A Survey on Biometric Security Threats and Countermeasure

Aanchal Jindal
IT dept NIEC

Devanshu Pal
IT dept NIEC

Nitish Bhardwaj
IT dept NIEC

Arvind Panwar
Assistant Professor
IT dept NIEC

Abstract

It has been quite a long time since the first biometric systems were introduced and, until present, they have not become widely used. In spite of this, the importance of the biometric security systems is growing now. Many research groups are working on the development of the individual biometric technologies such as the fingerprint recognition, iris or retina recognition or the speaker recognition. However, not many of them combine these technologies together. Future of the biometric security systems is in the combination of more technologies however it cannot be forgotten that we any technology that aims to provide a service for security, biometric systems are exposed to external attacks which would play with their reliability. Thus it is important to analyze the threats to which they are subjected and determine their vulnerabilities in order to prevent plausible attacks and increase their benefits for the users. Forget about PINs and passwords, you are your own key. However we know that every system have some problem and vulnerabilities, biometric system also have the same problem. Before presenting this paper we study biometric system and find some vulnerability which is harmful for the biometric security system. This paper presents a brief survey on biometric this paper is focused assessment of biometric security systems. Although it is relatively young compared to other established and long used technologies for security, biometrics have emerged in the last decade as an attractive alternative to applications where recognition of the people is needed. Certainly, biometrics is very attractive and useful for the final user: system attacks and vulnerability and a classification framework for different attacks on biometric security system which categories all attack of different class.

Keywords: Biometric system, attacks, vulnerability.

1. Introduction

It has been quite a long time since the first biometric systems were introduced and, until present, they have not become widely used. In spite of this, the importance of the biometric security systems is growing now. The biometric security system is a lock and capture mechanism to gain access to stored data. In order to gain access over the biometric security system, an individual must provide their distinctive characteristics or traits which will be matched to the database in the system. If a match is found, the system for locking will provide access to the data for the user. The lock & capture system will trigger and trace information of users who accessed the data. The biometric serves as the key to the biometric security system which server as the lock to provide security. Biometrics-based personal authentication systems that use physiological or behavioral traits (e.g., fingerprint, face, iris, hand geometry, signature, voice etc) of individuals have been shown to be capable candidates for either replacing the traditional systems. Biometric identifiers are the Unique & measurable characteristics which are used to label and depict individuals. Biometric identifiers can be categorized as physiological and behavioral characteristics. Physiological characteristics are related to the shape of the body. The Fingerprint, face, Palm print detection, hand geometry, iris detection, DNA, retina and odor/scent comes under this. Behavioral characteristics are related to behavior of a person, including rhythm, gait, and voice. Traditional means of access control uses token-based identification systems an individual's passport, and knowledge-based identification systems, a password. Since biometric identifiers are inimitable to individuals, they are more trustworthy in verifying identity than token and knowledge-based methods.

There are several basic criterion of security system in biometric systems namely unique, global, permanent, collectability, efficiency in performance, acceptability and circumvention. The following figure explains the various criteria of biometric security and its parameters. The figure 1 highlights basics of biometric parameters

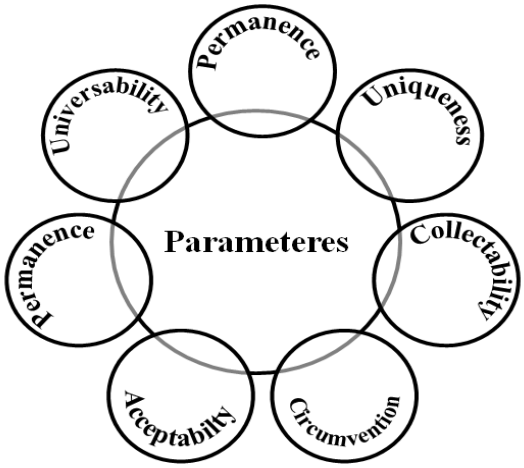

Figure 1 Criteria for biometric security

Uniqueness is taken as the priority one requirement for biometric data. It will show how differently and uniquely the biometric system will be able to identify each user among groups of users. The DNA is unique in each individual and it is impossible to mimic. Universality is the secondary criteria for the biometric security. This factor indicates requirements for unique characteristics of each person in the world, which cannot be simulated. As retinal and iris are characteristics will satisfy this requirement. Thirdly, a permanence factor is required for every solo characteristic or trait which is recorded in the database of the system and needs to be invariable for a certain period of time period. This factor will mostly be affected by the age of the user. Following the permanence factor is the collectability. The collectability factor requires the collection of each characteristic and trait by the system in order to verify their identification. Then, performance is the next factor for the system which outlines how well the security system works. The accuracy and robustness are important factors for the biometric security system. All these factors will decide the performance of the biometric security system. The acceptability factor chooses fields in which biometric technologies are correctly used. Lastly, circumvention will decide how easily each characteristic and trait provided by the user can lead to failure during the verification process. Although it is relatively young compared to other recognized and long used security technologies, biometrics have emerged in the last decade as an attractive alternate to applications where recognition of the people is needed. The term biometric security is used for controlling access to storage units based on physical details. The security has various vulnerabilities which the corresponding attacks. The attacks are classified as following

The brute force attacks try all possible combinations until the require key is found, also known as zero-effort or intrinsic failure. This threat is impossible to prevent and present in all biometric systems. Adversary attacks refers to the possibility that a malicious subject enrolled or not to the application tries to bypass the system interacting with it in a way for which it was not thought .The adversary attacks can be grouped in direct and indirect attacks as follows

Direct attacks are caused when a person tries to mask as someone else by data fallacy and therefore gaining an illegitimate advantage. These threats are aimed directly to the sensor trying to gain access to the system by impersonating a real user.

The figure 2 shows the categories of attack on biometric system

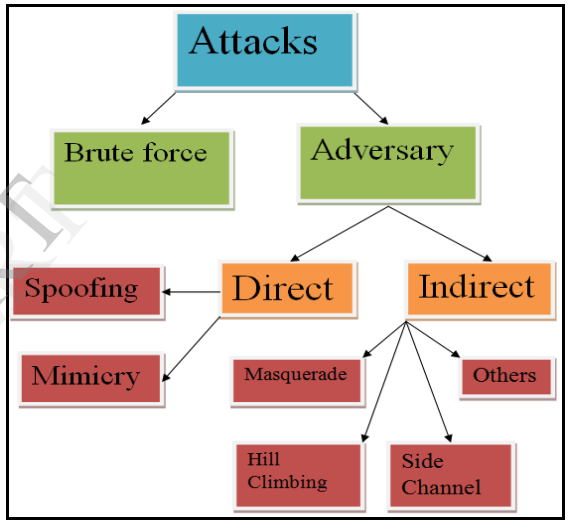

Figure 2 biometric attacks

Indirect attacks are caused due to intruders and cyber criminal hackers. This group carried out using a Trojan horse and can be categorized into masquerade, hill climbing, and side channel. The hill climbing attacks may be performed that sends random template to the system which is perturbed iteratively. The output reads out output match score and continues with the perturbed template only when the matching score increases until the decision threshold is exceeded.

This paper is organized as follows. In last section we explain the need of biometric system in today's world with history of security and future aspects of biometric. In next section we highlight the related work to biometric security in which we have provided a jist of the previous papers and their work in that field. The 3rd section described the research methodology which clarifies how to carry

out this work. In the next section we explain the framework of the biometric security that is design after the study of various research concept and biometric system. The same framework highlights various biometric security systems with their vulnerabilities which led to the exploitation of the different types of attacks. At last, we conclude our paper by mentioning the conclusions and future scope of the foresaid paper.

2. Related work

This section explains the work related to biometric security system. We have focused on vulnerability assessment to both direct and indirect attacks. The aim of this section is not to generate a comprehensive and broad review of the existing publications dealing with the above mentioned field, but to summarize the most significant works closely related to this paper which can ultimately help the reader to make up a general view of the state of art on this matter.

In the past few years, a significant effort has been carried out in analyzing, classifying and solving the possible security breaches that biometric verification systems are presenting [1]. Biometrics-based validation systems use physiological and behavioural traits are good alternatives to conventional methods. These systems are more reliable and more user-friendly . In spite of these advantages of biometric systems over traditional systems, there are many unresolved issues associated with the biometric system. For example, how secure the biometric systems are against attacks? After studied previous research we get the answer of this question and find out that there is also some vulnerability in biometric system. system which used to launch attacks against system. In next paragraph we explain research efforts corresponding to various attacks which try to breach biometric

Brute –force attack widely known as zero-efforts attacks or intrinsic. This threat is impossible to prevent and present in all biometrics systems [2]. The brute force vulnerabilities are inherent to the statistical nature of biometric systems, the biometric community has focused in the study of adversary attacks and classified into eight classes [3]. When the attacks are executed against a biometric system working on physical trait they are also known as spoofing and try to enter the system by presenting a fake biometric trait or artefacts to acquisition device [4].

The brute force vulnerabilities are intrinsic to the statistical nature of biometric systems; the biometric society has focused in the study of adversary attacks and divides it into eight classes [3]. When the attacks are executed against a biometric system working on physical trait they are also known as spoofing and try to enter the system by presenting a fake biometric trait or artefacts to attainment device [4].

Those biometric systems which are based on behavioural these types of approaches are well-known as mimicry, where the attacker tries to break the system by imitating the genuine user producing, called skilled forgeries [5]. The direct attacks threats to type 1 and aimed directly to the sensor trying to gain admission to the system by impersonating a real user[6]. The indirect attacks are also classified in the bibliography in terms of the techniques that may be used to carry them out [7]. The previous paper has furthermore listed out threats that may affect any security appliance, not only based on biometric recognition [8].

The first method of fingerprint attacks on spoofing can be traced to the 1920s, which focuses in photography and depiction to generate gummy fingers from dormant prints [9]. In case of face recognition systems, face photographs of the legimite users have been used to test their strength against direct attacks [10]. Different studies had been concluded to determine the vulnerabilities of signature recognition systems [11]. The previous efforts focuses on fingerprint live detection that initiated a research line using the skin perspiration method [12].Different model based algorithms have been presented in the literature to produce synthetic individuals for biometric traits [13].

3. Research Methodology

This paper presents an overview of biometrics in general and describes some of the issues related to biometrics vulnerabilities and security, and its other side, its prevention. It considers that for biometrics to be publicly accepted, implementations will require cooperation between organizations and individuals, we have to in cooperate certain security measures for its effective working. The following journals are studied in the preparation of its security:

- ELSEVIER
- IEEE
- ACM
- Science Direct
- IJBM

The paper first listed out the types of biometric; among them we have focused only on 7 or 8 types. The various types under consideration are explained in detail, then their respective vulnerabilities. This led to corresponding attacks. The attacks are classified into brute force and adversary which is further classified into direct and indirect. The paper also highlights the various security threats to the biometric and instead of having these threats, we have concluded with the solution.

	In Favor	Opp-osed	Declined To Response
Use of facial recognition to scan for suspected terrorists at various locations and public events	86%	11%	2%
Closer monitoring of banking and credit card transactions to trace funding sources	81%	17%	2%
Adoption of a national ID system for all U.S. Citizens.	68%	28%	4%
Expanded camera surveillance on streets And public places.	63%	35%	2%
Law-enforcement monitoring of Internet discussions in chat rooms and other forums	63%	32%	5%
Expanded government monitoring of cell Phones and e-mail to intercept messages.	54%	41%``	4%

Table 1 survey results of America

We have also provided the polls results conducted by the united state of America conducted in favour of biometric security which shows that biometric is encouraged in spite of having various threats after one week which enhances the future scope of biometric security. We conclude research by providing the solutions to biometric security. The table 1 highlights the poll results conducted by united state of America

4. Categorised Framework

The following framework classifies the types of biometrics, their related vulnerabilities. These vulnerabilities led to various types of attacks which are again bifurcated into direct and indirect. The framework shows the possible solution and prevention regarding the various security threats. The figure 4 explains the basic framework of biometric security, its vulnerabilities and their attacks.

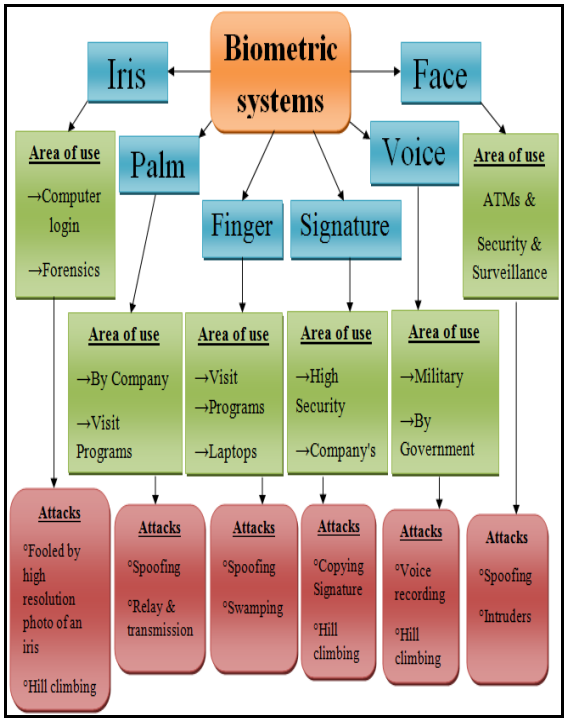

Figure 4 framework

4.1. IRIS

Iris, a biometric that provides one of the most safe and sound methods of authentication and classification thanks to the unique distinctiveness of the iris. Once the image of the iris has been captured using a normal camera, the authentication process, involves comparing the current subject's iris with the stored version, is one of the most suitable with very low fake acceptance and rejection rates. In these attacks, synthetic random minutia template is pre-executed to the input of the matcher and according to score generated; it is repeatedly changed until the system returns a positive verification. Iris is used widely in biometric system .Some of the applications are Physical Access, Information Security & Authentication Server. Though having such vast applications, the following biometric type is threatened by certain vulnerabilities and their respective attacks.

The security problem of spoofing are attacking the physical iris, using artefacts & attacking the fallback system. The name of the attack on iris biometric system is Hill climbing attack. This attack can be prevented by limiting the number of trials & by giving out those results which answer only yes or no. The proposed solution takes advantage of appropriate enhancements of iris Templates and relies on appropriate data alteration within the image space resulting in significant changes of the resulting code in the iris feature space.

4.2. FINGER

Fingerprinting or finger-scanning technologies are the oldest of the biometric sciences and utilize unique features of the fingerprint to verify or identify the identity of individuals. Finger-scan technology is the most commonly used biometric technology, used widely in physical access and logical access applications. All fingerprints have typical characteristics and patterns. A normal fingerprint pattern is made up certain of lines and spaces. Between them, Finger going rough with time, which is more difficult for machinery to identify accurately the needed for anxiety and conviction of criminals, identification of individuals, fingerprints for employment or licensing applications. In-spite of providing such useful advantage to the various systems and offices, the fingerprint biometric is exposed to vulnerabilities and attacks.

Finger print scanners can easily be spoofed with play-doh, gummy bears & Swamping. Swamping can be prevented by normalizing the number of minutiae. The solution is of not revealing the matching score and by just outputting the accept/reject decision may not be appropriate for certain biometric systems, where the matching score is necessary outside the matcher. In quantizing the revealed matching scores is shown to increase the time needed for positive identification, hence decreasing the feasibility of the attack. Another solution is to reveal the matching scores after they pass a masking procedure: with the constraint of not alternating the matching result (accept or reject), outputting randomly generated scores outside the matcher breaks the correlation between the attack data and the scores, hence resulting in attack algorithm drifting around in the search space and not reaching the portion of it that guarantees positive identification

4.3. FACE

A facial recognition system stems from a purpose-built blend of high-end hardware components and capable software to automatically verify or identify a person from a digital image, as necessary in several Security and Surveillance installations. The identification process is done by comparing the facial traits. It can be used as in ATM's as security measures. The problem associated with it are attacking the communication, compromising the template and attacking the fallback system.

The problems associated with it are attacks on intruders and spoofing. This attack can be prevented by limiting the number of trials & giving out only yes/no. The face based systems can be modified in illumination direction and/or face pose variations. More than one biometric system is used in multi modal systems

4.4. PALM

Palm vein image is captured by special kind of sensor. When reflection process takes place,, illumination also occurs in palm with the help of infrared rays and captures the light given off after transmission through the palm. The deoxidized haemoglobin level in palm vein absorbs the infrared rays which cause the palm vein to appear as a black pattern .This vein pattern is then confirmed against preregistered pattern to authenticate the human. The possible problems regarding palm are ineffective communication, compromising the template and attacking the fallback system.

The possible attacks are spoofing, replay and transmission. It can solved by multimodal biometric system or by biometric combined with password and watermarking. Cryptography is one of the most feasible solutions that would allow us to better guard against replay and database attacks.

4.5. VOICE

Voice recognition is "the tools by which words, sounds or phrases spoken by humans are transformed into electrical signals, and these signals are then changed into coding patterns to which a specific meaning is assigned and credentials of person has been permitted. A person's voice can be easily recorded and used for unsanctioned PC or network. It has low accuracy & any sickness such as a cold can change a individual's voice, making absolute identification difficult or not viable. Although having various field of advantage, it has some security threats associated with it.

Hill climbing is a threat in which one can repeatedly submit biometric data to an algorithm with slight differences & maintain modifications that result in an improved score. This attack can be prevented by limiting the number of trials & giving out only yes/no. Victrio is one of the most popular technology used in voice detection and correction rather than authenticates the customer, it also keep a tab of registered voce.

4.6. SIGNATURE

The signature verification is the behavioural attribute of biometrics and is used to authenticate a person. A signature verification system generally consists of various parts such as data acquisition, pre-processing, feature extraction and verification. The security problem in signature recognition is hill climbing in which one can repeatedly submit biometric data to algorithms with slight differences & preserve modifications that result in an improved score and then this security can be compromised.

This attack can be prevented by limiting the number of trials & giving out only yes/no. encryption of palm print images in the database is done when security and privacy of palm print database is required using cryptography

5. Conclusion and future work

Traditional personal authentication systems are based on knowledge (e.g., password,keys) or physical tokens (e.g., ID card,) are not able to gather strict security performance requirements of a number of modern applications. These applications make use of computer networks which affect a mass population, and control financially valuable and privately related tasks . Biometrics-based authentication systems use physiological and behavioural traits (e.g., fingerprint, palm, and signature) are good alternatives to traditional methods. These systems are more reliable (biometric data cannot be misplaced, forgotten, or guessed) and more user-friendly. In spite of these advantages of biometric systems over conventional systems, there are various unsettled issues associated with the biometric systems. For instance, how secure the biometric systems are against attacks? How can we guarantee the integrity of biometric templates? How can we use biometric components in conventional access control frameworks? How can we combine cryptography technology with biometrics systems to increase overall security? In this paper we try to get respond of all these type of question about biometric security system. This paper presents a classified framework of different types of attacks which can launch on biometric security and vulnerabilities of biometric system that can be exploited by the attacker. As far as concerned future work of this paper we are currently working an alternative solution of present biometric system, which will be more secure from current system. .The alternative solution all these types of attacks and vulnerabilities will be minimized

6. References

[1] A. Adler, *"Handbook of Biometrics*," chapter: *Biometric System Security*", pages 381-402 Springer, 2008

[2] A.K. Jain, A.K,.Nandakumar et.al. ,"*Biometric Template Security*," EURASIP Journal on Advances in Signal Processing, special issue on biometrics, 2008a

[3] H.ratha, J.H.Connell et.al," *An Analysis of Minutiae Matching Strength*," In proceeding of IAPR Audio-Video-Based Person Authentication (AVBPA), pages 223-228. Springer LNCS-2091, 2001a

[4] M.Lane and L. Lordan, "*Practical Techniques for Defeating Biometric Devices*," Master's Thesis, Dublin City University, 2005

[5] A. Eriksson and P. Wretling," *How Flexible is the Human Voice*, "In proceeding of European Conference on Speech Technologies (EUROSPEECH), pages 1043-1046, 1997

[6] S. Schuckers," *Spoofing and Anti-spoofing Measures*," Information Security Technical Report, 7:56-62, 2002

[7] N.K. Ratha, J.H. Connell et.al," *Enhancing Security and Privacy in Biometrics-based Authentication System,*" IBM Systems Journals, 40:614-634, 2001b

[8] D. Maltoni, D.Maio et.al*," Handbook on Fingerprint Recognition*," Springer, 2003

[9] A.Wehde and J.N. Beffel," *Fingerprints can be Forged*," Tremonia Publish Co., 1924

[10] L. Thalheim and J. Krissler," *Body check: Biometric Access Protection Devices and Their Programs Put to the Test*," C't Magazine, pages 114-121, November 2002

[11] J.Hennebert, R.Loeffel, et.al, "A *New Forgery Scenario Based on Regaining Dynamics of Signature*," In proceeding of. IAPR International Conference on Biometrics (ICB), pages 366-375

[12] R.Deraksshani, S. Schuckers et.al," *Determination of Vitality from Non-invasive Biomedical Measurements for Use in Fingerprint Scanners,"* Pattern Recognition, 36:383-396, 2003

[13] J. Cui, Y. Wang et.al," *An IRIS Image Synthesis Method Based on PCA and Super-Resolution,*" In proceeding of IAPR International Conference On Pattern Recognition (ICPR), pages 471-474, 2004