner that extracts a picture of a user's hand. Some characteristics like length of the fingers, distance between them or their relative position are computed. These characteristics are compared with the saved database and result will be displayed [1]. This method is not much complex as compared with IRIS or signature analysis type methods.

These methods are most commonly based either on mechanical or optical principle. Optical hand geometry scanners capture the image of the hand and using the image edge detection algorithm compute the hand's characteristics. There are basically 2 sub-categories of optical scanners. Devices from the first category create a black-and-white bitmap image of the hand's shape. This is easily done using a source of light and a black-and-white camera. The bitmap image is then processed by the computer software.

G. DNA Analysis

This method is based on a DNA analysis. To perform a DNA analysis the user has to give some of his cells such as skin hair etc. Analyzing DNA takes a long time. Everyone is unique through his DNA. But it can be easily fooled, because anyone can steal a hair [4]. It will maybe become the most efficient in crime department to identify criminal. DNA sampling is rather intrusive at present and requires a form of tissue, blood or another bodily sample.

H. Palm Print Recognition

Palm print is inner part of hand. Palm prints possess features such as principal lines, orientation, minutiae, singular points etc. Also palm print modality is unique. Palm print recognition is used in civil applications, law enforcement and many such applications where access control is essential. Palm has features like geometric features, delta point‟s features, principal lines features, minutiae, ridges and creases. Principal lines are heart line, head line and life line [6].

Palm print contains three principal lines which divides palm into three regions: Interdigital, Hypothenar and Thenar. An Inter-digital region lies above the Heart line. The Thenar lies below the Life line. And Hypothenar is between Heart and Life line. From palm print principal lines, minutiae, ridges features can be extracted for identification.

Hand vein geometry is based on the fact that the vein pattern is distinctive for various individuals. The veins under the skin absorb infrared light and thus have a darker pattern on the image of the hand taken by an infrared camera [8].The hand vein geometry is still in the stage of research and development. One such system is manufactured by British Technology Group. The device is called Veincheck and uses a template with the size of 50 bytes.

I. LIP Motion Based Authentication

Personal authentication is based on LIP motion only. It is composed of a password embedded in the lip movement and the underlying characteristic of lip motion. Subsequently, a lip-password protected speaker verification system aiming at holding a double security is established. That is, the claimed speaker will be verified by both of the password information and the underlying behavioral biometrics of lip motions simultaneously. Accordingly, the target speaker saying the wrong password or an impostor who knows the correct password will be detected and rejected [2].

Discriminative Analysis of Lip Motion Features for Speaker Identification and Speech-Reading gives explicit lip motion information, instead of or in addition to lip intensity and/or geometry information, for speaker identification and speech-reading within a unified feature selection and discrimination analysis framework. But the principal feature components representing each lip frame are not always sufficient to distinguish the biometric properties between different speakers; hence it is quite tedious complex method to implement.

3. STEPS OF FINGERPRINT RECOGNITION

Fingerprint recognition alludes to the robotized strategy for recognizing or confirming the personality of an individual dependent on the comparison of two fingerprints. Fingerprint recognition is a standout amongst the most outstanding biometrics, and it is by a long shot the most utilized biometric answer for confirmation on computerized systems. The purposes behind unique finger fingerprint recognition being so famous are the simplicity of obtaining, set up utilize and acknowledgment when contrasted with different biometrics, and the way that there are various (ten) wellsprings of this biometric on every person.

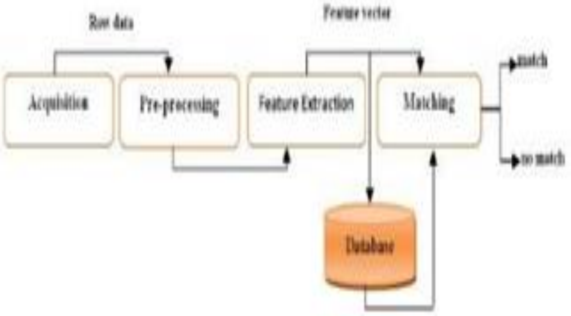

Figure 3: Basic steps of fingerprint recognition

The Image Acquisition arranges is the procedure to get images by various ways. There are two different ways to catch fingerprint image; on the web and disconnected. In the online fingerprint identification, the optical finger impression per user is utilized to catch the image of finger impression. The extent of fingerprint image will be 260*300 pixels. The disconnected fingerprint identification is acquired by ink in the region of finger and afterward put a sheet of white paper on the fingerprint lastly examines the paper to get a digital image.

The pre-preparing stage is the way toward expelling undesirable information in the fingerprint picture, for example, commotion, and reflection .and so forth. The fingerprint picture pre-handling is utilized to build the clarity of edge structure.

For automation, a reasonable presentation i.e., feature extraction of fingerprints is fundamental. This portrayal ought to have the accompanying properties –

Retention of separating intensity of each unique mark at a few dimensions of goals
Easy calculability
Amenable to computerized coordinating calculations
Stable and invariant to noise and contortions
Efficient and reduced portrayal

4. Fingerprint Matching Techniques

Matching fingerprint images is a to a great degree troublesome issue, for the most part because of the huge inconstancy in various impressions of a similar finger. Fingerprint matching algorithms are generally grouped into 3 noteworthy classifications.

A. Correlation-based Matching

Two fingerprint pictures are superimposed and the connection between relating pixels is registered for various arrangements (e.g., different relocations and turns). Fourier transform [10] and in addition Fourier-Mellin Transform [11] can be utilized to accelerate the connection calculation

B. Feature-based (or Minutiae- based) Matching

coordinating, where details (i.e., ridge ending and ridge bifurcation) are extricated from the enlisted fingerprint picture and the info fingerprint picture, and the quantity of Binarization Ridge Thinning relating particulars pairings between the two pictures is utilized to perceive a valid fingerprint image. Then again, Jain et al. [12] utilized a string coordinating method while Isenor and Zaky [13] propose a chart-based fingerprint verification algorithm. Fan et al. [14] portrays a fingerprint verification dependent on a bipartite chart development among model and question fingerprint include groups

C. Pattern-based (or Image-based) Matching

Pattern based algorithms look at the fundamental fingerprint patterns (between a recently put away layout and a competitor fingerprint. The images should be adjusted similarly situated, about a main issue on each image. The hopeful fingerprint image is then graphically contrasted with the layout with decide the level of match.

5. Application Of Fingerprint Recognition

Because it is one of the cheapest biometric solutions, fingerprint recognition already knows many different applications. We only list a few examples here:

- Logical access control, for example there exist numerous fingerprint reader devices and software for access control to personal computers. Logical access control is a major territory of use for biometric innovation. When we say, "It's an ideal opportunity to execute the secret word," this is the tech we're discussing. Regardless of whether it's anchoring the applications on your cell phone, accessing a work email or empowering a viable BYOD approach, biometric logical access control solutions can launch you into the up-and-coming age of comfort and digital security.

- Physical access control, for example locks with a fingerprint reader. Physical access control arrangements are more grounded validation strategies than keys, scratch cards and PINs for a straightforward reason: they're what you are, not what you have. While a key can be lost or stolen and utilized by an unapproved individual, your finger impression is something one of a kind that just you have. Fingerprint biometric locks are ideal for keeping entryways shut to everything except those approved to utilize them.
- Fingerprint attendance systems for time and attendance management
- Biometric alternative to loyalty card systems [15].
- Financial services (e.g., ATM)
- Immigration & border control (e.g., points of entry declared for frequent travelers, passport and visa cases)
- Social services (e.g., fraud preventation in entitlement programmers)
- Health care (e.g., security measure for privacy or medical records)

- Physical access control (e.g., at institutional, government & residential establishment)
- Computer Security (e.g., personal computer access, network access, Internet use, e-commerce, e-mail, encryption)
- Telecommunications (e.g., mobile phones, call center technology, phone cards, televised shopping)
- Law enforcement (e.g., criminal investigation, national ID, driving license, rehabilitation institutions/prison, home confinement, small gun)

CONCLUSION

Proper design and implementation of the biometric system can indeed increase the overall security. It is necessary to trust the input device and make the communication link secure. Facial recognition systems are often deployed at frequently visited places to search for criminals.

Fingerprint systems are used to find an offender according to trails left on the crime spot. Infrared thermographs can point out people under influence of various drugs. Biometric systems successfully used in non-authenticating applications may but also need not be successfully used in authenticating applications.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

FUNDING SUPPORT

The author declare that they have no funding support for this study.

REFERENCES

[1] S Harakannanavar, Sunil & C R, Prashanth & K B, Raja. (2019). Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends. International Journal of Advanced Networking and Applications. 10. 3958-3968. 10.35444/IJANA.2019.10048.

[2] Phadke, Sushil. (2013). The Importance of a Biometric Authentication System. The SIJ Transactions on Computer Science Engineering & its Applications (CSEA). 1. 10.9756/SIJCSEA/V1I4/0104550402.

[3] Phagwara, R.I. (2016). Design of Biometric Authentication System using Three Basic Human Traits.

[4] Mr. Mule Sandip S., Mr.H.B.Mali, "Review on Biometric Authentication Methods", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 11, November 2015.

[5] Kirti Pathak, "Roll of Fingerprint Identification/Recognition Techniques in Biometric Systems and its Applications", International Journal on Recent and Innovation Trends in Computing and Communication Volume: 6 Issue: 11, 2018.

[6] Singh, Tripty. (2016). Design of a dual biometric authentication system. 845-850. 10.1109/ICEEOT.2016.7754806.

[7] Omran, Safaa & Salih, Maryam. (2014). Design and Implementation of Multi-model Biometric Identification System. International Journal of Computer Applications. 99. 14-21. 10.5120/17448-8255.

[8] Robert Cockell and Basel Halak, "On the Design and Analysis of a Biometric Authentication System Using Keystroke Dynamics", Cryptography 2020, 4, 12; doi:10.3390/cryptography4020012.

[9] A. Joshy and M. J. Jalaja, "Design and implementation of an IoT based secure biometric authentication system," 2017 IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), 2017, pp. 1-13, doi: 10.1109/SPICES.2017.8091360.

[10] Jain, A.K., Nandakumar, K. (2009). Biometric System Design, Overview. In: Li, S.Z., Jain, A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_18.

[11] S. Kailasavalli, Dr. K. A. Jayabalaji, E. Jayanthi, Dr. P. Gnanachandra, R. Pandiarajan, "Design and Develop a Biometric Authentication System using Lip Image", Turkish Journal of Computer and Mathematics Education, Vol.12 No.9, 2021 pp-1836-1840.

[12] Sajaad Ahmed Lone, A. H. Mir, "Smartphone-based Biometric Authentication Scheme for Access Control Management in Client-server Environment", I.J. Information Technology and Computer Science, 2022, 4, 34-47

[13] Dakhil, I. and Ibrahim, A. (2018) Design and Implementation of Fingerprint Identification System Based on KNN Neural Network. Journal of Computer and Communications, 6, 1-18. doi: 10.4236/jcc.2018.63001.

[14] Dennis Mugambi Kaburu, Julianne Sansa-Otim, Kajumba Mayanja, Drake Patrick Mirembe, Tony Bulega, "A usability based approach to designing continuous user biometric authentication system", Quality and User Experience (2018) 3:8 https://doi.org/10.1007/s41233-018-0021-1