Biometric Authentication Systems Attacks: Liveness Detection to the Rescue

Osuagwu O.E. [1], Ndigwe Chinwe[2], Eze Irene F.[3], Oladimeji Biodun S[4], Akiene Promise [5]

[1]Department of Computer Science, Imo State University, Owerri
Profoliverosuagwu@gmail.com
[2]Department of Computer Science, Anambra State University, Ulli
[3] Department of Computer Science, Imo State Polytechnic, Umuagwo-Ohaji. Tel 0813291860
[4]Department of Computer Science, Federal Polytechnic, Nekede, Imo State
[5]Department of Computer Science, River State Polytechnic, River State

Abstract

Before current era of security complexities, password alone was enough to protect systems. However, hackers have perfected algorithms to break through data bases protected only by pass words. This has led to extended research towards the deployment of of Biometric Authentication Systems (BAS). Biometric systems are believed to have established trusted potential to provide security for a variety of applications. BAS are nowadays being introduced in many applications and have already been deployed to protect personal computers, Banking machines, credit cards, electronic transactions, airports, high security institutions like nuclear facilities, Military Bases and other applications like border control, access control, sensitive data protection and on-line tracking systems. Like any other security systems, biometrics has its own vulnerabilities and weakness. This paper has identified such vulnerabilities and threats, particularly susceptible to external vulnerabilities of biometric systems and countermeasures (e.g. ***liveness detection****) have been presented here to forestall such attacks and to provoke new research interest in this new field of authentication system.*

Keywords: Liveness, Biometrics, Biometric Systems, Authentication, Verification, Vulnerabilities, attacks, Threats.

1.0 Introduction

Informaton security is the profession that protects the **Confidentiality, Integrity** and **Availability** *(*CIA) of information systems and information services. The CIA triad is the pillar of Information security policies. Confidentiality is synonymous with privacy. It includes measures undertaken to ensure confidentiality are designed to prevent sensitive information from reaching the wrong persons, while ensuring that the right persons get the information: Access must be restricted to those authorized to view the data in question. It is common, as well, for data to be categorized according to the amount and type of damage that could be done should it fall into unintended hands. More or less stringent measures can then be implemented according to those categories. **Integrity** on the other hand involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people. These measures include file permissions and user access controls. Version control may be used to prevent erroneous changes or accidental deletion by authorized users becoming a problem. **Availability is** maintained by rigorously maintaining all hardware , performing hardware repairs immediately when needed and maintaining a correctly functioning operating system environment that is free of software conflicts. It is also critical to be up-to-date with all new software upgrades, provide adequate communication bandwidth and prevent the occurrence of bottlenecks. Fast and adaptive disaster recovery is essential for the worst case scenarios; that capacity is reliant on the extra security equipment or software such as firewalls and proxy servers can guard against downtime and unreachable data due to denial-of-service (DoS) attacks and network intrusions [4]. **Biometric Security Threat** is the prevailing phenomenon of active attack against vulnerability in a biometric Authentication Systems. Threats may be broadly classified as: ***Presentation attacks*** (spoofing), in which the appearance of the biometric sample is physically changed or replaced; ***Biometric processing attacks***, in which an understanding of the biometric algorithm is used to cause incorrect processing and decisions; ***Software and networking vulnerabilities***, based on attacks against the computer and networks on which the biometric systems run; and ***Social and presentation attacks***, in which the authorities using the systems are fooled. To defend against a biometric security threat, a biometric security measure may need be deployed.

Biometrics is the science that considers an individual as a union of different biological processes such as neural, skeletal; dermal that uniquely describes that individual**.** One or more subsets of these processes with higher specificity are used as biometrics in automatic identification systems. Since a biometric identifies an individual from one physiological process, the mapping from a biometric feature space to an individual will not be one to one. Thus, multi-modal biometrics increase precision by considering other highly specific biological traits to limit the bumber of claimants for an identify. Thus, ***Biometric identification systems*** are based on the science of pattern recognition. Acquisition scanning devices and cameras are deployed to capture images, or measurements of an individual's characteristics, and computer hardware and software are applied to extract, encode, store, and compare these characteristics. This process is fully automated, and thus makes decision-making very fast, taking only a few seconds. Depending on the application, biometric systems can be used in one of two modes: ***verification or identification***. Verification, also known as ***authentication*** is used to verify a person's identity "to authenticate that the man who claims to be *Oliver* is indeed *Oliver*". Identification is used to establish people's identity to determine who that individual is [2]. Figure 1 presents five samples of BAS currently in use today:

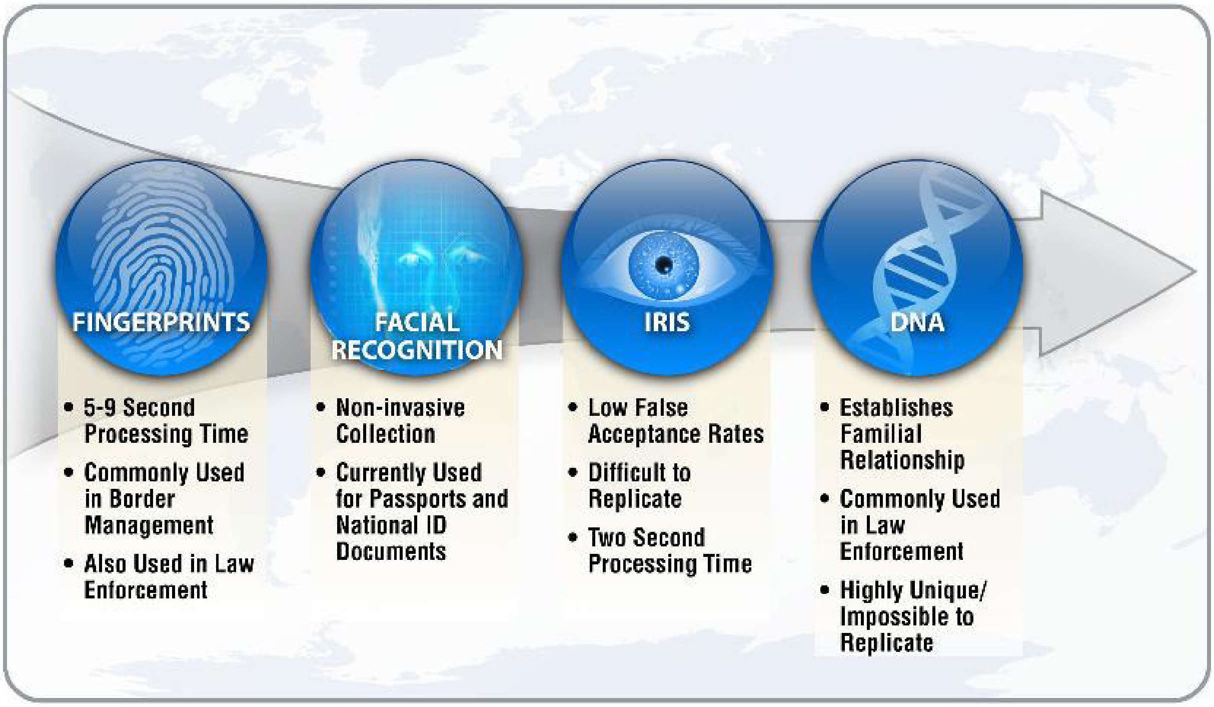
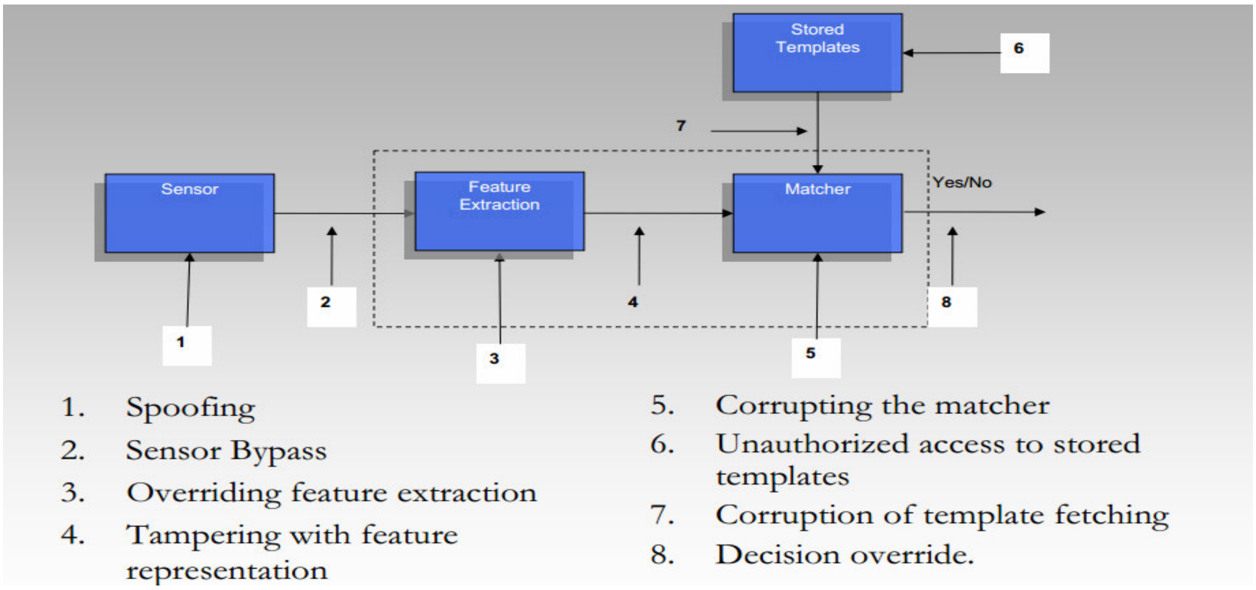

FINGERPRINTS
• 5-9 Second Processing Time
• Commonly Used in Border Management
• Also Used in Law Enforcement
FACIAL RECOGNITION
• Non-invasive Collection
• Currently Used for Passports and National ID Documents
IRIS
• Low False Acceptance Rates
• Difficult to Replicate
• Two Second Processing Time
DNA
• Establishes Familial Relationship
• Commonly Used in Law Enforcement
• Highly Unique/ Impossible to Replicate

Figure **1: Four examples of BAS** [3]

3.0 BAS can develop the problem of false positives, i.e. granting access to the wrong person due to any of the following vulnerabilities: *Spoofing, sensor Bypass, overriding feature extraction, tampering with feature representation, corrupting the* : *matcher, unauthorized access to stored templates, corruption of template fetching* and *decision override* [1]. [1] have identified eight attack points for stand-alone Biometrics shown in Figure 2 below



1. Spoofing
2. Sensor Bypass
3. Overriding feature extraction
4. Tampering with feature representation
5. Corrupting the matcher
6. Unauthorized access to stored templates
7. Corruption of template fetching
8. Decision override.

Figure 2: Eight attack points for stand-alone Biometrics identified by N.K. Ratha et.al. [1]

Explanation of attack points in Figure 2:

1. Spoofing: The word "spoof" means to hoax, trick, or deceive. Therefore, in the IT world, spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

2. Sensor Bypass: This is a technique to deceive the BAS device to accept false positives. The case study bellow illustrates **[7].** Though it might seem secure, this form of biometrics in its various manifestations has been bypassed by some remarkably simple techniques in the past. Security researcher Jan "Starbug" Krissler, from the famous Chaos Computer Club, told FORBES this kind of attack can be carried out against some iris-scanning kit just using high-resolution images found in Google searches. He believes that where photos are vivid and large enough, it's possible to simply print copies of people's eyes and bypass biometric authentication. Krissler, who is employed by Telekom Innovation Laboratories (T-Labs), has history in the biometrics space. In December, *he showed off a "clone" of the thumbprint of German defense minister Ursula von der Leyen* . He'd created the fake print by taking a number of his own snaps of the politician's hand and using commercial fingerprint software from Verifinger to get accurate readings of the minister's unique print. Krissler could then apply a layer of latex milk or wood glue over the top of an inverted image of the print on a transparent sheet to create an accurate clone.

3. Overriding feature extraction: These are already stored features of a BAS system. Overriding implies some tricks is played on the feature to deceive the system to allow access to unauthorized persons.

4. Tampering with feature Representation: Almost related to 3 above. Features may be tampered by hackers to deceive the BAS system.

5. Corrupting the Bas Matcher: The BAS matcher is module in an algorithm that tries to match BAS features presented during authentication with those already stored in the data base. If this module is deliberately tampered with, it will result in passing false positives and this means the system is compromised.

6. If the template are accessed by un-authorized persons, it has the same effect as in 5. It means the BAS system is also compromised.

7. Corruption of the Template Fetching: If the data fetching module in the BAS template is corrupt, the BAS system has failed and it will be fetching false information for comparison.

8. Decision override may occur, if a hacker has succeeded in changing the decision criteria of the BAS system. This will make guinuine decisions to be overtaken by wrong decision. This also implies that the BAS system has been heavily compromised.

In addition to the above possibilities, Biometrics can be faked for instance via:

- A person's finger can be placed in impression material and create a mold.
- Molds can also be created from latent fingerprints by photographic etching techniques like those used in making of PCB.
- play-doh, gelatin, or other suitable material can be used to cast a fake finger.
- Worst-case scenario: dead fingers can also be captured.

4.0 New Countermeasure identified

Liveness detection in multi-modal biometric devices has the potential to enhance security, reliability and effectiveness. Although biometric authentication devices can be susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented that may significantly raise the level of difficulty of such Attacks. Physiologic process of perspiration for instance is used to determine fingerprint vitality. ***It is believed that live fingers, as opposed to cadaver or spoof, demonstrate a specific changing moisture pattern due to perspiration*** [1]. Liveness detection is based on recognition of physiological activities as signs of life via processing the information already captured by biometric reader, from acquisition of life signs by using extra hardware and by introducing challenge-response mechanism and by putting biometric verification, in addition to enrolment, under supervision.

Counter-measures

Supervision of enrolment or verification may include:

- **Liveness Detection**: In biometric systems, the goal of liveness testing is to determine if the biometric being captured is an actual measurement from the authorized, live person who is present at the time of capture. While biometric systems may have an excellent performance and improve security, previous studies have shown it is not difficult to spoof biometric devices through fake fingers, high resolution images or video, contact lenses, etc. Though biometric devices use physiologic information for identification/verification purposes, these measurements rarely indicate liveness. *Liveness detection* reduces the risk of spoofing by requiring a liveness signature in addition to matched biometric information. Methods can include medical measurements such as pulse oximetry, electrocardiogram, or odor. In a few cases, liveness information is inherent to the biometric itself, i.e., the biometric cannot be captured unless the user is live [5]

.

- **Template Anonymization**: Data **anonymization** is a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets, so that the people whom the data describe remain anonymous. Therefore Template Anonymization is the protect personal identity of persons whose information is available on the tempate.

- **Cryptography** (storage and transport): Cryptography is an indispensable tool for protecting information in computer systems. It is the process of writing or reading secret messages or codes. the enciphering and deciphering of messages in secret code or cipher. Microsoft [6] defines cryptography as the ancient science of encoding messages so that only the sender and receiver can understand them. Cryptography is now available to everyone thanks to the development of modern computers, which can perform more mathematical operations in a second than a human being could do in a lifetime. An ordinary PC can produce codes of such complexity that the most powerful supercomputer using the best available attack algorithms would not break them in a million years. Cryptography is used to secure telephone, Internet, and email communication and to protect software and other digital property

- **Traditional Network Security Measures**: e.g. firewalls, ITS, IPS, passwords etc.

- **Challenge Response**: In computer security, **challenge-esponse** authentication is a family of protocols in which one party presents a question ("**challenge**") and another party must provide a valid answer ("**response**") to be authenticated.

5.0 Conclusions and Recommendations

We have successfully presented an emerging security scenario where the vulnerability of BAS has become more apparent requiring new techniques to fight the newly identified weaknesses. Of all the security measures in place today, BAS still remains the most reliable. Yet, it is not waterproof. Several hacker tools and countermeasures have been identified. Most prominent is the infusion of **liveness detection** into BAS authentication systems. This has been found in recent research to increase the precision of specific biological traits which limits the

.

number of claimants for an identity. The previous belief that BAS is impenetrable is now a mirage. Therefore efforts must be made to learn the new technique of **liveness detection** to increase the reliability of BAS in stand alone and networked systems.

References

[1] N.K. Ratha, J.H. Connell, R.M. Bolle, (2009) ***Enhancing security and privacy in biometrics-based authentication systems,*** IBM Systems Journal, VOL 40. NO 3 2001

[2] Abdulmonam Omar Alaswad, Ahlal H. Montaser, Fawzia Elhashmi Mohamad (20140), Vulnerabilities of Biometric Authentication "Threats and Countermeasures"
International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 4, Number 10 (2014), pp. 947-958
© International Research Publications House. http://www. irphouse.com

[3] A Chien Le (2011) ***A Survey of Biometrics Security Systems*** A project report written under the guidance of Prof. Raj Jain. **http://www.cse.wustl.edu/~jain/cse571-11/ftp/biomet/** pulled 7.03.2015

[4] Ndigwe Chenwe, Osuagwu Oliver et.al. (2013) ***Understanding Integrity in Networked Data Base Applications.*** **MicroWave International Journal of Science and Technology, Vol. 5 No.1 pp. 31-44.**

[5] Encyclopadia of Biometrics (2009) p.924

[6] http://research.microsoft.com/en-us/groups/crypto/ pulled 7.3.15

[7] http://www.forbes.com/sites/thomasbrewster/2015/03/05/clone-putins-eyes-using-google-images/