A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates

Joseph Mwema, Michael Kimwele, Stephen Kimani

School of Computing and Information Technology

Jomo Kenyatta University of Agriculture and Technology

(JKUAT)

Nairobi, Kenya

***Abstract*— In this paper, we base our research on biometric systems security. We begin by introducing biometrics after which we will describe how a biometric system works before we later define what a biometric template is. Thereafter, we will explore attacks on biometric systems and lay more emphasis on biometric template attacks and explore attacks targeting biometric templates in a biometric system database. These attacks motivated us to study the existing biometric template protection schemes and techniques currently in use to determine their strengths and weaknesses. In the end, we summarize this study in the conclusion section of the paper.**

***Keywords*— Biometric, Fingerprint, Template, Attacks, Threats, Security, Protection, Schemes, Techniques.**

1 INTRODUCTION

Biometric systems have been widely adopted and integrated into information systems to provide authentication procedures that guarantee non-repudiation. Unlike passwords & access PINs which are easily forgotten, stolen and easily guessed at in traditional authentication systems, biometrics are reliable, secure, efficient and a quick means of validating users if proper procedures and measures of using them are put into consideration. Biometrics have not been impervious to hacks as will later be shown in this paper and have on some known occasions been vulnerable to adversarial attacks.

We review the various attacks on biometric systems then explore biometric template attacks in databases and finally discover the existing biometric template protection techniques and schemes in existing literature while exploring their strengths and drawbacks.

The remainder of this paper is grouped into the following sections; Biometric Systems Key Definitions, Biometric Systems Attacks & Threats, Biometric Template Protection Techniques and finally the Conclusion.

2 BIOMETRIC SYSTEMS KEY DEFINITIONS

Biometrics refers to the automatic authentication of a person's physiological or behavioural characteristics. A biometric system is a pattern recognition system that retrieves biometric patterns from an individual, extracts biometric feature sets from them and thereafter stores them as *biometric templates* in a database. A biometric system consists of 5 major components. (Menariya & Ojha, 2012) put them into five (5) categories. They are; Sensor, Feature extractor, Template database, Matcher module and a Decision module.

In biometric template matching, comparison between saved biometric templates and captured biometric data is done to authenticate users. A certain threshold has to be met for a successful template match to be declared a *positive* match. A *failed* match is when the biometric features of a user do not match with those saved in a biometric system's database.

We conducted this review to find out the various biometric attacks and threats that have been documented in existing literature and determine the biometric template protection schemes and techniques currently being used towards securing biometric fingerprint templates in a biometric system's database.

3 BIOMETRIC SYSTEMS ATTACKS & THREATS

3.1 Biometric System Threats and Attacks

To understand significant attacks targeted at biometric systems, we embarked on familiarizing ourselves with the various biometric system attacks identified in existing literature. *Fig 1* below shows a graphical diagram of these attacks in a biometric system. We learned from Ratha et al in (Ratha, Connell, & Bolle, 2001) that these biometric system attacks are categorized as follows;

3.1.1 Attack at the scanner

In this attack also known as "Type 1 attack", the attacker can physically destroy the recognition scanner and cause a denial of service. The attacker can also create a fake biometric fingerprint trait such as an artificial finger to bypass fingerprint recognition systems, or inject a fingerprint image between the sensing element and the rest of the scanner module to bypass fingerprint recognition systems.

3.1.2 Attack on the channel between the scanner and the feature extractor

This attack is also known as "Type 2 attack" or "Replay attack". When the fingerprint scanner module in a biometric system acquires a biometric trait, the scanner module sends it to the feature extractor module for processing. At this point, the hacker can intercept the fingerprint and replace with theirs.

3.1.3 Attack on the feature extractor module

In this attack, the attacker can replace the feature extractor module with a Trojan horse. This attack is known as "Type 3 attack". The Trojan horse in this attack could be used to

harvest users' fingerprints extracted features and send them to the attacker.

3.1.4 Attack on the channel between the feature extractor and matcher

The difference in this attack also known as "Type 4 Attack" is that the attacker intercepts the communication channel between the feature extractor and the matcher to steal feature values of a legitimate user and replay them to the matcher at a later time.

3.1.5 Attack on the matcher

This point of attack is known as "Type 5 Attack". The difference is that the attacker replaces the matcher with a Trojan horse. The attacker can send commands to the Trojan horse to produce high matching scores and send a "yes" to the application to bypass the biometric authentication mechanism.

3.1.6 Attack on the system database

This attack is also known as "Type 6 Attack", the attacker compromises the security of the database where all the fingerprint templates are stored. Compromising the database can be done by exploiting vulnerability in the database software or cracking an account on the database. In either way, the attacker can add new fingerprint templates, modify existing templates or delete templates.

3.1.7 Attack on the channel between the system database and matcher

In this attack, the attacker intercepts the communication channel between the database and matcher to either steal and replay data or alter the data. This point of attack is known as "Type 7 Attack".

3.1.8 Attack on the channel between the matcher and the application

In this attack also "Type 8 Attack", the attacker intercepts the communication channel between the matcher and the application to replay previously submitted data or alter the data.

3.2 Biometric Fingerprint Template Security

In this section we explored the vulnerabilities posed by biometric template attacks then reviewed the 'Type 6 attack' which is the *attack on biometric templates in database*.

3.2.1 Biometric Template Vulnerabilities

Having studied attacks on biometric systems, we sought to understand what susceptibilities biometric templates were exposed to due to these attacks. We established from a more recent research by (Raju, Vidyasree, & Madhavi, 2014) that attacks on biometric templates can lead to the following vulnerabilities;

i. A biometric template can be replaced by an impostor's biometric template to gain unauthorized access.

ii. A physical spoof of a Biometric Template can be created from the biometric template to gain unwarranted access to the system including other systems that use the same biometric fingerprint trait.

iii. Stolen biometric Templates can be replayed to the matcher to gain unauthorized access past authentication vaults.

iv. Biometric Templates if not properly secured can be used by adversaries for cross-matching across other databases to covertly track a person without their consent.

3.2.2 Biometric Template Attack in the Database

We observed from the study of biometric system threats and attacks that "Type 6 attack" is where the adversary attacks the biometric fingerprint template in the database. As seen in this type of attack, the hacker can add new templates, modify existing templates or delete templates.

In a previous publication, Brindha in (Brindha V. E., 2012) mentioned that, one of the most vital harmful attacks on a biometric system happens when it is against the biometric templates. She further explained how attacks on the templates can lead to grave vulnerabilities where a template can be replaced by an impostor's templates to achieve unlawful access to a system. She further cautioned against biometric templates being stored in plaintext form and insisted that fool-proof methodologies are essential in securing storage of biometric templates to safeguard both safety of the biometric system and that of the users.

Attacking of biometric templates in a database with sole purpose of stealing them to later on present and use them to beat the biometric system security check is called *spoofing*. In a research study conducted by Mwema et al, we observed from results of the survey they performed that *spoofing* of biometric templates is the most persistent attack experienced in biometric systems (Mwema, Kimani, & Kimwele, 2015). In a biometric system, physical spoofing of biometric templates happens at the biometric system database 'Type 6 attack' thus these results were indicative of this significant attack cautioned about by Brindha in (Brindha V. E., 2012).

Having already understood the types of biometric system attacks that exist and noticing that most of the major attacks are targeted at biometric templates, we proceeded to study the biometric template protection techniques used to secure biometric systems against these attacks.

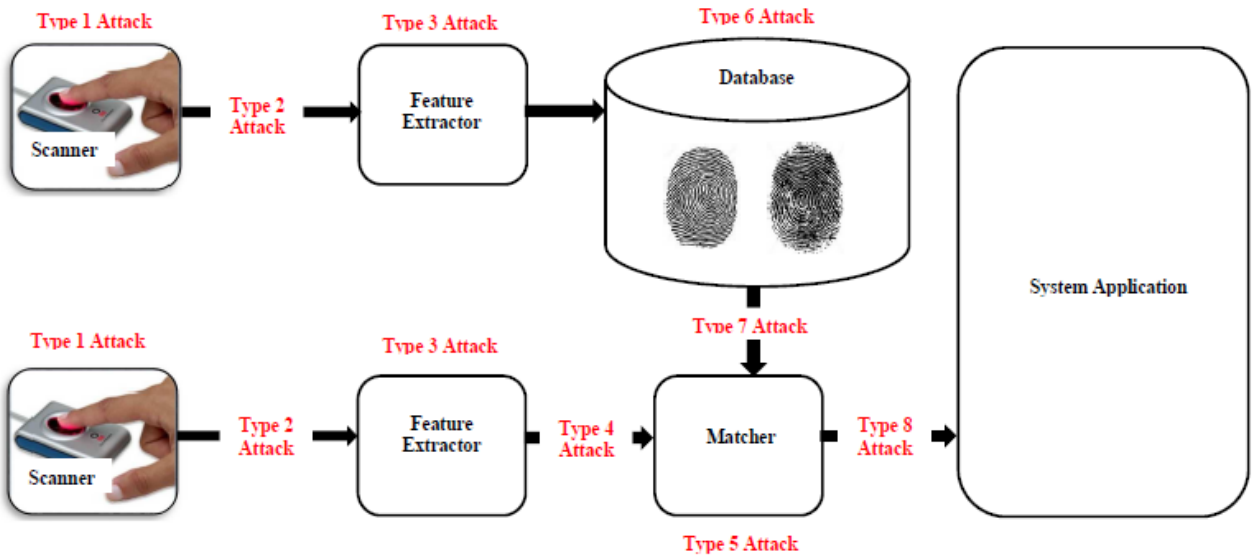

Fig. 1 Graphical Representation of possible Biometric System Attacks

4 Biometric Template Protection Techniques

Biometric Template Protection Schemes are classified into *Feature Transformation* and *Biometric Encryption*. Jain et al in (Jain, Nandakumar, & Nagar, 2008) categorized the various biometric template protection techniques as (i) *Feature Transformation* and (ii) *Biometric Encryption*. This has been the basis on which biometric template techniques have been classified. We explore and discuss the existing biometric template techniques in literature based on these categories. *Fig 2* below shows a graphical representation of biometric template protection techniques we will discuss in this section.

4.1 Feature Transformation

In Feature Transformation, a biometric template *(BT)* is transformed to *F (BT,X)* after a function *F* with a randomly generated key *X* is applied to it. Feature Transformation is further categorized into either *invertible* or *non-invertible* transform. In *invertible* transform, the key *X* can be used to recover the original biometric template *(BT)* while in *non-invertible* transform the key *X* is a one-way key that makes it hard to recover the original biometric template *(BT)* even if the key *X* is known as was pointed out by (Arjunwadkar & Kulkarni, 2010). Existing literature identify *bio-hashing* as an invertible transformation and *cancellable biometrics* as non-invertible transformation (Gaddam & Lal, 2011). To understand how feature transformation of biometric templates worked we explored bio-hasing and cancellable biometrics to depth.

4.1.1 Cancellable Biometrics

Unlike passwords, PINs and access codes, biometric templates can never be replaced with newer ones if they are compromised. To circumvent this challenge, cancellable biometrics were introduced such that biometric templates could be cancelled and replaced (Radha & Karthikeyan, 2011).

Cancellable biometrics scheme is an intentional and systematic repeatable distortion of biometric template data with the purpose of protecting it under transformational-based biometric template security. In the concept of cancellable transformation, a transformed template can be *cancelled* and *re-issued* by changing transformation parameters if misplaced.

Cancellable biometric is not without its fair share of challenges, (Rathgeb & Uhl, 2011) raised concerns that if transformed biometric data is compromised then transformation parameters should be changed to deter adversaries from tracing and cross-matching users' biometric templates.

From studying cancellable biometrics, we discovered that if transformational parameters are known to hackers, cancellable biometrics will not be secure. The other downside of cancellable biometrics as reported by (Du, Yang, & Zhou, 2011) is that it reduces recognition accuracy of the biometric-based system due to the high variance brought about by the distorted data when transformation is applied on users' biometric data.

4.1.2 Bio-hashing

Biohashing is a biometric template protection approach in which features from a biometric template are transformed using a transformation function defined by a password or a key known only to the user (Kannan & Thilaka, 2013). This key or password needs to be securely stored and remembered by the user for subsequent authentication.

In contrast to *Cancellable biometrics*, the key or password used in *biohashing* increases entropy of biometric template which further deters adversary attacks. Direct mixing of pseudo-random number (which is kept secret) and biometric data is used to compute a binarized key of 80-bits key with a 0.93% false rejection rate of the system (Radha & Karthikeyan, 2010). This generated physical token as we observed, can be used in smart card or USB tokens as shown by (Kannan & Thilaka, 2013).

The major drawback of *biohashing* as compared to *cancellable biometrics* is its reduced performance when a legitimate token is retrieved and presented by an adversary purporting to be a legitimate user (Gaddam & Lal, 2011). Das Karthik, & Garai however are of the opinion that bio-hash must be linkable to the original template to permit authentication and at the same time be non-invertible to thwart incidences of theft but then the need to have some elasticity to make *biohashing* robust introduces possibility of some unavoidable information leakage in the process of computing the bio-hash (Das, Karthik, & Garai, 2012).

4.2 Biometric Cryptosystems

Traditional identity authentication based on simple passwords have always been easy to break using e.g. simple dictionary attacks (Li & Hwang, 2010). To bypass these caveats, cryptographic secret keys and passwords have been proposed. In an earlier research, Jain et al in (Jain, Nandakumar, & Nagar, 2008) subdivided biometric cryptosystems into *Key Generation* and *Key Binding.*

4.2.1 Key Generation

While exploring biometric cryptosystems, we observed from literature that in Key Generation a biometric key is derived directly from biometric data (Blanton & Aliasgari, 2013). Under Key Generation we explore and discuss secure sketches and fuzzy extractors.

4.2.1.1 Secure Sketches and Fuzzy Extractors

Dodis et al originated with *secure sketches* and *fuzzy extractors* in a preliminary version of their research work in year 2004 which was later published in (Dodis, Ostrovsky, Reyzin, & Smith, 2008). Dodis et al's scheme of using secure sketches and fuzzy extractors was significant in the biometric cryptosystems as it allowed for correcting of error codes in biometric data and generating almost linear encryption keys for use in encryption and decryption. In their later published research work they alleged that they were formally defining efficient and secure techniques for;

- Retrieving keys for any cryptographic application from noisy data including biometric data.
- Then reliably and securely performing authentication of biometric data.

They defined *Fuzzy Extractor* and *Secure Sketch* as follows;

i. *Fuzzy Extractor*: Dodis et al said that a Fuzzy Extractor reliably extracts almost uniform randomness *R* from its input: The significance of fuzzy extraction is that it is error-tolerant in the sense that *R* will not change even if the input changes e.g. if another biometric template from the same finger is used, as long as it is almost similar to the original *R* implying *R* can be used in a cryptographic application as a *key*.

ii. *Secure Sketch*: Dodis et al held that their Secure Sketch produced public information about its input *w* that did not reveal *w* and yet allowed exact recovery of *w* given another value that is close to *w* which was an advantage that made it possible for it to be reliably used to reproduce error-prone biometric inputs without incurring security risks inherent in storing them.

In a recent publication on analysis of reusability of fuzzy extractor and secure sketch by (Blanton & Aliasgari, 2013), Blanton & Aliasgari looked at a number of the original *fuzzy extractors* and *secure sketches* constructions and argued that they could not be safely applied severally to the same biometric, thus significantly limiting and reducing their usability in practice.

4.2.2 Key Binding

In Biometric Cryptosystems, we learned that *Key Binding* is where a secret key and the biometric template are monolithically bound within a cryptographic framework whilst it is computationally infeasible to decode the key or biometric template without prior knowledge of the user's biometric data (Kannan & Thilaka, 2013). We explored *Fuzzy vault* and *Fuzzy commitment* cryptographic schemes which use key binding in our research to understand how *key binding* works.

4.2.2.1 Fuzzy Vault

Fuzzy vault is a cryptographic construct that was first proposed by Jules and Sudan in (Juels & Sudan, 2002) where secret information is encrypted and decrypted securely using a fuzzy unordered set of genuine points and haff points. Geetika & Kaur described a biometric fuzzy vault as a biometric cryptosystem used for protecting private keys and releasing them only when the legitimate users enter their biometric data as shown by (Geetika & Kaur, 2013) while Deshpande & Joshi defined a fuzzy vault as a scheme utilized for secure binding of randomly generated key with extracted biometric features (Deshpande & Joshi, 2013).

While studying significance of a biometric fuzzy vault scheme, we observed that Prakash & Bharathan had alleged that the motivation to protect secret key in biometric cryptographic modules using fuzzy vault scheme came from the analogy that, the current cryptographic algorithms have a very high proven security but have problems in guaranteeing absolute secret key security management (Prakash & Bharathan, 2012). This was further affirmed by Meenakshi & Padmavathi who confirmed that fuzzy vault schemes eliminated key management problems found in other practical cryptosystems (Meenakshi & Padmavathi, 2010). The limitations of a fuzzy vault scheme as listed by Hooda & Gupta in (Hooda & Gupta, 2013) are;

i. Difficulty in revoking a compromised vault which is also prone to cross-matching of biometric templates across databases.

ii. Easy for an attacker to stage attacks after statistically analysing points in vault.

iii. It is possible for an attacker to substitute his biometric features with that of the targeted biometric features thus beating vault authentication.

iv. The other threat is that, if the original template of the genuine user is temporarily exposed, the attacker can glean the template during this exposure.

4.2.2.2 Fuzzy Commitment

Fuzzy Commitment is a biometric cryptosystem which is used to secure biometrics traits represented in binary vector (Jeny & Jangid, 2013). Jeny & Jangid added that, a fuzzy commitment scheme is one where a uniformly random key of length 1 bits is generated and used to exclusively index an *n-bit* codeword of suitable error correcting code where the sketch extracted from the biometric template is stored in a database.

The difference between *fuzzy vault* and *fuzzy commitment* as brought out by Geethanjali et al is that biometric traits secured by 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 (Geethanjali et al, 2012).

Al-Saggaf & Acharya in (Al-Saggaf & Acharya, 2013) claimed that the ordinary fuzzy commitment scheme cannot satisfy hiding and binding properties of biometric traits and considered it insecure. They pointed out that the cryptographic hash function $h(c)$ where the secret message c is hidden in the hash value $h(c)$ as not secure enough because the cryptographic hash functions such as *MD5* and *SHA* families have already been proven theoretically and practically vulnerable to collision and second pre-image attacks. Their argument that MD5 and SHA are vulnerable is undeniably supported by (Schmitt & Jordaan, 2013).

4.2.3 Advantages of Biometric Keys

We established that the advantages of using biometric keys as compared to traditional passwords as shown by (Das A. K., 2011) are as follows;

i. Biometric Keys cannot be misplaced or forgotten.
ii. It is difficult to copy and distribute them.
iii. They are extremely hard to reverse engineer, forge or distribute
iv. They are not easy to guess at unlike passwords.

4.3 Other Biometric Template Protection Schemes

In this section we reviewed watermarking scheme, RSA and ECC algorithms.

4.3.1 Watermarking

The aim of watermarking is to use biometric fingerprint templates as a message to be integrated in a robust watermarking application like copyright protection in order to enable biometric recognition after the extraction of the watermark. In a biometric watermarking scheme, if an attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden as shown by (Malhotra & Kant, 2013).

While surveying existing biometric template protection techniques, Poongodi & Betty in (Poongodi & Betty, 2014) listed the advantages of watermarking approach as follows; They said it was difficult to forge stored biometric templates and that watermarking provided high security of biometric templates. (Fazli & Zolfaghari-Nejad, 2012) backed their assertions that biometric watermarking is one of the template protection techniques that prevents attack on biometric templates then added that it was the best technique when biometric data is to be transmitted via network or by a person e.g. in a smart card.

We then determined the downsides of watermarking as compared to other biometric template techniques and established that there is a greater amount of time taken in inserting a watermark in biometric templates as we found out from (Poongodi & Betty, 2014) and that most of the algorithms used for watermarking require an original image to be used to extract the watermark. Unlike biometric cryptosystems techniques which do not need to keep the original image after encryption is done, watermarking schemes need the original image to aid in recovering the watermark as was also shown by (Naik & Holambe, 2010). We were of the opinion that storing the original image in watermarking scheme would not only lead to need for more storage space but will present an opportunity for adversaries to spoof the original biometric image.

4.3.2 Rivest, Shamir and Adleman (RSA) Technique

RSA is an encryption algorithm for public key cryptography based on the practical difficulty problem of factorization of large integers as was described by (Nasir & Kuppuswamy, 2013). RSA algorithm's debut was in 1978 when it was first introduced by Rivest, Shamir and Adleman and was named after their names i.e. Rivest, Shamir and Adleman. The implementation of RSA algorithm involves a public key and a private key where the public key can be known to everyone and used for encrypting messages. This is such that the message encrypted with public key will only be decrypted using the private key (Chandra, Paul, Saha, & Mitra, 2013).

RSA is implemented in three (3) phases where in the 1st phase, key generation happens and in the 2nd and 3rd phase encryption and decryption takes place. RSA is secure if long keys are used and is significant in that it protects files from hackers and ensures safe transmission of files between two (2) points as was explained by (Zhou & Tang, 2011). Based on this observation, we concluded that an RSA encrypted message is likely to be decrypted if brute force is used where public key is known and the private key used is short.

4.3.3 *Elliptic Crypto Curve (ECC) Technique*

Muthukuru & Sathyanarayana described an Elliptic Curve Cryptography also known as ECC as a public key cryptography that makes use of algebraic forms of elliptic curves over elements restricted to finite fields (Muthukuru & Sathyanarayana, 2013). They added that ECC algrorithm uses a smaller key leading to lower memory usage and reduced computational requirements than traditional encryption and decryption algorithms.

4.3.4 *RSA and ECC Algorithms Comparison*

While comparing RSA and ECC encryption algorithms we established from a research experiment done by (Maniroja & Sawarkar, 2013) while comparing the two algorithms that RSA scheme takes 10 seconds to encrypt an image of size 256 by 256 whilst ECC scheme takes 30 seconds. We also noted that an equivalent amount of time was required in decryption of images during verification and identification of persons on a biometric authentication system using these biometric template protection schemes and due to this bottleneck, there was need for alternative biometric encryption schemes or rather the need for RSA and ECC schemes to be optimized for short turnaround times since a biometric system's performance is critical if it is to be considered efficient for use in verification and identification processes.

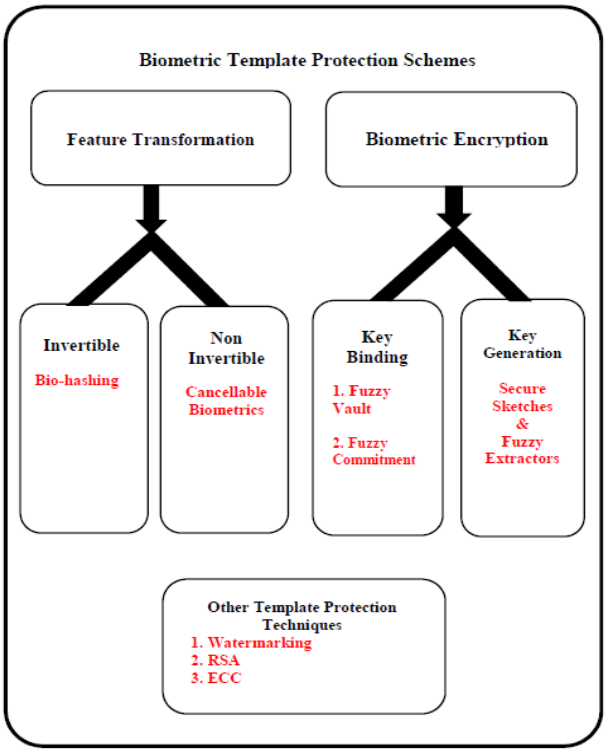

Fig. 2 Graphical Representation of Biometric Template Protection Techniques Discussed

4.4 *Features of an Ideal biometric template protection scheme*

According to (Maltoni, Maio, Jain, & Prabhakar, 2003) as we found out, an ideal biometric template protection scheme should consist of the following four attributes.

i) *Diversity*: A secure biometric template must not allow crossmatching across databases, thus ensuring their bearer's privacy.

ii) *Revocability*: It should be straightforward to revoke a compromised biometric template and reissue a new one based on the same biometric physical traits of the initial bearer.

iii) *Security* : It should not be possible to reverse engineer the secure biometric template to obtain the original biometric template. This property discourages adversaries from recreating original biometric traits and using them as a physical spoof in stolen templates.

iv) *Performance*: The biometric template protection scheme should not reduce the matching speeds of templates or trigger an upward surge in False Acceptance Rates and False Rejection Rates.

5 Conclusion

In this paper we introduced biometric systems then progressed to identify biometric attacks and threats documented in existing literature. We found out from existing literature that most of the biometric attacks target biometric templates. We then determined vulnerabilities that biometric templates are exposed to as a result of these attacks and continued to explore the 'Type 6' attack on biometric templates, which is the *attack of biometric templates* in databases. The various biometric template techniques which usually fall under *feature transformation* and *cryptosystems* were explored to identify their strengths and shortcomings.

This review gives a clear and precise understanding on the current status of biometric attacks, biometric template vulnerabilities arising as a result of these attacks and finally shows what researchers have been working on to stop these biometric template attacks. It was noted that there was no particular biometric template protection technique that proved satisfactory in all aspects of an ideal biometric template protection scheme and that there was still need for more research work to be done to establish secure, reliable, efficient and fool proof biometric template protection techniques. In future work, we will propose a two-step encryption & decryption approach for securing biometric fingerprint templates stored in a database.

References

[1] Al-Saggaf, A. A., & Acharya, H. (2013). Statistical Hiding Fuzzy Commitment Scheme for Securing Biometric Templates. *International Journal of Computer Network and Information Security*, 8-16.

[2] Blanton, M., & Aliasgari, M. (2013). Analysis of Reusability of Secure Sketches and Fuzzy Extractors. *Journal of Computer and System Sciences, 58*, 148-173.

[3] Brindha, V. E. (2012). Biometric Template Security using Dorsal Hand Vein Fuzzy Vault. *Journal of Biometrics*.

[4] Chandra, S., Paul, S., Saha, B., & Mitra, S. (2013, May-June). Generate an Encryption Key by using Biometric Cryptosystems to

secure transferring of Data over a Network. *IOSR Journal of Computer Engineering (IOSR-JCE), 12*(1), 16-22.

[5] Das, A. K. (2011, March). Cryptanalysis and Further Improvement Of a Biometric-Based Remote User Authentication Scheme Using Smart Cards. *International Journal of Network Security & Its Applications (IJNSA), 3*(2), 13-28.

[6] Das, P., Karthik, K., & Garai, B. C. (2012, September). A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition, 45*(9), 3373-3388.

[7] Deshpande, A., & Joshi, R. B. (2013). Information Security using Cryptography and Image Processing. *IJSRD - International Journal for Scientific Research & Development, 1*(9).

[8] 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.

[9] Du, E. Y., Yang, K., & Zhou, Z. (2011, October). Key Incorporation Scheme for Cancelable Biometrics. *Journal of Information Security*, 185-194.

[10] Fazli, S., & Zolfaghari-Nejad, M. (2012, March). An Improved Watermarking Algorithm for Hiding Biometric Data. *International Journal of Science and Engineering Investigations, 1*(2), 11-15.

[11] 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.

[12] Geetika, & Kaur, M. (2013, April). Fuzzy Vault with Iris and Retina: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(4).

[13] Hooda, R., & Gupta, S. (2013, April). Fingerprint Fuzzy Vault: A Review. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(4), 479-482.

[14] Jain, A., Nandakumar, K., & Nagar, A. (2008). Biometric Template Security. *EURASIP Journal on Advances in Signal Processing (2008).*

[15] Jeny, J. V., & Jangid, C. J. (2013). Multibiometric Cryptosystem with Fuzzy Vault and Fuzzy Commitment by Feature-Level Fusion. *International Journal of Emerging Technology and Advanced Engineering , (Volume 3, Issue 3, March 2013)*.

[16] Juels, A., & Sudan, M. (2002). A Fuzzy Vault Scheme. *IEEE International Symposium Information Theory*.

[17] Li, C. T., & Hwang, M. S. (2010). An efficient biometric-based remote authentication scheme using smart cards. *Journal of Network and Computer Applications*, 1-5.

[18] Malhotra, S., & Kant, C. (2013, May). A Novel approach for securing biometric template. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(5).

[19] Maltoni, D., Maio, D., Jain, K., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition.* Berlin, Germany: Springer.

[20] Maniroja, M., & Sawarkar, S. (2013). Biometric Database Protection using Public Key Cryptography. *IJCSNS International Journal of Computer Science and Network Security, VOL.13 No.5, May 2013*.

[21] Meenakshi, V. S., & Padmavathi, G. (2010, September). Securing Revocable Iris and Retinal Templates using Combined User and Soft Biometric based Password Hardened Multimodal Fuzzy Vault. *IJCSI International Journal of Computer Science Issues, 7*(5), 159-167.

[22] Menariya, D., & Ojha, D. B. (2012, October). A vital application of security with biometric templates. *International Journal of Engineering Research and Applications (IJERA), 2*(5), 328-332.

[23] Muthukuru, J., & Sathyanarayana, B. (2013, January). A Survey of Elliptic Curve Cryptography Implementation Approaches for Efficient Smart Card Processing. *Global Journal Of Computer Science and Technology, 12*(1).

[24] Mwema, J., Kimani, S., & Kimwele, M. (2015, February). A Study of Approaches and Measures aimed at Securing Biometric Fingerprint Templates in Verification and Identification Systems. *International Journal of Computer Applications Technology and Research, 4*(2), 108-119.

[25] Naik, A. K., & Holambe, R. S. (2010). A Blind DCT Domain Digital Watermarking for Biometric Authentication. *International Journal of Computer Applications, 1*(16), 11-15.

[26] Nasir, M. S., & Kuppuswamy, P. (2013, October). Implementation of Biometric Security using Hybrid Combination of RSA and Simple Symmetric Key Algorithm. *International Journal of Innovative Research in Computer and Communication Engineering, 1*(8), 1741-1748.

[27] Poongodi, P., & Betty, P. (2014, January). A Study on Biometric Template Protection Techniques. *International Journal of Engineering Trends and Technology (IJETT), 7*(4).

[28] Prakash, O., & Bharathan, D. (2012, March). A New Palm Print Based Fuzzy Vault System for Securing Cryptographic Key. *International Journal of Information and Electronics Engineering, 2*(2).

[29] Radha, N., & Karthikeyan, S. (2010, July). A Study on Biometric Template Security. *ICTACT Journal on Soft Computing*(01), 31-41.

[30] Radha, N., & Karthikeyan, S. (2011, July). An Evaluation Of Fingerprint Security Using Non-Invertible Biohash. *International Journal of Network Security & Its Applications (IJNSA), 3*(4)

[31] 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.

[32] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). An Analysis of Minutiae Matching Strength. *Proceedings of Third International Conference on Audio and Video-Based Biometric Person Authentication (AVBPA)* (pp. 223–228). Halmstad: Sweden.

[33] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security*.

[34] Schmitt, V., & Jordaan, J. (2013, April). Establishing the Validity of Md5 and Sha-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in these Algorithms. *International Journal of Computer Applications, 68*(23), 0975 – 8887.

[35] Zhou, X., & Tang, X. (2011). Research and Implementation of RSA Algorithm for Encryption and Decryption. *The 6th International Forum on Strategic Technology*, 1118-1121.