ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 3, March 2016

Vulnerability of Biometric Authentication System

Ekwonwune Emmanuel, Nwabueze[1], Dominic Edebatu[2], Nwachukwu Catherine Ada Ngozi[3]

Department of Computer Science, Imo State University, Owerri, Nigeria[1]

Department of Computer Science, Nnamdi Azikiwe University, Awka, Nigeria[2]

Department of Computer Science, Federal Polytechnic, Nekede, Owerri, Nigeria[3]

ABSTRACT: Biometrics is a means of identifying somebody or an electronic system through some measurable, behavioral or biological characteristics such as fingerprints, voice or iris, patterns, a password etc for the singular aim of distinguishing between a specific individual and an impostor. In computer technology, biometrics relates to identity confirmation and security techniques that rely on measurable, individual biological features that recognize or verify the identity of individuals through automated means. This paper is motivated by the fact that some traditional authentication methods as mentioned above might not be sufficient to combat identification (ID) theft or ensure adequate security. For example, password could be easily forgotten, lost, guessed or stolen. Again, the Biometric System may also fail to operate as intended due to manipulations by adversaries. Thus, the objective of this work is to examine the Biometric Authentication System vulnerabilities and attack which may come in form of intrinsic limitation, adversary attacks, Biometric Encryption. The methodology used involved steganographic and water making techniques and cancelled Biometric Techniques. It was found that spoofing attacks are major threat to Biometric Systems and Liveness detection are vulnerable.

KEYWORDS: Security, Biometric Authentication, Verification, Vulnerability, Attacks

I. INTRODUCTION

Generally, there are three levels of computer identification/authentication security schemes: According to Microsoft Encarta [1], Level 1 relies on something a person carries, such as an ID badge with a photograph or a computer cardkey, magnetic or chip card. Level 2 relies on something a person knows, such as a password or a code number or PIN. Level 3, the highest level, relies on something that is a part of a person's biological or physiological makeup or behavior, such as a fingerprint, a facial image, or a signature upon which biometrics is based. Thus, Biometrics is therefore the use of physiological and/or Behavioral characteristics to recognize or verify the identity of individual through automated means. Matyas and Riha [2] state that Proper user identification/authentication is an essential requirement for reliable access control and as such is a key enabler for electronic commerce.

Biometric systems can be used in two different modes. One is Identity Verification (one-to-one comparison or authentication), which occurs when the user claims to be already enrolled in the system as he presents an ID card or login name; in this case the biometric data obtained from the user are compared to the user's data already stored in the database. Another is Identification (search, recognition or one-to-many comparison), that occurs when identity of the user is unknown. In this case, the user's biometric data are compared against all records in the database as the user can be anywhere in the database or might actually not have being there at all. Authentication is typically a pre-requirement of authorization (to log in, to access files, to enter an aircraft, etc.). While biometric authentication is attractive because it principally authenticates the user and not something that can be disclosed or passed to a colleague, its shortcomings relate to problems with accuracy, privacy protection, secrecy of the biometric data and therefore the need for a reliable testing. Before a user can be successfully verified or identified by the system, he must be registered with the biometric system as his biometric data are captured, processed and stored in the database.

In the opinion of Matyas and Riha [3], there are basically two kinds of biometric systems:

(a) 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

DOI:10.15680/IJIRSET.2016.0503006

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.

(b) 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.
Note that the involvement of a human factor in (a) above enormously encourages reduction in the problems of the latter type of system or (b) type.

Dynamism of Biometric Data: It is often suspected that most biometric data are not secret. Photos, fingerprints and other biometric data can be more-or-less easily obtained by a targeted attack. Therefore security of any system cannot be fully based on the secrecy of biometric data. Having said that, Matyas and Riha [3], believe that we had to admit that the acquisition of the biometric data was a factor that could make overall attack more expensive in terms of time, money and/or effort. Therefore the use of biometric data as an additional security factor could have a security value in some cases. The secrecy of biometric data relates to ease of covert and overt acquisition of such data and to the diversity of such data in separate instances of biometric systems. According to them, there were natural differences between the various biometric techniques, which they described as being Particular.
Parvathi [4] states that every Biometric System consists of four basic modules as shown below:

i. Enrollment Unit: The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual’s biometric characteristic to produce its digital representation.

ii. Feature Extraction Unit: This module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

iii. Matching Unit: This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user’s master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values.

iv. Decision Maker: This module accepts or rejects the user based on a security threshold and matching score.

II. RELATED WORK

Anil and Karthik [5], are of the view that biometric system first records a sample of a user’s biometric trait using an appropriate sensor for example, a camera (for the face) during enrollment. It then extracts salient characteristics, such as fingerprint minutiae (details), from the biometric sample using a software algorithm called a feature extractor. The system stores these extracted features as a template in a database along with other identifiers such as a name or an identification number.

According to Anil and Karthik [5], to be authenticated, the user presents another biometric sample to the sensor. Features extracted from this sample constitute the query, which the system then compares to the template of the claimed identity via a biometric matcher. The matcher returns a match score representing the degree of similarity between the template and the query. The system accepts the identity claim only if the match score is above a predefined threshold.

Jain and Karthic [5], believed that the irrefutable link between users and their biometric traits had triggered valid concerns about user privacy, in which case, knowledge of the biometric template information stored in the database can be exploited to compromise user privacy in many ways. Template protection schemes, according to them could mitigate this threat to some extent, but many thorny privacy issues remained beyond the scope of biometric technology, which included:

a) Who owns the biometric data; the individual or the service providers?

b) Will the use of biometrics be proportional to the need for security in a given application? For example,
Should a fingerprint be required to purchase a hamburger at a fast food restaurant or access a commercial website?

c) What is the optimal tradeoff between application, security and user privacy? For example, should governments, businesses, and other entities be able to use surveillance cameras at public spaces to covertly track benign activities of users?

They believe that biometric recognition provides more reliable user authentication than passwords and identity documents, and is the only way to detect duplicate identities. While biometric systems aren’t foolproof, the research community has made significant strides to identify vulnerabilities and develop measures to counter them.

Some of the biometric techniques include the following: Facial Systems, Infrared Facial Systems, Fingerprint Systems, Iris Based Systems, Voice Based Systems, Sub-skin biometric characteristics, Retina Based Systems.

Finger print use image of ridge patterns on finger tips or hand palms [6]. Biometric system use live finger print and scanners for fingerprint acquisition but people leave fingerprint on anything they touch.

Biometric Encryption: In the views of Matyas and Riha [2], the idea of cryptographic keys derived exclusively from biometric data bore some very attractive advantages. For example, the keys being used only with the rightful owner present (and being re-generated 'on the fly' then) could be destroyed after use. However, such derived keys also had some unpleasant properties that make them useless in many traditional cryptographic applications [2]. According to them, these types of keys have limited entropy and are created through a deterministic process from non-secret biometric data, and cannot be changed severally though.

In their opinion, invariant features can obviously be extracted from a biometric sample and encoded so that they can be used as encryption keys. The basic problem with this concept is that such keys cannot be treated in the same way cryptographic keys are usually treated. *Here, we shall again, stress the fact that biometrics are not secret*. Other factors may include the volume of data that is truly invariant over time and the problems with changing one's key as soon as the data subject actually finds out that his fingerprint has been disclosed. Moreover, a damaged fingerprint would disable any operations with the derived key [2].

A. Entropy of Biometric Characteristics: while unprocessed biometric samples have the size of kilobytes or megabytes (e.g., the scan of a hand palm in a high resolution), the entropy of the repeatable invariant biometric features is much smaller. The estimation of the entropy of biometric characteristics has recently become an area of active research [2]. The entropy estimates cannot evaluate the entropy of general biometric samples, but are specific for biometric modality (fingerprints) and the particular features used for identification (fingerprint at minutiae or details). It should be noted that it is hard to pin down the entropy in a precise way

B. Secrecy and Changeability of Biometric Data*:* According to Matyas and Riha [2], important properties of cryptographic (symmetric and private asymmetric) keys include *secrecy of the keys and changeability after a key compromise*. As we have discussed above, biometric data are neither secret nor changeable. This means that 'keys' derived by publicly available algorithms from non-secret data cannot be considered secret and do not fulfill this critical requirement of cryptographic keys. They maintained that to improve secrecy of the resulting data, they are of the view that we can either make the algorithm secret (but security-by-obscurity is not a good design principle) or make the result a function of not only the biometric data, but other secret data as well (password or secret key). Then the biometric data are only one of several authentication factors.

III. BIOMETRIC SYSTEM VULNERABILITIES

Anil, Ross and Karthik [7], are of the view that a biometric system is vulnerable to two types of failures, as Figure 1 shows. A denial of service, which occurs when the system doesn't recognize a legitimate user, while an intrusion refers to the scenario in which the system incorrectly identifies an impostor as an authorized user. While there are many possible reasons for these failures, they can be broadly categorized as intrinsic limitations and adversary attacks. Intrinsic Limitations: Anil, Ross and Karthic [7], maintain that unlike a password-based authentication system, which requires a perfect match between two alpha-numeric strings, a biometric-based authentication system relies on the similarity between two biometric samples. Because an individual's biometric samples acquired during enrollment and authentication are seldom identical as Figure 3 shows, [7] a biometric system can make two types of authentication errors:

The first is false non match which occurs when two samples from the same individual have low similarity and the system can't correctly match them.

Anil et al [7], further stressed that false non match leads to a denial of service to a legitimate user, while the second is false match which can result in intrusion by an impostor. Because the impostor needs no expert, any special effort to fool the system; such an intrusion is known as a zero-effort attack.

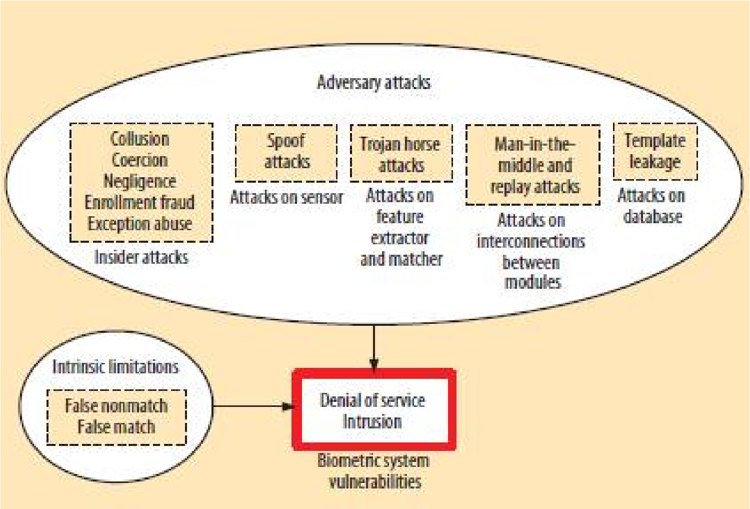

Figure 1. A biometric system is vulnerable to denials of service and intrusions, which can be caused by both intrinsic limitations and adversary attacks.

Source [5]

Rival Attacks: A biometric authentication system may disappoint as expected as a result of to manipulation by rival. Such manipulations, according to Jain and Karthik [5], can be carried out via insiders, such as system administrators, who may be directly attacking the system infrastructure. They believe that an adversary could circumvent a biometric system by coercing or colluding with insiders, exploiting their negligence (for example, failure to properly log out of a system after completing a transaction), or fraudulently manipulating the procedures of enrollment and exception processing, originally designed to help authorized users. Jain and Karthik [5], said that External adversaries could also cause a biometric system to fail through direct attacks on the user interface (sensor), the feature extractor and matcher modules, the interconnections between the modules, and the template database.

Examples of attacks targeting the system modules and their interconnections, according to [5] include: Trojan horse, man-in-the-middle, and replay attacks. As most of these attacks are also applicable to password-based authentication systems, several counter measures like cryptography, time stamps, and mutual authentication are available to prevent them or minimize their impact.

They showed that two major vulnerabilities that specifically deserved attention in the context of biometric authentication

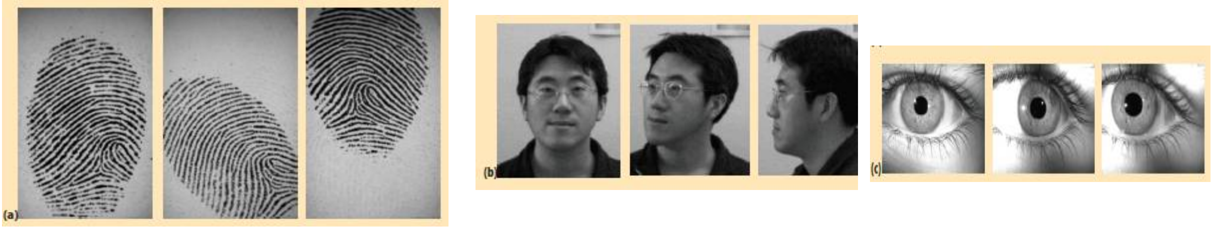

Figure 2. Inherent variability between biometric samples of the same individual. (a) Variations in fingerprint patterns of the same finger due to differences in finger placement on the sensor. (b) Variations in face images of the same person due to changes in pose. (c) Variations in iris images of the same eye due to differences in pupil dilation and gaze direction.

DOI:10.15680/IJIRSET.2016.0503006

Source [5]

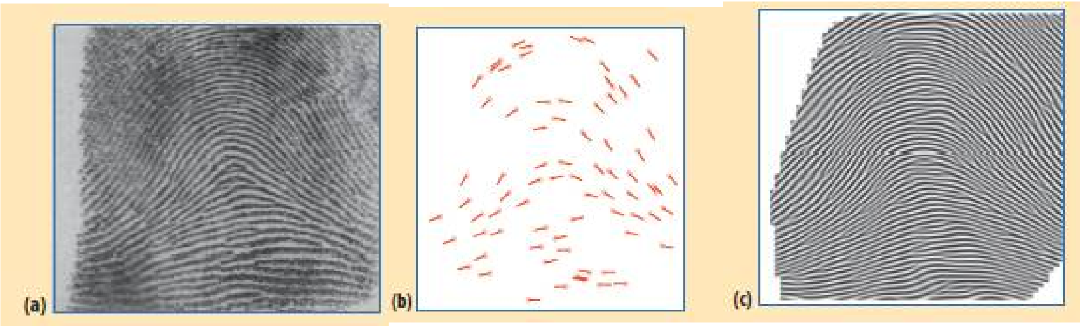

Figure 1. A biometric system is vulnerable to denials of service and intrusions, which can be caused by both intrinsic limitations and adversary attacks.

Source [4]

are spoof or counterfeit or mock attacks at the user interface and template database leakage and these attacks have serious adverse effects on biometric system security. A spoof attack involves presenting a counterfeit biometric trait not obtained from a live person. Examples of spoofed biometric traits include a gummy finger, photograph or mask of a face, or dismembered finger from a legitimate user. A fundamental tenet of biometric authentication is that even though biometric traits aren’t secrets, it may not be very difficult to covertly obtain a photo of a person’s face or the fingerprint pattern from an object or surface touched by a person.

These researchers have developed numerous live detection techniques. For example, verifying the physiological properties of human fingers or observing involuntary human actions like blinking of the eye, which ensure that the biometric trait captured by a sensor indeed comes from a live person.

Drawbacks of Biometric Authentication: According to Fustier and Burger [8], the first drawback of biometric authentication was that some methods couldn’t work for some people. For example, it was impossible to use fingerprint authentication for someone who had no hands. Some behavioral authentication method couldn’t work, if something was changed from its initial state. For example, if you had new shoes, perhaps your gait would change, and can be a problem to authenticate you.

They further maintained that if your finger was severely hurt, the fingerprint authentication would not work and also some characteristics as your face could also change with age. Again, most of the biometric authentications systems were still in the developing states then and it could be very expensive to install them. Someone could fool the biometric authentication. Some biometric authentication systems were not really user–friendly as in DNA or retina recognition. It could be also not very clean. It is possible that users might not want to use such system.

Fustier and Burger, [8] opined that Biometric authentication also raised the problem of respect for privacy pointing out that it was worrying, if one’s fingerprints were asked for everywhere that one wanted to go or if every time that one speaks, someone could identify one by analyzing one’s voice. Thus, using biometrics should be a choice for a user and not an obligation. Laws, according to them, had to be done in order to limit the use of biometrics information in a reasonable way.

Attacks on a Biometric System: Ratha et al [9], believed that there were eight points in a generic Biometric System which could be attacked as shown below:

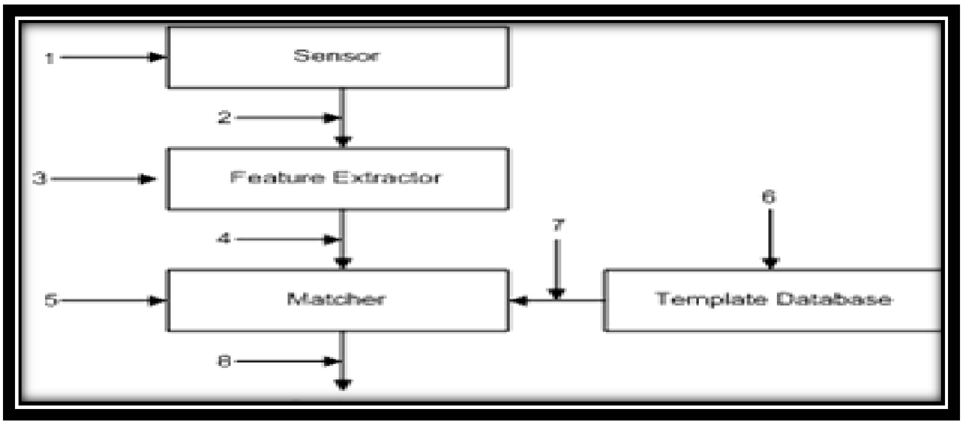

Figure 4: Attack Points in a Biometric System.

Source [9]

I. Attacking the Sensor: In this type of attack a fake biometric such as a fake finger or image of the face is presented at the sensor.
II. Resubmitting Previously Stored Digitize Biometric Signals: In this mode of attack a recorded signal is replayed to the system bypassing the sensor.
III. Overriding the Feature Extractor: The feature extractor is forced to produce feature sets chosen by the attacker, instead of the actual values generated from the data obtained from the sensor.
IV. Tampering With the Biometric Feature Representation: The features extracted using the data obtained from the sensor is replaced with a different fraudulent feature set.
V. Corrupting the Matcher: The matcher component is attacked to produce pre-selected match scores regardless of the input feature set.
VI. Tampering With the Stored Templates : Modifying one or more templates in the database, could result either in authorizing a fraud or denying service to the person, associated with the corrupted template. A smart card based system where the template is stored in the smart card is also vulnerable to this form of attack.
VII. Attacking the Channel Between the Stored Template and the Matcher: Data traveling from the stored template to the matcher is intercepted and modified in this form of attack.
VIII. Overriding the Final Decision: Here the final match decision is overridden by the hacker disabling the entire authentication system [9].

IV. TECHNIQUES THAT RESIST BIOMETRIC SYSTEM ATTACKS

Steganographic and Watermarking Techniques: These measures are used to resist attacks at the attack points 2 and 7 in figure 5. Steganography, which means secret communication, involves hiding critical information in unsuspected carrier data, can be suitable for transferring critical biometric information from a client to a server. In the views of Jain and Uludag [10], there are two application scenarios where hiding method is the same, but differs in the characteristics of the embedded data, host image and medium of data transfer as shown below:

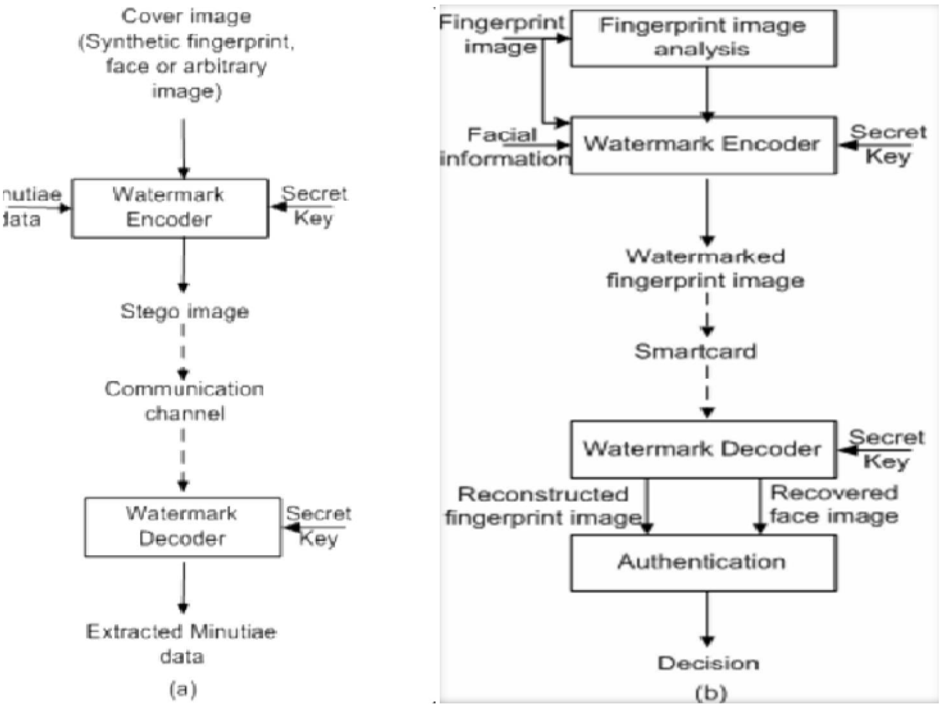

Figure 5: Steganographic (a) and Watermarking (b) techniques

Source [4]

In the first scenario the biometric data that need to be transmitted is hidden in a host or carrier image whose only function is to carry the data. The carrier image can be a synthetic fingerprint image, a face image or any arbitrary image. These experts [10], maintain that using such a synthetic image to carry actual fingerprint data provides good security since the person who intercepts the carrier image might treat that image as the real fingerprint image. The security of transmission can be further increased by encrypting the stego image before transmission.

In the second scenario an additional biometric (e.g. Face) is embedded into another biometric (e.g. Fingerprint) in order to increase the security of the latter and stored on a smart card. At the access control site, the fingerprint of the person is compared to the fingerprint on the smart card. Then the face information hidden in the fingerprint is recovered and used as a second source of authenticity either automatically or by a human in a supervised biometric application. Ratha et al [9] propose a water marking technique applicable to fingerprinting images compressed with WSQ wavelet-based scheme.

According to Ratha et al [9], when the image is received by the service provider, it is decompressed and the image is checked for a one-time verification string. Here, the message is not hidden in a fixed location, but is deposited in different places on the structure of the image so that it cannot be easily recovered. Spatial domain water marking methods for fingerprint images and utilizing verification keys are also available. Water-marking the information in the biometric template database allows for the integrity of the contents to be verified when retrieved for matching.

Cancelable Biometrics: Cancelable biometrics can be used to resist attacks at point 6 (template database). Cancelable biometrics involves an intentional repeatable distortion of a biometric signal based on a chosen noninvertible transform [8]. This reduces the stored template compromise by using the legitimate substitution of a transformed version of a template for matching against a similarly transformed vector. *Cancelable biometrics also addresses the issue of non replaceability of biometric systems.* Here, cancellation simply requires the specification of a new distortion transform. The distortion transforms selected are non-invertible so that the original biometric cannot be recovered even if the transform function and the transformed biometric data are known.

Liveness Detection Mechanisms: Liveness detection can be used to thwart the attacks at attack point: 1(attacking the sensor). Liveness detection refers to the ability of the system to distinguish between a sample feature provided by a live human being and a copy of a feature provided by an artifact. Liveness detection can be implemented using software or hardware means, thus [5]:

❖ Using extra hardware to acquire life signs like temperature, pulse detection, blood pressure etc for fingerprints and movements of the face for face recognition: Iris recognition devices can measure the involuntary papillary hippos (Constant small constrictions and dilations of the pupil caused by spontaneous movements of the Iris). The drawback is that extra hardware makes the system expensive and bulky.

❖ Using the information already captured to detect life signs: The only researched method is using information about sweat pores. For this, a sensor that can acquire a high-resolution image is required. It is difficult to reproduce the exact size and position of the pores on an artificial mold.

❖ Using Liveness information inherent to the biometric being obtained: For fingerprints, using a side impression near the nail, which has been enrolled earlier, can do this. The advantage is that people do not leave side impressions as latent prints and no major changes in the scanner is needed to acquire this additional information. A system that uses multiple instances of the same biometric can be used for Liveness detection by asking the user to provide a random subset of biometric measurements. For example, left index finger followed by right middle finger [5]. Liveness detection can also be done through challenge-response like passing a small impulse current to the finger and capturing the fingers, response.

V.CONCLUSION

There is no security system that is completely foolproof. Every system is breakable with an appropriate amount of time and money. The techniques used to prevent the attacks help to increase the time, and cost of money. Fingerprints can be easily discovered from touched surfaces and can be copied in a small amount of time using readily available materials. All the liveness detection mechanisms in fingerprint systems can be easily defeated using wafer thin gelatin and silicon artificial fingerprints as illustrated by the Japanese cryptographer, Matsumoto and a student thesis in Linkoping University, Sweden [4]. The Liveness detection in face recognition systems can also be defeated using video clips of faces and playing them back. But it is very difficult to fake the iris and retina systems because they use physiological reactions to changing illumination conditions for Liveness detection. A physical modeling of the eye or implanted iris device will be needed to defeat them which are very hard and expensive.

The primary advantage of biometric authentication methods over other methods of user authentication is that they really do what they should, i.e., they do authenticate the *user*. They do not rely on objects the user carries or something the user has remembered. Biometric authentication methods use the real human physiological or behavioural characteristics to authenticate users. These characteristics should not be duplicable, but it is unfortunately often possible to create a copy that is accepted by the biometric system as a true sample.

Biometric data are not secret and the security of a biometric system cannot be based solely on the secrecy of the biometric characteristics. The server cannot authenticate the person just after receiving her correct biometric characteristics. User authentication can be successful only when the person’s characteristics are fresh and have been collected from the person being authenticated.

REFERENCES

[1] Microsoft Encarta, © 1993-2008 Microsoft Corporation, 2009.

[2] Z. Riha and V. Matyas, “Biometric Authentication Systems”, Faculty of Informatics, Masaryk University, (FIMU) Report Series, 2000.

[3] Z Riha and V. Matyas, “Security Biometric Authentication Systems”, International Journal Of Computer Information System and Industrial Management Applications. ISN 2150-7988 Volume 3 (2011) pp 174 - 184 Dynamic Publishers Inc., USA, 2011.

[4] A. Parvathi, “Security of Biometric Authentication Systems”, 21st Computer Science Seminar SA1-T1-1, 2010.

[5] J. Anil and N. Kathik, “Biometric Authentication System Security and User Privacy”, IEEE Computer Society, 2012.

[6] K. Krishneswari and A. Arumugam, “A Review on Palm Print Verification System”, International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), ISSN: 2150-7988 Vol.2, 2010.

[7] J. Anil, A. Ross and N. Kathik, “Security of Biometric Systems: *Introduction to Biometrics”*, Springer, pp. 259-306), 2011.

[8] A. Fustier and V. Burger, “Internet Security and Privacy (2G1704)”, It – universitetet (KISTA), 2005.

[9] N. Ratha, J. Connell and R Bolle, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Systems Journal, Vol. 40, no. 3.

[10] J. Anill and Uludag, “Hiding Biometric Data, Pattern Analysis and Machine Intelligence”, IEEE transactions on Volume 25, Issue II, 2003.