Reasoning for Template Protection Techniques in Biometric Technology

Omotosho F.S.
Computer Science Department,
Faculty of ICT,
Kwara State University,
Malete, Nigeria

Babatunde R.S.
Computer Science Department,
Faculty of ICT,
Kwara State University,
Malete, Nigeria

Gbolagade K.A.
Computer Science Department,
Faculty of ICT,
Kwara State University,
Malete, Nigeria

ABSTRACT
Biometrics technology has played a vital role in authentication and securing applications, mobile, smart devices and so on. Despite this widespread deployment of biometric technology, its uses have raised quite a few security and privacy treat. In a typical generic biometric system certain critical points were identified as security threats that can deflate the purpose of its use. One of the points identified is the attack targeted on biometric template, which is disastrous, since biometric traits are permanently bound to an individual, hence, once it is compromised, they cannot be revoked or reissued. It has been established from research that a stolen biometric template can be used by adversaries to break into the system and cross-matching to databases that uses similar biometric trait.

This paper presents some techniques/approaches to template protection available in the literature.

Finally, it itemized the strength added to the security of biometric technology by each biometric template protection approach. Indeed, researchers are still working tirelessly to improve on the existing techniques to curtail to minimal level the incidence of biometric template compromised.

General Terms
Pattern Recognition, Biometric, Security

Keywords
Authentication, Traits, Features, Template, Treat, Protection, Revoked, Reissue,Transformed, Cryptosystem.

1. INTRODUCTION
It is a general conception that when it comes to securing our applications and devices biometric technology has completely replaced the traditional methods of usage of password and Personal Identification Number (PIN) for authentication [1]. Even in healthcare sector many medical systems switch to electronic healthcare records in order to explore the advantages of electronic medical records (EMR) biometric technology [27].

Brief definition of biometric technology

Bio is connected with life and living things.

Metric is quantitative analysis that offers a positive identification of an individual

In case of human being the metrics are traits that are common to everyone.

These traits are classified as physiological and behavioral traits.

Physiological are face, iris, hand geometry, fingerprint, voice and palm print.

Behavioral are handwritten signatures, gait and keystroke dynamics [2].

Motives for integrating Biometric technology in application and devices.

Biometric technology helps to resolve the issue of who is the right owner and to find out who you claimed to be through authentication [7]. It is possible to bond digital data to our identity permanently and retrieve same data through computers/smart devices accurately. Biometric recognition provides a reliable solution to the problem of identifying the right owner in identification management system [21].

Biometric system

A generic biometric authentication system comprises of five main components which are: sensor, feature extractor, template database, matcher, and decision module as depicted in figure1. Sensor scans the biometric trait of the user both at enrollment and verification stages. Quality assessment module examines the scanned image if it is satisfactory to be used for processing [22]. Feature extraction module extract salient information (feature set) from scan image which is called template. At enrollment stage, the raw template is stored in the system database. as a template (TT). During verification, the sensor scans the query trait to extract query feature (Tq). Matcher module compares the query template with template stored in the database. Matcher module is an executable program that accepts two biometric features sets TT and TQ ((TT and query TQ)) as inputs and a matching score (S) output. The matching sore (S) indicate similarity of the two sets. Lastly, decision and response are taken by decision module based on matching score and threshold value set

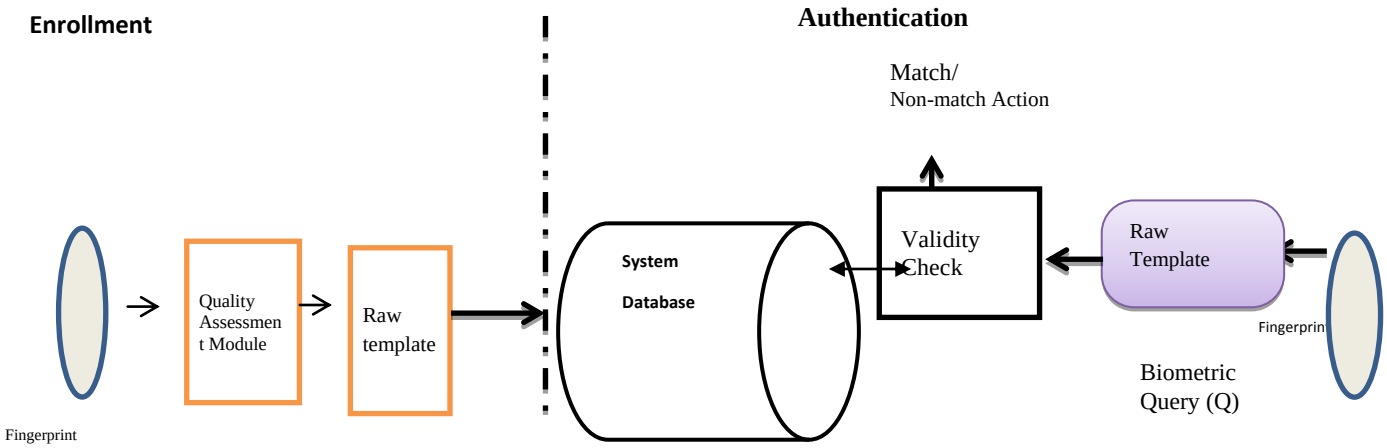

Figure 1: A generic biometric system [2]

This paper provides reasons for biometric template protection and a review of available techniques/approaches in the literature.

2. CHALLENGES OF BIOMETRIC TECHNOLOGY SYSTEM

Regardless of the massive inclusion of biometric systems in many applications, there are still concern on violation of privacy and security despite its inclusion [4, 23].

A. Susceptibility Points of Biometric System

Certain critical points that pose a security threats have been identified in a biometric system. The possible points are grouped into eight (8) classes. These locations are shown in fig.2.

Categories 1: In this type of attack a fake biometric (e.g., finger crafted from silicon, face mask, lens such as fake iris texture) is presented to the sensor [10]. Category 2: This is known as replay attack, it involves presenting an intercepted biometric record to the feature extractor, in an attempt to by past the sensor. Category 3: This entails changing of the feature extractor or module with a Trojan horse program.This Trojan horse program would have been designed to perform specific tasks as desired by the hacker. Category 4: At this stage hacker uses artificial/fake value to replace genuine feature values. Category 5: The matcher function is override with a Trojan horse program [13, 8]. Category 6: This is attack stage on the template database, this aim to modify or remove the template. Category 7: This occurred during transmission activities between the template database and matcher. The template may be stolen, replaced or altered by hacker at this stage. It is also possible to replace the output of the matcher at this stage by an attacker.

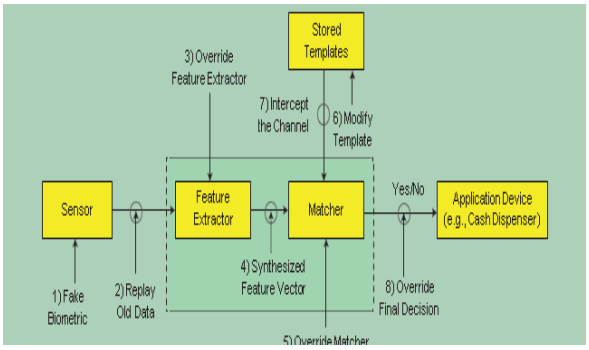

Figure2: Points of possible attacks in a biometric system [8],

B. BIOMETRIC TEMPLATE COMPROMISE

Biometric Template: Compressed digital features extracted from scan biometric traits is called template. The template contains salient discriminatory information that can be used to identify individual.

What are actually compared in biometric recognition system database are the biometric templates. There is need for great care to be taken so as not to expose the template of users that are enrolled in the biometric system to adversaries, as this pose great danger to biometric system.

The need for privacy protection in biometric information was first suggested in 2001 by Ratha, N. K., Connell J. H., and Bolle, R. M. in a seminal paper they presented, title "Enhancing security and privacy in biometrics-based authentication systems". Since then, many research works have been done on it [25, 23].

C. Effect of Biometric template attacks

It has been established from research that the following highlighted dangers can results from compromised biometric templates [3, 5, 25]:

i. Replacement of genuine biometric template with an impostor's biometric template so as to gain unauthorized

access.
ii. Gleaning or spoofing of fake biometric template from the stolen biometric template to gain unauthorized access to the system and other systems that uses the same stolen biometric template as security.Fingerprint image reconstructed from the stolen template is known as a "masquerade" image, as it is not the original image.

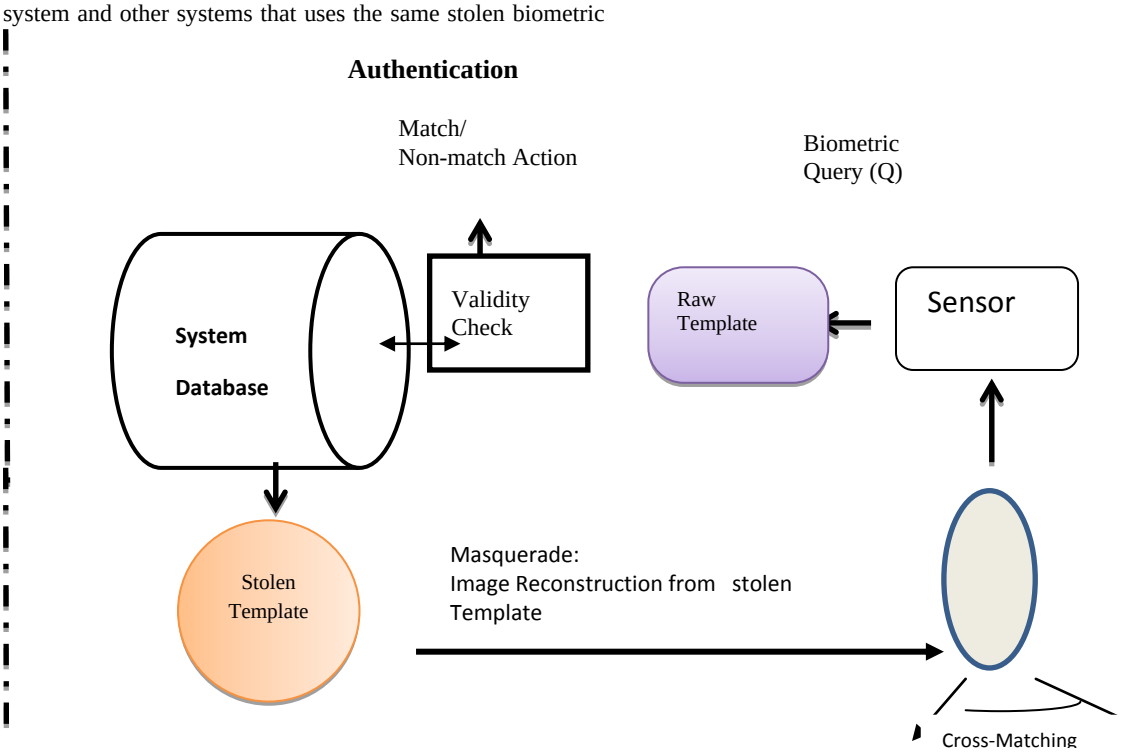

Figure 3: Image Reconstruction (Masquerade) from stolen templates [10]

This could probable deceive the system when submitted [9]
In 2007, Cappelli, Raffaele, Dario Maio, Alessandra Lumini, and Davide Maltoni carried out an experiment to analyze the minutiae standard template of ISO/IEC 19794-2 with different approaches of test. With nine different systems use for the tests, the average percentage of successful attacks was 81% when the threshold value was set to high security level and 90% on a medium security level. Figure 3. depicted a physical spoof reconstructed from stolen fingerprint template.

A physical spoof of a Biometric Template is a major threatening attack in biometric system, because, hackers may use it to hack bank accounts and other secured accesses [17].

iii. Adversaries can also use stolen biometric templates to cross-match to other databases that uses the same biometric traits.
Attack against template is the most devastating biometric system attacks, since biometrics traits cannot be replaced unlike password or Personal Identification Number (PIN). Reasons for various works carried out on biometric template protection algorithms by researchers to combat the menace of biometric systems attacks.

D. PROPERTIES OF IDEAL TEMPLATE PROTECTION SCHEME

ISO/IEC 24745: (2011) and 30136: (2018) on biometric template protection stated certain criteria/condition that an ideal biometric template protection scheme must satisfied. The four points are highlighted below:

(1) Diversity: The secured template must not allow cross-matching across databases, so that the user's privacy can be ensured.
(2) Revocability: It must be easier to revoke a compromised template and reissue a new one based on the same biometric data.

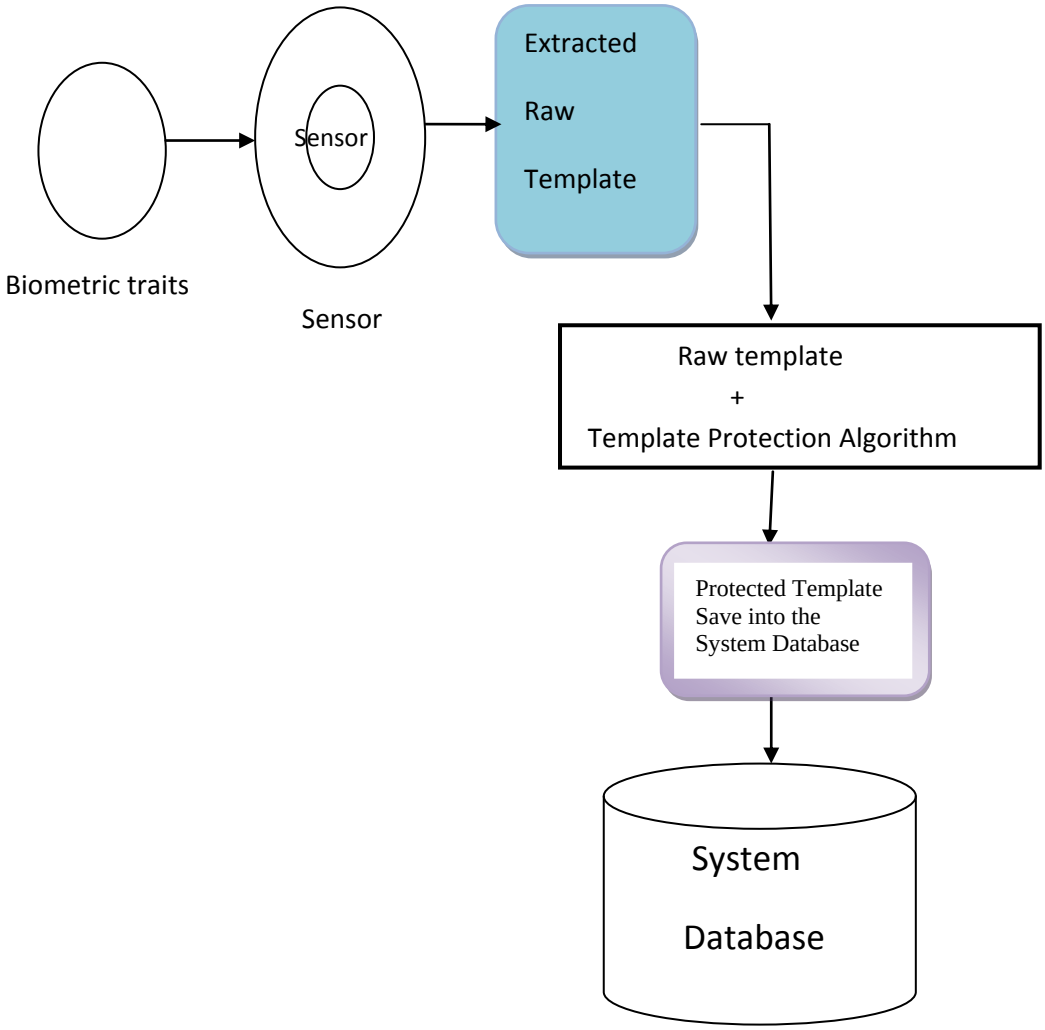

Fig.4. General Principle of template protection schemes [13]

(3) *Security*: It must be computationally hard to obtain the original biometric template from the secured template. This property prevents an adversary from developing a physical spoof of the biometric trait from a stolen template.
(4) *Performance:* The biometric template protection scheme should not degrade the recognition performance (False acceptance Rate (FAR) and False Rejection Rate (FRR) of the biometric systems.
The main task is designing a biometric template protection scheme that satisfies all of the above conditions [14].
In biometric template protection techniques instead of storing the raw biometric template in its original form (TR), a biometric template protection algorithm act on it to generate a protected template (TP) which is store in the system database [13, 4].
Figure 4 present a typical framework of a biometric system with template protection.

3. CATEGORIZATION OF BIOMETRIC TEMPLATE PROTECTION TECHNIQUES

The subsequent section gives an in-depth explanation on the techniques that has been proposed to secured biometric templates [4, 14].
The template protection schemes proposed within the literature can be extensively classified into three categories: (i) Feature transformation approach, (ii) Biometric cryptosystem and (iii) others as shown figure 5.

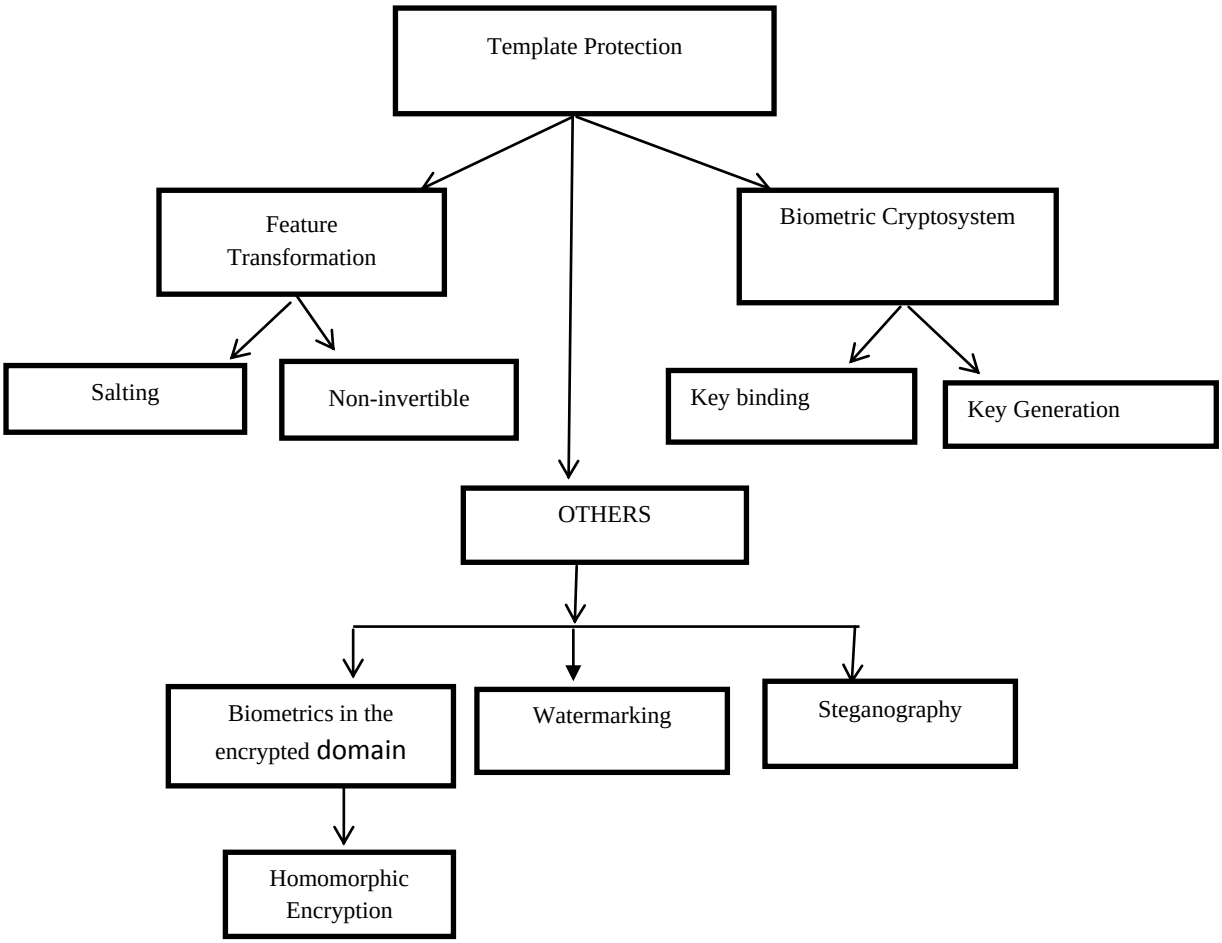

Figure 5: Biometric template Protection techniques Categorization [26]

3.1 Feature Transformation Techniques

In feature transformation techniques, the template is transformed using a one-way function. It may be carried out either in the original domain or in the feature domain. A transformation function (F) is applied to the biometric template (T) and only the transformed template (F (T; K)) is stored in the database. The parameters of the transformation function are derived from a random key (K) or password. The same transformation function is applied to query features (Q) and the transformed query (F (Q; K)) is directly compared against the transformed template (F (T; K)).

Subject to the characteristics of the transformation function F, the feature transform schemes can be further categorized as (i) Salting (invertible) and (ii) Noninvertible transform [2, 15, 26].

(i) Salting (Invertible)

In Salting or Biohashing template protection technique, the raw biometric template is transformed using a specific defined function with a user-specific key or password supply by the user. This key is needed at authentication stage. Due to the fact that the transformation is invertible to a large extent, the key needs to be securely saved. The need of extra information in the form of key increases the entropy of the biometric template and consequently makes it difficult for an adversary to guess the template [13, 4].

(ii) Noninvertible transform (Cancellable)

This approach secured biometric template by means of applying a non-invertible transformation function to it. Non-invertible transform is a one-way function, F, that is "easy to compute" (in polynomial time) however "difficult to invert" that is if (given F(x), the possibility of finding x in polynomial time is small). The parameters of the transformation function are defined through a key which have to be available at the time of authentication to transform the query feature set

Strength of the transformation techniques

1) The need of key as additional parameter for authentication reduces false acceptance rates.

2) Because the key is personal to an individual user, it is therefore possible to generate more than one template for the user biometric trait using different keys (thereby permitting diversity).

3) Additionally, in case a template is compromised, it is easy to revoke the compromised template and replace it with a brand new one generated by using a different user-specific key (thereby permitting revocability).

4 Computationally hard to recover the original biometric template from a transformed template without the user specific key thereby preserves privacy.
5) Prevents cross-matching between databases due to the fact each application makes use of different transformation.
6) it maintained statistical characteristics features of the traits after transformation hence, accuracy of the matching algorithm does not diminish.

3.2 Biometric Cryptosystem Techniques

Biometric cryptosystems were initially developed for the use of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features. But, it has additionally been used as a template protection mechanism. These techniques integrate cryptographic keys with transformed versions of the original biometric templates to generate secure templates. In these techniques, some public information, referred to as helper data, is generated. Depending on how the helper data is used, biometric cryptosystems can be broadly classified into key binding and key generation [4].

(i) Key Generation

In Key Generation, a biometric key is directly generated from the helper data and the query biometric features [10]. Under Key Generation secure sketches and fuzzy extractors has also been proposed.

Fuzzy Extractors and Secure Sketches

Error codes can easily be corrected. It also generates linear encryption keys for use in encryption and decryption.

Fuzzy Extractor: It accurately extracts uniform randomness R from its input, even if the input change R will not change. Any other biometric template from the same finger can be used, once it is nearly similar to the original R. It then means R can be used in a cryptographic application as a key.

Secure Sketch: Experiment has proved that secure sketch produced public information about its input w that did not reveal w but allowed precise recovery of w given another value that is close to w. Therefore, it can be used to reproduce error-prone biometric inputs without incurring security risks inherent in storing them [20].

Strength of Key generations
It guaranteeing absolute secret key in security management
It permits correction of errors codes
It generates linear encryption keys for encryption and decryption.
It is also error-tolerant

(ii) Key binding

In key-binding biometric cryptosystem the helper data is acquired through binding a key which is independent of the biometric features with the biometric template. Though, given only the helper data, it is computationally difficult to recover either the key or the original template. Matching in a key-binding system entails recovery of the key from the helper data using the query biometric features. Under Key binding fuzzy vault and fuzzy commitment has also been proposed [19].

Fuzzy Vault and Fuzzy Commitment

Biometrics traits represented in binary vector are secure using fuzzy commitment. In a fuzzy commitment technique, a uniformly random key of length 1 bits is generated and it is used to specifically index an n-bit code-word of suitable error correcting code where the sketch extracted from the biometric template is stored in a database,
The main difference between fuzzy vault and fuzzy commitment is that biometric traits secured through fuzzy commitment are represented in the form of binary vectors which are divided into a number of segments and each segment is separately secured, while biometric traits in fuzzy vault are represented in the form of point set which are secured by hiding them with chaff points [19].

Strength of the Key binding cryptosystem techniques

It is used to protect private keys and release them only when the valid users enter their biometric data

3.3 Hybrid Schemes

Hybrid template protection techniques combined two template protection approaches example, implementing salting approach then followed by key- binding approach [6, 29].

Strength of the Hybrid techniques

It increases the security of biometric templates
Minimizes error rates of biometric system.

3.4 Biometrics in the Encrypted Domain

Homomorphic Encryption

Apart from the two major categories discussed, when the privacy of the user is not completely protected or verification overall performance degrades, homomorphic cryptosystems has been proposed for use so as to carry out biometric recognition in the encrypted domain at the same time obtain results wholly comparable to those yielded by plain data [16].
Homomorphic Encryption schemes permits computations to be performed on cipher texts, without adding auxiliary data, and generate encrypted results which decrypt to plaintexts that match the result of the operations carried out on the original plaintext.
Thus, combining such an encryption approach with biometric verification systems would improve security at the same time preserve verification performance [18].
Although, practical implementations of Fully Homomorphic Encryption (FHE) schemes still stand a big issue. To some extent Homomorphic Encryption (HE) schemes, that allow a limited subset of operations in the encrypted domain, are presently being introduced into many applications through signal processing and biometrics.

Strength of Homomorphic Encryption
It is suitable in multi-biometric template protection.
It permits template comparisons to be carried out in the encrypted domain without the use of helper data and receiving the same comparison outcomes as achieved in the encrypted domain.

3.5 Watermarking

Watermarking integrate biometric fingerprint templates as a message in a standard watermarking application e.g. copyright protection so as to enable biometric recognition after the extraction of the watermark. In a typical biometric watermarking scheme, an attacker will need to have the knowledge of pixel values in which watermark information is hidden before he can attempts to replace or forge the biometric template [24, 28].

Strength of Watermarking
It provides high security of template by making it hard to forge stored biometric templates.

Watermarking is an excellent approach to transmit biometric data through network, smart card or someone.

4. CONCLUSION

The paper attempt to justify the need for biometric template protection algorithm in biometric system, it started by brief introduction to biometric system, then, progressed to identify possible points in a biometric system that are vulnerable to attacks as presented in reviewed literature.

It was discovered from reviewed literature that biometric templates stored in the database is mostly the main target in biometric system attacks. Also, the dangers pose by compromising biometric template.

The paper highlighted some of the various techniques proposed in the literature to secure biometric templates. These techniques were formally categorized as feature transformation and cryptosystems but another category has been identified by researcher as biometrics in the encrypted domain.

Finally, it itemized the strength added to security of biometric technology by each biometric template protection approach. Indeed, researches are still on going so as to curtail to minimal level the incidence of biometric template attacks through various biometric template techniques proposes in the literature.

It was discovered from papers review that no precise techniques proved excellent as expected when match with factors of a perfect biometric template protection scheme as stated in ISO/IEC 24745: (2011) and 30136: (2018).

Therefore, there is yet, need for greater research works to be carried out, so that we can have a secured, dependable, efficient and excellent biometric template protection techniques.

5. ACKNOWLEDGMENTS

Our thanks to the experts who have contributed towards this field of research.

6. REFERENCES

[1] Matyáš, V., &Rıha, Z. (2000). Biometric authentication systems. In verfügbarüber: http://grover. informatik. uni-augsburg. de/lit/MM-Seminar/Privacy/riha00biometric. pdf.

[2] Jain, A. K., Ross, A., &Pankanti, S. (2006). Biometrics: a tool for information security. IEEE transactions on information forensics and security, 1(2), 125-143.

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

[4] A. K. Jain, K. Nandakumar, and A. Nagar(2008) , Biometric template security, EURA- SIP J. Adv. Signal Process., vol. 2008, pp. 113:1–113:17.

[5] Raju, S. V., Vidyasree, P., & Madhavi, G. (2014, (February). Enhancing Security of Stored Biometric Template in Cloud Compuuting Using FEC. International Journal of Advanced Computational Engineering and Networking, 2(2), 35-39.

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

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

[8] Nagar, A., Nandakumar, K., & Jain, A. K. (2010). Biometric template transformation: a security analysis. In IS&T/SPIE Electronic Imaging (pp. 75410O-75410O). International Society for Optics and Photonics.

[9] Fingerprint Biometrics: Address Privacy before Deployment. https://www.ipc.on.ca/wp-content/uploads/2008/11/fingerprintbiosys-priv.pdf,.

[10] Cappelli, Raffaele, Dario Maio, Alessandra Lumini, and Davide Maltoni. (2007) Fingerprint image reconstruction from standard templates. IEEE transactions on pattern analysis and machine intelligence 29, No.9.

[11] Information Technology Security Techniques Biometric Information Protection, (2011), Standard ISO/IEC 24745:2011, 2011.

[12] Information Technology Performance Testing of Biometric Template Protection Schemes, (2018), Standard ISO/IEC 30136:2018,

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

[14] Karthik Nandakumar and Anil K. Jain (2015) Biometric Template Protection: Bridging the Performance Gap Between Theory and Practice, To Appear in IEEE Signal Processing Magazine - Special Issue on Biometric Security and Privacy

[15] LoubnaGhammam, Morgan Barbier, Christophe Rosenberger (2018). Enhancing the Security of Transformation Based Biometric Template Protection Schemes. Cyber Worlds, Oct, Singapour, Singapore. hal-01862157

[16] Marta Gomez-Barrero, Emanuele Maiorana, Javier Galbally, Patrizio Campisi, Julian Fierrez (2017) Multi-biometric template protection based on Homomorphic Encryption, Elsevier journal on Pattern Recognition 67 149–163.

[17] A. Hadid, N. Evans, S. Marcel, J. Fierrez (2015), Biometrics systems under spoofing attack: an evaluation methodology and lessons learned, IEEE Signal Process. Mag. 32 (5) 20–30.

[18] M. Barni, G. Droandi, R. Lazzeretti) (2015), Privacy protection in biometric-based recognition systems: a marriage between cryptography and signal processing, IEEE Signal Process. Mag. 32 (566–76.

[19] Geethanjali, N., Thamaraiselvi, K., &Priyadharshini, R. (2012, (December). Feature Level Fusion of Multibiometric Cryptosystem in Distributed System. International Journal of Modern Engineering Research (IJMER), 2(6), 4643-4647.

[20] Dodis, Y., Ostrovsky, R., Reyzin, L., & Smith, A. (2008). Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. SIAM Journal on Computing, 38(1), 97-139.

[21] Luca Debiasi, Simon Kirchgasser, Artur Grudzien´ and Marcin Kowalski (2019), Biometric Template Protection in the Image Domain Using Non-invertible Grey-scale Transforms, 978-1-7281-3217-4/19/$31.00 © IEEE

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

[23] A. K. Jain, D. Deb, and J. J. Engelsma (2021), Biometrics: Trust, but verify, arXiv preprint arXiv:2105.06625,.

[24] Rohit M. Thanki, Vedvyas J. Dwivedi, Komal R. Borisagar (2018), Multibiometric Watermarking with Compressive Sensing Theory, Springer Science and Business Media LLC,

[25] Kevin Atighehchi, LoubnaGhammam, Morgan Barbier, Christophe Rosenberger (2019), "GREYCHashing: Combining biometrics and secret for enhancing the security of protected templates", Future Generation Computer Systems,

[26] Vishal M. Patel, Nalini K. Ratha, and Rama Chellappa (2015), Cancelable Biometrics, IEEE SIGNAL PROCESSING MAGAZINE p 54-68

[27] OmotoshoFolorunsho Segun and Fadiora Babatunde Olawale (2017), Healthcare data breaches: Biometric technology to the rescue International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 11 p-ISSN: 2395-0072.

[28] C. Kant and S. Chaudhary, (2020) "A Watermarking Based Approach for Protection of Templates in Multimodal Biometric System", Proc. Computer Science, pp. 932-941.

[29] Sarkar, A., Singh, B.K. (2021). Design of a hybrid approach using a revocable technique and steganographic text color coding technique for fingerprint template protection. Multimed Tools Appl 80, 20641–20670 https://doi.org/10.1007/s11042-021-10690-w