International Journal of Computer Trends and Technology
ISSN: 2231-2803 / https://doi.org/10.14445/22312803/IJCTT-V68I8P106

Volume 68 Issue 8, 39-43, August 2020
© 2020 Seventh Sense Research Group®

Original Article

How Secured is the Securer: Biometric Technology Overview

Omotosho Folorunsho Segun[1], Babalola Moyin Florence[2], Fadiora Babatunde Olawale[3]

[1]*Dept. of Computer Science, College of ICT, Kwara State University Malete, Kwara State, Nigeria.*
[2,3]*Department of Computer Science, Faculty of Science, The Polytechnic, Ibadan. Oyo State, Nigeria.*

Received Date: 30 June 2020
Revised Date: 11 August 2020
Accepted Date: 29 August 2020

Abstract *- To improve the security of real identity management systems, many application now uses biometrics-based personal authentication systems. Biometric physiological traits such as fingerprint, face and iris or behavioural traits such as speech and handwriting are often engaged. As a result of the widespread deployment of biometric systems in many applications, there are growing concerns about the security and privacy of biometric technology. Public acceptance of biometrics technology will depend on the ability of system developers to convince the users that these systems are robust with low error rates and are tamper-proof. This research focuses on likely areas on which biometric systems can be hacked because, unlike passwords and tokens, compromised biometric templates cannot be revoked and reissued. In this study, we present a categorization of various weaknesses points of a biometric system and countermeasure approaches that have been propounded.*

Keywords *- Biometric, Templates, Physiological, Behavioral, Traits, Fingerprint*

I. INTRODUCTION

The Biometric system automatically recognizes the person based on his/her physiological or behavioural characteristics [1]. As the biometric features are distinct to each person, it establishes a direct connection between users and their identity. These systems are easier and more secure as there is no need to remember any password or carry any token to gain access to the applications [3]. Further, Biometric recognition offers a reliable solution to the problem of user authentication in the identity management system. Also, it is fast and easy to use, precise, trustworthy and cost-effective over traditional knowledge-based and token-based methods [2].

A. *Biometric Template*

A biometric template is a set of features extracted from the biometric trait. A template is stored in the biometric system database and is used for matching with the input biometric during an authentication [3].

B. *Biometric systems modes*

Two different modes are involved in the biometric system process–enrollment and verification.

C. *Enrollment*

As shown in Fig. 1, the biometric trait of the individual is captured during the enrollment process, the sensor for fingerprint, microphone for speech recognition, camera for face recognition, camera for iris recognition. The unique features are then extracted from the biometric sample (e.g., image) to create the user's biometric template [3, 7]. This biometric template is stored in a database or on a machine-readable ID card for later use during a matching process.

D. *Verification*

Fig.1 illustrates the biometric verification process. The biometric trait is again captured, and a unique feature is extracted from the biometric trait to create the user's "live" biometric template. This new template is then compared with the stored template previously in the system database, and a numeric matching (similarity) score(s) is generated based on a determination of the similarity features between the two templates [11]. System designers determine the threshold value for this verification score based upon the security and convenience requirements of the system [6].

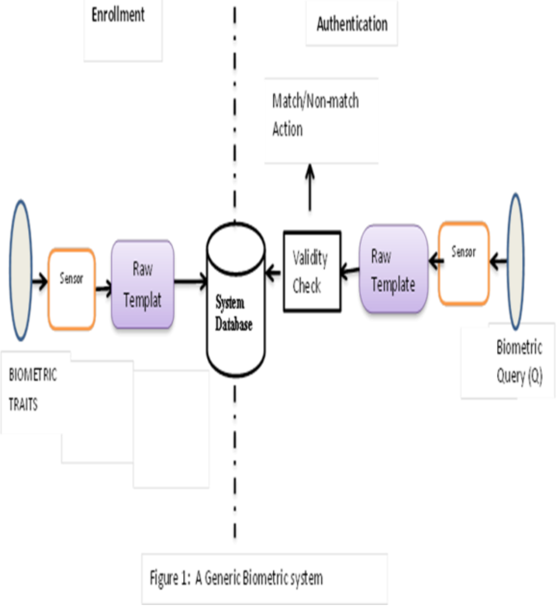

Fig. 1 A generic biometric system

II. RELATED WORK

A. Deployment of Biometric Technology

Despite the advantages of biometrics-based authentication systems compared to traditional authentication schemes, there are still unresolved problems associated with biometric technology [13]. These problems generally emerge from the security characteristics of biometrics-based systems. Here, the term security is used to denote the overall reliability of the system [14]. The mentioned issues below need to be taken into account before arriving at a truly secure biometric system.

One security-related issue is the strength of the biometric systems against attacks specifically targeted to impede their operation. The security analysis of traditional password-based authentication schemes can be based on simple parameters, such as the minimum length of passwords (e.g., minimum of 8 characters), the password change frequency (e.g., at least twice a year), and the complexity of the passwords (e.g., it must include upper and lower case letters, numbers and special characters such as #,&,*) [10].

Biometric systems, on the other hand, are essentially much more complicated than traditional authentication schemes. As a result, there are many critical points in a biometric system that can be compromised, which are naturally absent in traditional authentication schemes [8].

B. *Categorization of the various factors that cause a biometric system failure*.

In this paper, we categorize the various factors that cause biometric system failure and the effects of such. This paper takes note of some necessary points in terms of security threats that have been identified; it also provides a high-level classification of the possible security threats.

At the highest level, the failure modes for the biometric system can be categorized into two classes: intrinsic failure and failure due to an adversary attack [8].

a) Intrinsic failure

Intrinsic failure is due to inherent limitations in the sensing, feature extraction, matching technologies, as well as the limited discriminability of the specific biometric trait. The intrinsic failure occurs when the biometric system takes an incorrect decision during verification. In a biometric verification system, two types of errors may be committed at verification which is false accept and false reject.

b) Adversary attacks

Here, an adversary intentionally stages an attack on the biometric system whose success depends on the loopholes in the system design and the availability of adequate computational and other resources to the adversary. We categorize the adversary attacks into three main classes: administration attack, non-secure infrastructure, and biometric overtness [10].

C. Effects of biometric system failure

When a biometric system is compromised, it can lead to two main effects : (i) Denial-of-service and (ii) Intrusion.

a) Denial-of-service

Refers to the scenario where a legitimate user is prevented from obtaining the service that he is entitled to. An adversary can sabotage the infrastructure (e.g., physically damage a fingerprint sensor), thereby preventing users from accessing the system.

b) Intrusion refers

To an impostor gaining illegitimate access to the system, resulting in loss of privacy (e.g., unauthorized access to personal information) and security threats (e.g., terrorists crossing borders).

D. Susceptibility Points of Biometric System

The most likely attack points can be grouped into eight classes. Fig.2 shows the locations of these attacks in a generic biometric system. A Type 1 attack involves presenting a fake biometric (e.g., finger made from silicon, facemask, lens including fake iris texture) to the sensor [12]. The second type of attack is called a replay attack because an intercepted biometric (with or without the cooperation of the genuine user) data is submitted to the feature extractor bypassing the sensor. In the third type of attack, the feature extractor module is replaced with a Trojan horse program that functions according to its designer's specifications (henceforth, these users that try to break into systems protected by biometric authentication will be collectively called "Trudy"). In the fourth type of attack, genuine feature values are replaced with values (synthetic or real) selected by the attacker. In the fifth type of attack, the matcher is replaced with a Trojan horse program [7, 8]. The attacks on the template database (e.g., addition, modification, or removal of templates) constitute the sixth type of attack. In the seventh type of attack, the templates are tampered with (stolen, replaced, or altered) in the transmission medium between the template database and the matcher. Lastly, the matcher result (accept or reject) can be overridden by the attacker.

- Fake fingerprint
- Replay old data
- Override feature extractor
- Synthesized feature extractor.
- Override matcher
- Modify template
- Intercept the channel
- Override final decision

Eighty (80%) percent of all cybercrimes (an assessment based only on reported security breaches) cases resulted from hackers likely known an authorized user. Personally, a hacker can acquire a sample biometric (for example, a latent fingerprint), can make a duplicate (such as a three-dimensional mould of the fingerprint) and present it to the biometric system.

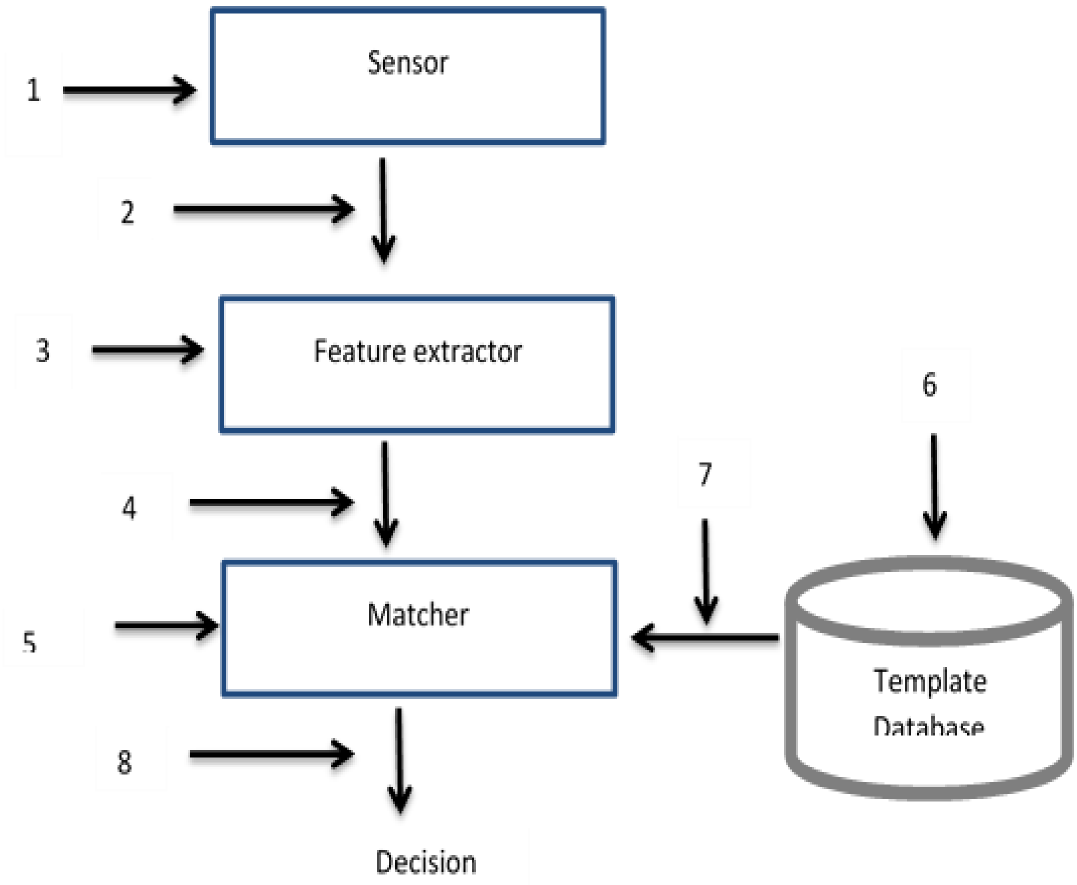

Fig. 2 Locations of possible attacks in a biometric system

Let us analyze this threat. To lift a latent fingerprint, the hacker must know the legitimate user's whereabouts and the surfaces she has touched. Next, the hacker must lift a latent fingerprint of good quality. This is not easy in practice because most latent fingerprints we leave are incomplete, wrapped around irregular surfaces, or partially cancelled by fingers slipping. Then, the hacker has to make an accurate three-dimensional model of the finger.

In fact, a fake biometric attack on a biometric-based network access application presents a much smaller risk than an attack on a password-based system. This is because a hacker could launch an attack against a password-based network access application remotely without knowing any of the users. Also, the hacker could use the same password (for example, a dictionary word) to launch an attack against all the enrolled users at no extra cost.

III. RESULTS AND DISCUSSION

A. Counter Measures to Safeguards against Attack

It has been stated the possibilities of breaking into the biometric system database.

Some of the techniques used for resisting attacks in biometric systems are discussed below:

To alleviate the attack of breaking into the database, a masking operator can be applied to the output matching scores. This masking operator alters the scores randomly without affecting the accept/reject decision, so the matcher does not return the actual matching score between the target template and the synthetic template. Instead, the matcher returns a random score that is smaller than the present decision threshold (i.e., Sthreshold = 12.22) for unsuccessful attempts (for successful attempts, this is noted to mask the scores).

IF the information is leaked from the matcher, the masked score obtained is not the actual score, so the attacker wanders in the search space without actually detecting the matching scores. When the scores are masked, the attacker will find it difficult to break any of the accounts before the maximum iteration number reaches. Masking the scores is most likely an effective way of repelling the attacker.

Another simple but effective solution is to block matching attempts; if there are too many false matches in a given period of time, it may indicate a hacker is trying to break into the system. It is unlikely that a legitimate user can provide more than 20 false matches per day. Hence, several unsuccessful attempts may indicate an attack by an imposter.

B. Liveness detection at sensor

This approach is used to prevent attacks at the sensor. Liveness differentiates between a real input sample feature provided by the living human being and a fake input feature provided by an artefact. Liveness detection can be applied using software or hardware means. There has been a development of extra hardware to detect various life signs like pulse, blood pressure, temperature for fingerprints and movements of the face, eyes for face recognition. Software is also used as means to detect life signs.

Multimodal- biometrics has also been proposed as means of increasing security.

C. Biometric cryptosystems

This technique combines biometrics and cryptography features to strengthen the security of the biometric system.

Biometric cryptosystems are subdivided into key generation and key binding [8]

a) Key generation

In this, helper data is only obtained from the biometric traits, and the cryptographic key is directly generated from the helper data.

b) Key binding

In this helper, data is obtained by binding a key with a biometric template

D. Steganography and Watermarking

Steganography and watermarking have also been proved to be very effective in preventing attacks on attack points on the channel between the sensor and feature extractor and attacks on the channel between matcher and application device. Watermarking is used in the authentication of ownership claims. Steganography can be used for transferring critical biometric information from a client to a server [9, 14].

E. Cancellable biometrics

Cancellable biometrics is a technique that involves intentional and systematic distortion of biometric templates based on a selected non-invertible transform [7,10]. If the transformed template is stolen or hacked, then it can be cancelled and reissued by changing the parameters of the template.

Cancellable biometrics is used to prevent attacks on template databases.

F. Visual Cryptography

The use of visual cryptography is explored to preserve the privacy of biometric data by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available. Further, the individual component images do not reveal any information about the original image [15]. In this process during the enrolment process, the private biometric data is sent to a trusted third-party entity [15]. Once the trusted entity receives it, the biometric data is decomposed into two images, and the original data is discarded. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. During the authentication process, the trusted entity sends a request to each server, and the corresponding sheets are transmitted to it. Sheets are superimposed in order to reconstruct the private image, thereby avoiding any complicated decryption and decoding computations that are used in watermarking, steganography, or cryptosystem approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image[15].

G. Homomorphic Encryption

Homomorphic encryption (HE) schemes allow a "limited subset of computation on the encrypted data." Combining HE with biometric recognition systems would meet the requirements of template protection schemes without degrading the accuracy [17].

IV. CONCLUSION

Biometric systems are being widely used to achieve reliable user authentication in an identity management system. But, biometric systems themselves are vulnerable to a number of attacks. It has been demonstrated through experiments the possibilities of breaking into the biometric system database.

In this paper, we have summarized various aspects of the vulnerability of the biometric system and discussed techniques to counter some of these threats.

This is the fact that an attack against stored biometric templates is a major concern due to the strong linkage between a user's template and his identity and the irrevocable nature of biometric templates.

REFERENCES

[1] Adler, A. Vulnerabilities in biometric encryption systems. In International Conference on Audio-and Video-Based Biometric Person Authentication. S pringer Berlin Heidelberg. (2005)1100-1109

[2] Angle, S., Bhagtani, R., & Chheda, H. Biometrics: A further echelon of security. In UAE International Conference on Biological and Medical Physics (2005).

[3] Campisi, P. Security and privacy in biometrics: towards a holistic approach. In Security and Privacy in Biometrics. Springer London., (2013) 1-23.

[4] Clancy, T. C., Kiyavash, N., & Lin, D. J. Secure smartcard-based fingerprint authentication. In Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications). ACM. (2003) 45-52.

[5] Ghany, K. K. A., Hefny, H. A., Hassanien, A. E., & Ghali, N. I. A hybrid approach for biometric template security. In Proceedings of the 2012 International Conference on Advances in Social Networks Analysis and Mining (2012) 941-942. IEEE Computers Society .

[6] Gudavalli, M., Kumar, D. S., & Raju, S. V. Integrated Biometric Template Security using Random Rectangular Hashing. Global Journal of Computer Science and Technology(2014) 14(7).

[7] Jain A. K, Biometric System Security , Dept. of Computer Science and Engineering Michigan State University, http://biometrics.cse.msu.edu, (2015).

[8] Jain, A. K., Nandakumar, K., & Nagar, A. Biometric template security. EURASIP Journal on advances in signal processing, (2008)113.

[9] Security Vulnerabilities Against Fingerprint Biometric System Mahesh Joshi1 Bodhisatwa Mazumdar Somnath Dey phd1701101004, Indian Institute of Technology Indore, India arXiv:1805.07116v1 [cs.CR] (2018).

[10] Kareem Kamal, Ghany A., Hesham A., Hefny Aboul, Hassanien E., Neveen I., Ghali I. A Hybrid approach for biometric template security. IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (2012).

[11] Ratha, N. K., Connell, J. H., &Bolle, R. M.. Enhancing security and privacy in biometrics-based authentication systems. IBM Systems Journal, 40(3) (2001)614-634.

[12] Ratha, N., Connell, J., Bolle, R. M., & Chikkerur, S. Cancelable biometrics: A case study in fingerprints. In Pattern Recognition, 2006.ICPR 2006.18th International Conference on 4 (2006)370-373. IEEE.

[13] Omotosho, F.S., Babatunde, R.S., Gbolagade, K.A Framework for Secured Biometric system. International Journal of Scientific & Engineering Research, 8(7) (2017) 2318- 2322.

[14] Rubal Jain and Chander Kant. Attacks on Biometric Systems: An Overview. International Journal of Advances in Scientific Research, 1(07) (2015) 283-288.

[15] Ross A. and Othman, A. Visual Cryptography for Biometric Privacy, in IEEE Transactions on Information Forensics and Security, 6(1) (2011). 70-81. doi: 10.1109/TIFS.2010.2097252

[16] Erkin, Z. Franz, M., Guajardo,J., Katzenbeisser, S., Lagendijk, I., Toft, T. Privacy-preserving face recognition, in Privacy Enhancing Technologies Springer, Berlin,(2009). 23 –253.

[17] Ye, S., Luo, Y., Zhao, J. Cheung, S.C.S., Anonymous biometric access control. EURASIP J. Inf. Secur. 2(1–17) (2009).

[18] Disha Lobo, Anoop C. V. and Mahesha Y, Securing Fingerprint Based Biometric System SSRG International Journal of Electronics and Communication Engineering, 3(10). 2019.