SECURITY, PERFORMANCE, ATTACKS & FUTURE TRENDS IN BIOMETRIC SYSTEM: A REVIEW

S. Joyce[1], Dr. S. Veni[2]

ABSTRACT:

Biometric System offers more advantages than Traditional Systems like pin, password, Key, card, Id etc., which can be forgotten or stolen. It is consistent and user friendly. It is a technology where a person is identified based on the physiological or behavioral characteristics. This paper is a review on the Biometrics History, Types and its internal working. The literature survey of various technologies suggests the need to protect Biometric system using watermarking. The Functionality and Recital metrics conditions which satisfies the Biometric system. Its Attacks and techniques to protect the System and recent Trends in the Biometric System.

Keywords: -

Biometrics, Attacks, Watermarking, Biometric Security, Performance Metrics of Biometric System, Least Significant Bit (LSB), Malicious Attacks.

1. INTRODUCTION:

In 1800'-s Alphonse Bertillon, anthropologist and a police assistant developed Bertillonage method for detecting offenders. The dimensions [1] of the body were taken for sorting and assessment purposes. In 1880 Dr. Henry Faulds used thumbprints as a means of Detecting Offenders. In 1897 in India, Edward Henry established the practice of classification of thumbprint ID. In 1902 New York civilian provision they used this Henry method for Army, Navy etc. Henry system is commonly used in all countries. In 2013, Apple and Samsung developed Fingerprint Scanners on their smart phones.

Biometrics is the term derived from the Greek term "bio" meaning lifecycle and "metrics" means quantity. Biometrics authentication in the field of computer science is used for the identity of a person [1]. The old-style means of admission controller includes token-based ID systems, for example, car driver authorization or visa, and knowledge-based ID systems, as a code word or individual ID numeral.

1.1. Biometric Types: -

Biometrics stays divided under physical and behavioral features. Physical features are related to the form of the body like impression, palm veins, face structure, DNA, palm print, hand geometry, iris, retina and odour/scent. Behavioral features are related to the form of behavior of a person such as keystroke, signature and voice.

Table 1. Two Types of Biometrics System

PHYSIOLOGICAL TYPE	BEHAVIORAL TYPE
FACE	KEYSTROKE
FINGER PRINT	SIGNATURE
HAND	VOICE
IRIS	
DNA	

1.2 ARCHITECTURE OF BIOMETRICS SYSTEM:

There are two basic modes in a biometric system: one is verification and the other identification [1]. In verification mode the captured biometric is likened to the template

[1] *Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore.*

[2] *Professor & Head, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore.*

in the database to confirm the identity of a person. It has three steps. As a first step, a model is formed and warehoused in the database.

In the next step, models are coordinated with the reference models. The last step is testing. In verification mode one to one comparison is done. In Identification mode one is compared to many. When a person uses the biometric, it is called Enrollment. The biometric is taken and warehoused in the database. In the initial step, the image is captured using the sensor, it is called as Image Acquisition System.

In the subsequent step, the background noise is removed, and the required structures are taken out. In the fourth step the template is generated, in the fifth the template is warehoused in the database and in the sixth the pattern is coordinated using the matching program. The template is tested in the last step and the concerned biometric is displayed on the device which is the sensor.

1.3 Merits and Demerits of biometric System:

Table 2. Merits & Demerits of biometric system

Merits

Merits	Demerits
Uniqueness, Easy to use.	A user cannot alter them remotely. e.g., fingerprint, iris, voice.[2]
The hacker is near you.	The hacker cannot modify your fingerprint, Iris or voice.
Preventing methods can be used to secure the biometrics system	Hacking methods are available.[3]
Convenient and less time consuming.	Can be expensive and takes more time.
Low cost maintenance	Cost of installation is higher compared to other systems.

1.4.1 Direct Attacks: -

The attack is made easier, since no information about the attack is needed. Some of the attacks are Spoofing, mimicry.

1.4.2 Indirect Attacks: -

The attack is made internally in the biometric system [11]. Some of the attacks are Trojan Horse, Hill climbing, Brute force, Channel Interception and Replay attacks.

The Biometric system has four rudimentary modules. They are: sensor module, Feature Extractor module, matcher module and decision module. The attack can be done in any of these modules.[7]

Some of the techniques [4] used to guard against attacks are Liveness detection, Biometric Cryptosystems, Stenography, Watermarking and Cancellable Biometrics.

2. Literature survey: -

Various technologies are suggested to protect Biometric System using Watermarking. Sushant Kumar, Manu K. Yadav, Reshma Pawar and, Madhuri Patil [8] suggested Asymmetric digital Watermarking approach. The technique used is Biometric Template and, Visual Cryptography is explained. It provides Security and the Image is stored in the database randomly. Christophe Rosenberger [12] applied a template Protection System. The approach used is Evaluation methodology. It uses metrics for testing the performance and robustness of face Recognition Attacks. It also provides privacy and security against the attacks. Anil K. Jain, Karthik Nandakumar and Abhishek Nagar [13] used Biometric Pattern Security. It provides various Biometric Pattern Protection Schemes. The Biometric endures security and matching accuracy.

Komal and, Dr. Chander Kant [5] uses a Digital Watermarking Techniques using Least Significant Bit

[LSB] watermarking. The image is embedded in bit planes. The Biometric template is secured while travelling through a secure network. P. Anitha, K. Narayana Rao, V. Rajasekhar and, Ch. Hari Krishna [14] implemented a Novel Security Architecture. The technique used is Biometric protection watermarking and Visual Cryptography.

The template which is stored in the database can be modified by the attacker. The proposed Biometric Protection System provides security so that the Biometric can be secured from various malicious attacks. Rubal Jain and Chander Kant [11] provides an overview of Attacks in the Biometric system. It reduces the security of the system, to study about the various techniques to overcome these attacks.

3. BIOMETRICS SYSTEM FUNCTIONALITY: -

A biometric system should satisfy the following conditions: - Acceptability [2] (The biometric system which is developed should be acceptable by the user). e.g., Face and Fingerprint accepted biometric rather than Iris Recognition [9], Collectability (It must be easily collected. E.g., passport and immigration.), Circumvention (The action of overcoming a problem or difficulty is called circumvention) E.g. to prevent various attacks in biometric system, Permanence (The biometric system must be stable. All the limitations must be overcome by the biometrics system.), Performance (The accurateness of a biometric is not still. It is prone to various errors). E.g. FTE, FAR and FRR, Universality (It must be present in all the individuals). e.g., fingerprint can have cuts and uniqueness (The biometric system used by an individual must be unique). E.g. Facial of twins can be same.

4. RECITAL METRICS OF A BIOMETRIC SYSTEM: -

In the biometric system the performance [1] is considered as follows: - The False Match Rate (FMR) which is invalid inputs that are in correctly accepted. The False Non-Match Rate (FNMR) also called FRR (False reject rate) is where structure fails to spot a match. The Receiver operating characteristric (ROC) is the Trade - off between FMR and FNMR. The Equal error rate (EER) is when the receipt and Denunciation errors are equivalent [10].

The Failure is to enroll rate used to make a pattern from an input which is ineffective. The Failure to capture rate (FTC), is the biometric input which is presented correctly but the structure fails to spot it. In the Pattern capacity, the number of data groups stored in a system is the True Acceptance Rate (TAR) and is defined as 1-FRR.The Weighted Error Rate (WER) is the subjective sum between FNMR and FMR and the Matching Speed is the Biometric system calculating the time for an individual to be Identified or Verified.

5. FUTURE TRENDS OF BIOMETRIC SYSTEM:

The biometric technology is used in Airfield safekeeping, Structure Admittance, cars, blood banks, institutes etc. Biometrics based on the following have emerged: mind and emotion signals, Operator Signatures, public networks, Animal Biometrics, Mobile based Technology and, cloud-based Solutions. India's nationwide identification package (Aadhaar Package) is one of the ongoing processes and a major record in the world. This Package is done using fingerprint, Iris and face Recognition.

6. CONCLUSION: -

This paper gives a clear review of the Biometric Authentication System, Behavioral and physiological types of Biometric System and, Internal Working of the System. A study on various techniques used in the Biometric System is made as a survey so that the biometric can be well-preserved.

The biometrics can be preserved using various technologies, but even when the technology grows

there are certain problems to be faced. Hence, a clear study can be made so that the veracity and security of the biometric structure can be preserved using several upcoming techniques.

REFERENCES :

1. "Biometrics, From Wikipedia, the free encyclopedia", https://en.wikipedia.org/wiki/Biometrics.
2. "Biometric authentication overview, advantage and disadvantages" https://heimdalsecurity.com/blog/biometric-authentication/.
3. "Biometric security advantages and disadvantages",https://www.slideshare.net/prabhjeet946/biometric-security-advantages-and-disadvantages.
4. Arpita Sarkar and Binod Kr Singh, "A Review on Security Attacks in Biometric Authentication Systems", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 12 | Dec 2018.
5. Komal and Dr. Chander Kant, "An Approach to Enhance Security of Biometric System Using LSB Watermarking", International Journal of Advanced Research in Computer Science, Volume 8, No. 5, May – June 2017
6. Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng and Craig Valli" Security and Accuracy of Fingerprint-Based Biometrics: A Review", Symmetry, received: 2 December 2018; Accepted: 23 January 2019; Published: 28 January 2019.
7. K. Sambasivarao and Mrs. T. Vishnu Priya," Improvisation of Template Protection in Iris Biometric Recognition Using Watermarking Technology", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735.Volume 12, Issue 3, Ver. II (May - June 2017).
8. Sushant Kumar, Manu K. Yadav, Reshma Pawar and Madhuri Patil," Security Using Biometrics Template and Visual Cryptography: A Two-Fold Approach ", International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS), volume 2, Issue 1(Jan-Feb 2015), PP 685-692.
9. Biometrics System Functionality – Javatpoint," https://www.javatpoint.com/biometric-system-functionality.
10. .Biometric Performance Metrics: Select the Right Solution – Bayometric https://www.bayometric.com/biometric-performance-metrics-select-right-solution/.
11. Rubal Jain and Chander Kant," Attacks on Biometric Systems: An Overview", International Journal of Advances in Scientific Research ISSN: 2395-3616.
12. Christophe Rosenberger," Evaluation of Biometric Template Protection Schemes based on a Transformation" ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy, ISBN: 978-989-758-282-0.
13. Anil K. Jain, Karthik Nandakumar and Abhishek Nagar," Biometric Template Security", To appear in EURASIP Journal on Advances in Signal Processing, Special Issue on Biometrics, January 2008.
14. P. Anitha, K. Narayana Rao, V. Rajasekhar and Ch. Hari Krishna," Security for Biometrics Protection between Watermarking and Visual Cryptography", SSRG International Journal of Electronics and Communication Engineering– (ICEEMST'17) - Special Issue- March 2017.