International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 2, February 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Biometric System and Recognition: Authentication and Security Issues

Shweta Naik

Department of MCA SEM VI, YMT College of Management,
Institutional Area, Kharghar, Navi Mumbai, Maharashtra, India

ABSTRACT

In recent days Biometric has become the most popular technique used. The purpose of biometric systems is used to achieve high security, authentication and many more. Through this scheme or technique it ensures that the services are accessed only by the authorized persons. This system works effectively and is user friendly. Biometric systems are progressively exchanging the ongoing password and authentication (token based) system. Authentication and Security recognition are the two most essential characteristic to consider in scheming a biometric system. In this paper, a broad review is presented to illuminate on the latest technologies in the study of fingerprint-based biometric covering these two characteristic with a view to improving system security and authentication recognition.

KEYWORDS: *Biometric system, Security, Authentication, Recognition, Authorization*

How to cite this paper: Shweta Naik "Biometric System and Recognition: Authentication and Security Issues" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-2, February 2020, pp.911-915, URL: www.ijtsrd.com/papers/ijtsrd30195.pdf

IJTSRD30195

I. INRODUCTION

Biometric is the particular phrase for human body measurements and calculations. It refers to the function related to human quality. Biometric are sensual or related human attributes to that can be used to numerically distinguish a individual to permit access to systems, devices or data. With different biometric scanners on phones and other electronic devices are universal or familiar and used frequently, as well as a increasing the number of services calling for high level security and good experience of customers, usual methods of authentication (e.g. passwords and PIN s) are progressively being supplant with biometric technologies.

Passwords have some obvious or open drawbacks—they could be sneak, forgotten, or lost. In comparison, biometric offer an substitute or an alternative solution to the task of personal or public authentication or identification based on biometric features. To be unnoticed or lost is not possible, and unlike passwords, they are hard to form. There are some biometric features that can be defined for an individual. Examples: fingerprint, finger-vein, iris, face, voice, and many more.

Generally, a biometric system consists of four modules namely sensor module, feature extraction module, template database, and matching module. Specifically, the sensor module acquires the biometric image.

The use of biometric can build up the security level in authentication. User authentication is the main step for securing any information in the computer system. With different biometric devices such as scanners on smart phones, desktops, laptops and other devices has becoming more frequent and dominant and also has increased the number of services for more security and customer experience, and other methods for authentication like password, PINs are increasingly displace by the biometric technologies.

A set features are taken out from the biometric image by the feature extraction module. Organized features offerings are stored in the template database as template data. The matching module is responsible for examining the query and template data to check whether the meet or not.

Types of Biometrics:

A biometric identifier is one that is related to integral human characteristics. They fall into two categories: physical identifiers and behavioral identifiers. Physical identifiers are those, for the most part, fixed, rigid and device free.

Fingerprints: Fingerprint scanners have become omnipresent in recent years due to their distributed deployment on smart-phones. Any device that can be touched or which one can feel while using it, such as a phone screen, computer mouse keyword or touchpad, or a door

panel, has the potency to become an easy and favorable fingerprint scanner.

Photo and video: If a device is provided with a camera, it can br easy to use for authentication purpose. Facial recognition and retinal scans are two common approaches.

Voice: Voice-based digital instrument and telephone-based portals are already using voice recognition systems to identify and verify users and authenticate the customers.

Signature: Digital signature scanners are already in distributed among different places such as in checkouts and in banks and are a good choice for environment where users and customers are already assumes to have the signature of their names.

DNA: Today, DNA scans are used mainly in law enforcement to determine the suspects -- and also in movies. In practice, DNA combinations has been too slow for common use

Face Recognition: The anatomy facial features or patterns are used for authntication and recognition of an person's identity.

II. LITERATURE REVIEW:

Biometric based security, such as fingerprint authentication, is proven to be both more protected and handy than passwords, making fingerprint sensing making progressively common and product differentiating feature in smart phones, tablets and PCs. However, fingerprint authentication also increased security concerns that can be addressed with protections purpose built for biometrics. Synaptic s helps ensure biometric data protection through the Sentry-point Security Suite of features and architectures that meets or suits the full range of market needs.

Spoofing attacks to the user interface (the sensor module) are mostly because of the presenting the fake biometric trait.[4]. A different forms of fingerprint sensors are approved to see if they can reject a fake fingerprint film or not. The test results show that the fake finger films are accepted by most of the approved sensors in[4]. In recent years, energetic work has been done in the research, which is used to detect whether the existing feature is from a live human being or not. The security vulnerabilities of a biometric system were underlined using threat models [6].

The security and privacy about the biometric authentication raises need to be addressed. It is analyzed that automatic fingerprint recognition is the best candidate biometric technology for explosives security from an technical analysis of the requirements: security, usability, toughness, size, form factor, privacy and operational temperature range are solved in this [7].

Fingerprint scanner is used with great extent in today‟s attendance system. It provide huge security. Padma Rekha [8] proposed the attendance is handled in every institution or organization. In the old, the attendance is handled in written work. In this paper, to put off the human work, the automatic process is been maintained.

Kamta Nath Mishra, [6] have concisely explained about the thumbprint based identification system used with the help of soft computing technique. Dr. Naik and Patil [9] uncovered the biometric authentication is the most trusty method for authenticating a user based on his/her thumb impression. Now in modern approach, live fingerprint readers are used. These are based on optical, thermal, capacitive, silicon or ultrasonic principles [10, 11, 12] the variance between valley and rigid.

When it is time arises to use the biometric authentication, the degree of security is concerned. In this paper, we will discuss about recent research and insights into security authentication and recognition accuracy. There are various factors with the help of which we can judge the performance of any biometric authentication techniques.

III. RESEARCH METHODOLOGY:

A. Biometric Authentication:

Biometric authentication is used in computer science as a form used for recognition and for controlling the access. It is also used for recognizing a single user or for a groups that are under observation. The use of biometric can build up the security level in authentication. User authentication is the main step for securing any information in the computer system. With different biometric devices such as scanners on smart phones, desktops, laptops and other devices has becoming more frequent and dominant and also has increased the number of services for more security and customer experience, and other methods for authentication like password, PIN s are increasingly displace by the biometric technologies. Authentication is done through number of measures like Password, PIN, ID Cards etc. Misuse of this measures are also increasing to a higher level nowadays. It is an essential an most important step which restricts the access to the critical data or personal information only to the legislative users.

B. Authentication Process :

Authentication in biometric are carried out in two stages the enrolment stage and verification stage. Fingerprint recognition as an example. In the enrolment stage, a user presents their finger to the fingerprint sensor and a fingerprint image is generated by the sensor module. Certain features of the generated fingerprint image are taken out and further they are passed forward to generate template data for the purpose of comparison in the verification stage. In the second stage of verification, the fingerprint image of a query is collected by the sensor module.

The image or photo of the query fingerprint image goes through the similar process as in the enrolment stage, so as to obtain query data. The query data are then compared with the template data so that a similar result is obtained. Compared with other biometric methods like (e.g., fingerprint, face, iris, voice, hand geometry) fingerprint-based recognition systems are influenced more largely and deployed more widely. Fingerprint recognition consider the patterns found on a fingertip. The use of fingerprints as a biometric is both the oldest way of computer-aided recognition, and the latest technology used most widely established today. It has been compute that the probability to find two persons with the same fingerprint is one in one billion.

According to the recognition accuracy of fingerprint-based recognition systems is very high but the general open public showing medium acceptability to fingerprint accquring system. This is why fingerprint biometric systems occupy a high market shares and have been adopted and used in various applications.

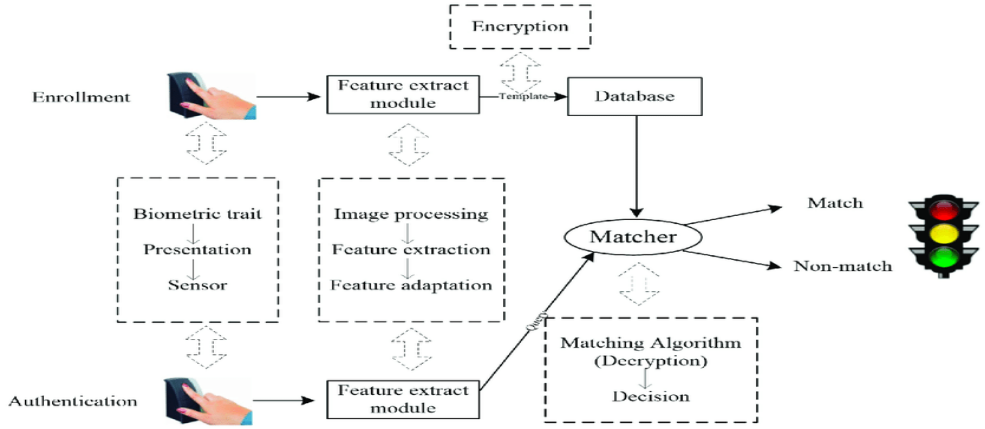

Fig1: Two stages of Biometric Authentication (enrolment and verification).

Although fingerprint recognition shows significant strength and a rich and a well-heeled future, it has some unsolved issues, such as inadequate accuracy and security concerns. In this paper, a broad review is been presented to clarify on the latest development in the study of fingerprint-based biometric they are focused on two important aspects—authentication and recognition accuracy.

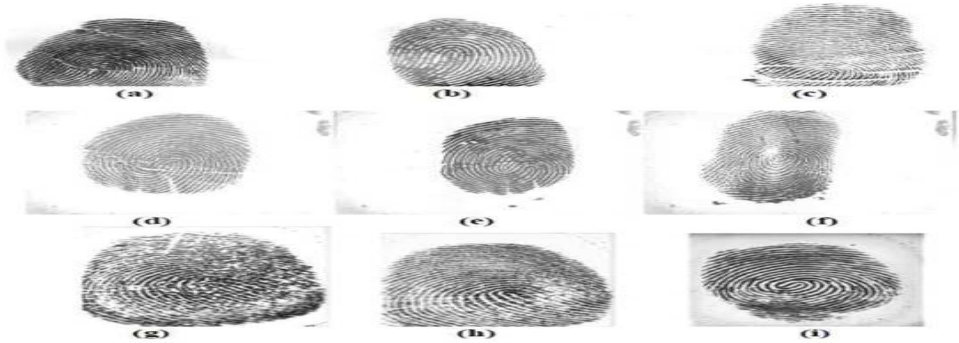

Fig2 [13]: Analysis of Fingerprint

Spoofing attacks to the user interface (the sensor module) are mostly because of the presenting the fake biometric trait. Since biometric traits are not secret or hidden, an adversary can intrude into the system with a fake trait (e.g., artificial fingerprint, face mask or through other things) to spoof the biometric system if the system is unable to differentiate or recognize between a fake and a genuine biometric trait. A number of fingerprint sensors are tested to see if they can reject a fake fingerprint film or not. The test results show that the fake finger films are accepted by most of the tested sensors.

C. Liveness Detection:

Liveness detection one of the technique is useful not only for authentication but also for identification of proofing. Where biometric authentication involves verification that the user or an individual is the same identical person who initially at the beginning enrolled, biometric identity proofing can be performed as part of an organizational socialization process to verify that the person or an applicant is in fact a actual person. An example is using a mobile banking application for applying for a new account. The applicant is not known to the bank, so liveness detection technique can be used to confirm and sustain that the applicant is not trying to open a fraudulent which is illegal account.

In biometric systems, the purpose of liveness testing is to determine whether the biometric being captured of an person is an actual measurement from the authorized legitimate, live person who is physically present at the time of capture the fingerprint. While fingerprint systems may have an superior performance and improve the security.

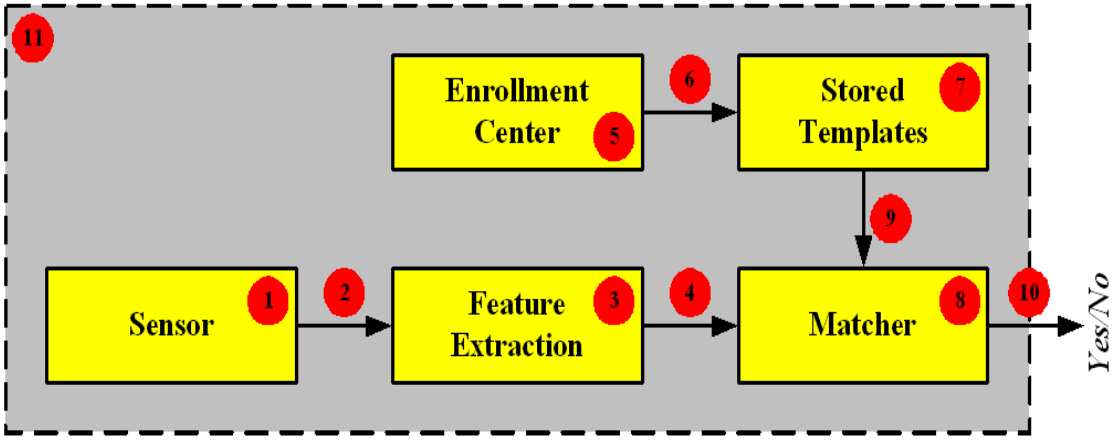

Fig3 [14]: Liveness Detection Process

Former studies have shown that it is not difficult to make molds of present potential fingerprints left by authorized users and to create fake fingers made from Play-Doh, gelatin, and silicone like other materials to fool a variety of collections of fingerprint scanners, termed spoofing. Liveness detection deflate the risk of spoofing by demanding for a liveness signature, in addition to matched with biometric information. Methods can be divided into two categories: hardware and software categories. Hardware methods which includes various estimations like monitoring oxygen level, (ECG), or odor (fragrance), while software based measurements uses additional processing of the biometric information itself to Segregate liveness signatures like moisture and distorting.

While liveness algorithm makes spoofing more difficult and challenging, they need to be considered as components of various biometric system, which bring with it performance characteristics along with factors such as ease of use (the way of using it), collectability (collected data), unviersality, spoof-ability, performance, and in some of cases, even uniqueness. No system is perfect in its potentiality to prevent spoof attacks. However, the liveness algorithm can reduce the vulnerability to decrease the risk of spoofing

The main efforts of this paper are highlighted as follows:

1. Security and recognition accuracy, despite being two most important aspects in biometric system design, have not been fully satisfied the study simultaneously. Prior to this paper, no research work has delivered or presented a comprehensive review considering both of them. In this paper, the recent research and insights into security and recognition accuracy are completely analyzed, examined and discussed.
2. Based on a careful analysis, limitations of existing research are discussed and suggestions for the future work has been given and to overcome with the limitations are provided.
3. The two most critical attacks to biometric systems have been discussed in this paper. How to resolve the challenges, so as to defend or justify the biometric systems, is the focus of current and future biometric security research.
4. Most existing methods, either with or without template protection, were set forward for the ideal situations. In this paper, we underline the importance of considering recognition accuracy under non-ideal conditions. Our analysis is backed by solidified evidence and with elaborated comparison.

Fig4 [14] Example of liveness Detection Fingerprint

IV. CONCULSION:

This paper gives a wide review of two significant measures for fingerprint-based biometric systems that is, authentication and recognition accuracy. In regards to authentication, we have analyzed the method of liveness detection. Most currently available methods, either with or without template protection, were set forward for the ideal situations. In this paper, we underline the importance of considering recognition accuracy under non-ideal conditions. Our analysis is backed by solidified evidence and with elaborated comparison. Since 2009, the fingerprint Liveness Detection was aimed to allow the research companies sensible and individual assessment in anti spoofing algorithms and systems. Based on a careful analysis, limitations of existing research are discussed and suggestions for the future work has been given and to overcome with the limitations are provided.

V. FUTURE ENHANCEMMENT:

In our future work, biometric technologies like facial scanning, voice and iris recignition, fingerprint scanning can be more popularly because of which authentication becomes much more convenient and secure for the data or information in different organizations and smart phone. More realistic methods and tenchology in future can be used for the security purpose of authentication in biomerics systems.

VI. REFERENCE:

[1] https://www.google.com/search?tbm=isch&sxsrf=ACYBGNSdHd5S8CnLDsMryFaT6vR6JW_mcg:1576511105164&q=+biometric+authentication+diagram&chips=q:biometric+authentication+diagram,g_1:identification&usg=AI4_-kQN22p03Sx-tc_YU7ei6F_rGghyXw&sa=X&ved=0ahUKEwizm6HDwbrmAhUzguYKHVR5BT4Q4lYIKigA&biw=1242&bih=568&dpr=1.1#imgrc=8ht8EGwm6csK5M:

[2] https://scholar.google.co.in/scholar?q=Security+and+Accuracy+of+Fingerprint-Based+Biometrics:+A+Review&hl=en&as_sdt=0&as_vis=1&oi=scholart

[3] https://www.researchgate.net/figure/Eight-possible-attack-points-to-a-typical-biometric-authentication-system-adapted-from_fig2_330711092

[4] Kang, H.; Lee, B.; Kim, H.; Shin, D.; Kim, J. A study on performance evaluation of the liveness detection for various fingerprint sensor modules. In Proceedings of the International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, Oxford, UK, 3–5 September 2003; pp. 1245–1253

[5] https://www.researchgate.net/publication/330711092_Security_and_Accuracy_of_Fingerprint-Based_Biometrics_A_Review

[6] Security Vulnerabilities Against Biometric System Mahesh Joshi1 Bodhisatwa Mazumdar1 Somnath Dey1 {phd1701101004, bodhisatwa, somnathd}@iiti.ac.in 1 Indian Institute of Technology Indore, India

[7] A Study of Biometric Approach Using Fingerprint Recognition Ravi Subban and Dattatreya P. Mankame.

[8] P. Padma Rekha, D. Amudhan, V. Narendhiran, N. Pavithra, S. Ramya, "AUTOMATIC ATTENDANCE MONITORING SYSTEM".

[9] Dr. Naik, P. G. and Patil, M. B, "BIOMETRIC DATA ANALYSIS OF STUDENT ATTENDANCE SYSTEM AT CSIBER", International Journal of Current Research, 8(2), 26751-26762, 2016.

[10] A. Ross, S. Dass, and A. K. Jain, "A deformable model for fingerprint matching", Journal of Pattern Recognition, Elsevier, Volume 38, No. 1, Jan. 2005, pp. 95–103.

[11] T. Matsumoto, H. Hoshino, K. Yamada, and S. Hasino, "Impact of artificial gummy fingers on fingerprint systems", In Proc. of SPIE, Volume 4677, Feb. 2002, pp. 275–289.

[12] A. K. Jain, A. Ross, and S. Pankanti, "Biometric: A Tool for Information Security", IEEE Trans. Information Forensics and Security, Volume 1, No. 2, Jun. 2006, pp. 125–144.

[13] https://www.semanticscholar.org/paper/Review-of-the-Fingerprint-Liveness-Detection-2009-Ghiani-Yambay/086b02da66d0f0128ec721974faad979452749cd

[14] https://www.intechopen.com/books/advanced-biometric-technologies/liveness-detection-in-biometrics