IJFEAT
INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

CRYPTOGRAPHY IN BIOMETRICS TECHNOLOGIES

Simran Rai[1], Sonali Dhalwar[2]
[1]*Student, Computer Science & Engg., Jawaharlal Darda Institute of Engineering &Technology, Yavatmal, Maharashtra, India,* ***simran98rai@gmail.com***
[2]*Student, Computer Science & Engg., Jawaharlal Darda Institute of Engineering &Technology, Yavatmal, Maharashtra, India****, sonali038@gmail.com***

Abstract

Biometrics refers to metrics related to human characteristics. Biometrics authentication (or realistic authentication) is used in computer science as a form of identification and access control Biometrics is seen by many as a solution to a lot of the user identification and security problems in today s networks. Technology that identifies you by "something you are" is showing up in e-passports, laptop login screens, smart firearms and even consumer products like the iPhone.
Biometrics technologies from accuracy perspective? Multimodal biometric systems can fuse these unimodal systems.While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. cryptography-based technologies, presents a new secure cryptographic authentication method using biometric features we can simultaneously achieve the error tolerance of biometric recognition.it can be used to improve the confidentiality of biological data storage and data identification processes.

Index Terms: *Biometrics, Multimodal Biometrics,Authentication, Cryptography.*

--- *** ---

1. INTRODUCTION

Like all new technologies, advances in biometrics will bring new advantages and also new risks. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric identifiers are then distinctive, measurable characteristics used to label and describe individuals.

Proper biometric use is very application dependent. Certain biometrics will be better than others based on the required Biometric Technology has contributed tremendously to boost the advancement in digital electronics. It has made it easier to authenticate a trusted user. More importantly, it has speed up the authentication process and it is 100% secure when multimodal authentication methods are used together. Despite the fact that there exist some drawbacks, it is a boon to the digital world. To understand its significance, you can compare the age old pattern based authentication and one touch finger scan on your smartphoneBiometrics comprises of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. Certain characteristics of every human being such as fingerprint, iris, retina, voice, face, DNA differ from each other. Biometric authentication makes use of these characteristics to identify individuals. In information technology, in particular, biometrics is used as a form of identity access management and access control.

Table-1: Comparison of unimodal and multimodal

Sr.No. Comparison	unimodal biometric system	Multimodal biometric system
1. Basis of senses	this modal implements the single biological senses	It makes use of various biological senses of body
2. Recongnization	Recongnization of single biological senses are take place.	Recongnization of multiple and result comes with majority vote are takes place
3. Robustness	less robust	it is more robust hard to attack

1.1Biometric Technology is also used to identify individuals in groups, thus Biometric characteristics can be divided into two main classes:

1. **Physiological** : This is related to the shape of the body. Examples include fingerprint, face recognition, DNA, hand and palm geometry, iris recognition etc.
2. **Behavioral**: This is related to the behaviour of a person. Examples include typing rhythm and voice. Some researchers have coined the term behaviometrics for this class of biometrics.

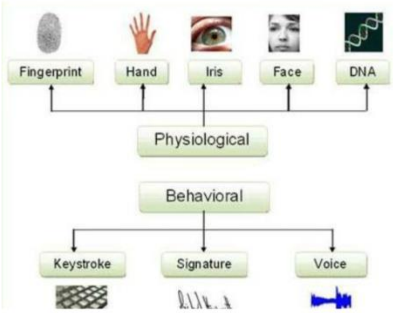

Fig-1:Biometric characteristics

1.2How does the biometric authentication work?

The biometric authentication is a two-step process.

1. In the first step, the biometric information from an individual is captured and stored. This is called the enrollment phase.

2. In the second step, the stored data is detected and compared with the information stored at the time of enrollment. If the data matches then the user is considered to be authentic.

Every biometric authentication process needs a device/sensor to read input samples. This data is called a template. For a single biometric authentication method, thousands of image combinations are generated. Biometrics system makes use of a database storage to store a combination of templates.

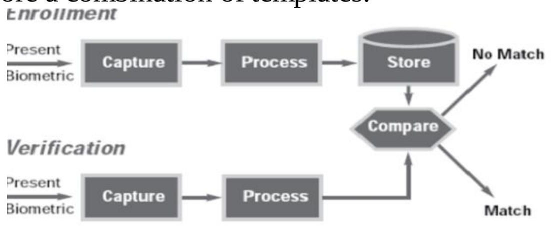

Fig-2:The biometric authentication work

1.3The authentication modes:

In the verification mode , following three steps are involved.

1. In the first step, reference models for all the users are generated and stored in the model database.

2. In the second step, some samples are matched with reference models to generate the genuine and impostor scores and calculate the threshold.

3. The third step is the testing step. This process may use a smart card, username or ID to indicate which template should be used for comparison.

In the identification mode, the system performs a one-to-many comparison against a biometric database in an attempt to establish the identity of an unknown individual.

1.4 Some of the commonly used Biometrics are:

•Fingerprints
•Hand geometry
•Retina
•Iris
•Facial recognition
•Voice

1.5 Some of the disadvantages involved in the Biometric Technology are:

•Security of the biometric data: There is a chance that the thieves will stalk and assault the property owner to gain access. With the increase incybercrimes,attacks such systems must be kept under high surveillance.

• Biometric data cannot be re-issued: If an unusual activity is detected against your account passwords, PINs can be re-issued and your account can be reprotected but in the case of biometrics, you cannot do that. If someones face is compromised from a database, you cannot cancel or reissue it.

•Biological Existing asymmetric encryption algorithms require the storage of the secret private key. Stored keys are often protected by poorly selected user passwords that can either be guessed or obtained through brute force attacks.

2. The trends and reviews which indicate how biometric technology is evolving to make authentication more convenient and secured:

2.1 Cryptography technology:

Cryptography is one of the most important fields in computer security. It is a method of transferring private information and data through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be documents, phone conversations, images or other form of data.

To implement privacy simply by encrypting the information intended to remain secret can be achieved by using methods of Cryptography. The information must be scrambled, so that other users will not be able to access the actual information. For example, in a multi-users system, each user may keep his privacy intact via her/his own password.

2.1.1Authentication Methods:

•APassword authentication protocol:

A password authentication protocol (PAP) is an authentication protocol used by Point to Point Protocol to authenticate users before allowing them access to data resources. Password isthe most common used method in authentication protocols. Whereby, the user should prove his/her username and password by comparing it with the system stored value. This authentication method is important for users since it is easy to be memorized. However, password can be recently classified into two main types; textual password and graphical password.

•Graphical password:

A graphical password is one of the most important fields of authentication in system access control techniques. It allows users to draw or select in the the passwords from images bar, in a specific order. Then the password will be presented in a graphical user interface

(GUI). On other hand, the graphical password is also defined as graphical user authentication (GUA). Therefore, graphical password is considered easier than other password techniques base text, since it is easy to be remembered for most computer users. In term of security, graphical password offers better security than other textual passwords because the graphical password is created by selectable images as a series. These series is normally combined in specific order of images. Therefore, the graphical passwords are recently designed to be resisted to many kinds of attacks such as; shoulder-surfing. Whereas, it will be difficult to recognize the exact images series order (graphical password) by attackers.

•Authentication Token

Is a portable device used for authenticating users thereby it is allowing authorized access into a network system. Authentication technique using a portable device to carry the embedded software that is called software token. There are several token systems, these are: RSA Secure ID Token Crypto cards.

Biometric systems refer to biometric technologies which can be used to achieve authentication. Unlike cryptography-based technologies, the ratio for certification in biometric systems needs not to achieve 100% accuracy. It overcomes repeated use, improper storage, or transmission leaks may compromise security. Prior studies have attempted to combine cryptography and biometrics, but these methods require the synchronization of internal systems and are vulnerable to power analysis attacks, fault-based cryptanalysis, and replay attacks. By adding a subsystem to existing biometric recognition systems, we can simultaneously achieve the security of cryptographic technology and the error tolerance of biometric recognition. This method can be used for biometric data encryption, signatures, and other types of cryptographic computation.

These technologies can be implemented through hardware or software applications and combine biometric systems in current use.

2.1.2How the Cryptography Authentication is used in Biometric Recognition:

Biometric systems refer to the use of biometric recognition technology to authenticate a person’s identity through his or her unique biological characteristics (e.g., fingerprints, palm prints, iris, and personal signature) in lieu of a password. This approach can thus authenticate the user’s identity without requiring the user to remember multiple passwords. This authentication method usually first obtains a threshold range to discriminate between acceptable and unacceptable inputs. However, repeated use, improper storage, or transmission leaks may compromise security.

The difference with cryptographic technology is that these authentication ratios do not need to achieve 100% accuracy. That is, a certain degree of error in data matching is tolerated.

Thebiometric processing methods of the proposed cryptography-integrated technology. The processed values can be directly applied to biometric recognition. This processing mode can be divided into eight parts as follows:

(1) Data collection subsystem
(2) Signal processing subsystem
(3) Biometric feature extraction subsystem
(4) Numerical quantization subsystem
(5) Adjustment subsystem
(6) Hash subsystem
(7) Biometric feature registration/input subsystem
(8) Matching and decision subsystem

2.2 proper guidance while enrolment of finger scan, Iris scans and faces recognazation:

•sweeting on hands, dust on hands, effect of skin health d dryness include age.

•proper distance should be standardised forrecognazation of face and iris.

2.3Auto update method:

An Adaptive biometric System aim to auto-update the templates or model to the intra-class variation of the operational data. The two-fold advantages of these systems are solving the problem of limited training data and tracking the temporal variations of the input data through adaptation.

Recently, adaptive biometrics have received a significant attention from the research community First, with an adaptive biometric system, one no longer needs to collect a large number of biometric samples during the enrollment process. Second, it is no longer necessary to re-enroll or retrain the system from scratch in order to cope with the changing environment. This convenience can significantly reduce the cost of maintaining a biometric system. Despite these advantages, there are several open issues involved with these systems. For miss-classification error (false acceptance)by the biometric system, cause adaptation using impostor sample.

Future scope:

•Biometrics in Healthcare

•College entrance exams

3. CONCLUSION

This technology is getting better every day and spreading globally at a faster rate. We hope for much such advancement in the field of the biometrics.

This systems implements less time complexity as compare to existing systems.Of course, every technology has some drawbacks. We should concentrate on overcoming these drawbacks instead of crushing the technology.

This paper reviews a biometric authentication method with the security of cryptographic technology, simultaneously achieving the functions of cryptographic technology and biometric recognition.

As the reviewed points discussed above in paper are helpful for overcoming the concerned disadvantages of Biometrics system.

ACKNOWLEDGEMENT

It gives us proud privilege to complete this paper on "CRYPTOGRAPHY IN BIOMETRICS TECHNOLOGIES" in under guidance of Prof. A.Kazi.We would also like to thanks all Staff Member of Computer department for timely help and encouragement of fulfillment of work .At last I would like to thanks all my colleague for providing help in my work.

REFERENCES

[1]. www.mistralsolutions.com/new-technologies-biometrics/

[2]. http://www.m2sys.com/blog/mobile-biometrics-2/5-recent-trends-in-biometric-technology/

[3]. https://books.google.co.in/books?id=EIXvDAAAQBAJ&pg=PA349&lpg=PA349&dq=different+concept+about+biometrix&source=bl&ots=rBRrzFchI-&sig=Phx43B9me9snz_0j-tbNWepBnRQ&hl=en&sa=X&ved=0ahUKEwjz84zxnrnWAhUMsY8KHQUmAqYQ6AEIWzAJ#v=onepage&q=different%20concept%20about%20biometrix&f=false

[4]. https://www.techopedia.com/definition/26990/biometric-system.

[5]. M. Scott, "Cryptanalysis of an ID-based password authentication scheme using smart cards and fingerprints," ACM SIGOPS Operation System Review, vol. 38, no. 2, pp. 73–75, 2004.

[6]. https://en.m.wikipedia.org/wiki/Biometrics

[7]. https://www.hindawi.com/journals/bmri/2013/623815/

[8]. https://krazytech.com/technical-papers/biometric-technology

[9]. https://www.tocbiometrics.co.uk