Contents lists available at Science-Gate

International Journal of Advanced and Applied Sciences

Journal homepage: http://www.science-gate.com/IJAAS.html

Biometric covert acquisition protection by enhancing sweat glands and cryptography

Noor-Ul-Qamar *, Kamran Mustafa

Computer Science Department, Lahore Garrison University, Lahore, Pakistan

ARTICLE INFO

Article history:
Received 25 July 2017
Received in revised form
19 October 2017
Accepted 19 November 2017

Keywords:
Covert
Spoof attacks
Rejection of service
Biometric cryptosystems
Template protection scheme

ABSTRACT

Various biometric technologies were developed and effectively used around the world which includes fingerprints, face, iris, palm-print, speech and signatures. Fingerprints are most preferred mainly due to low cost of algorithms and sensors. Spoof attacks and template leakage are the major vulnerabilities to biometric authentication system. A biometric authentication plan with template protection is an opposition to almost all types of adversaries. If someone's biometric template which is stored in the database of the system is compromised, it might result in identification theft of that person. In this paper template protection scheme with security approaches and effective preventions regarding spoof attacks are proposed having possible secure authentication through detection of sweat glands and application of cryptography techniques.

1. Introduction

Biometrics has various applications all around the world. Various biometric technologies were developed and effectively used around the world which includes fingerprints, face, iris, palm-print, speech and signature. Biometric systems are based on matching of two samples of same individual but there can be errors which can cause harm to authentication security. However Biometric frameworks are not perfect and are powerless, that includes the templates being stored. A stolen format prompts interruption and various other attacks. Several procedures have been intended to enhance the security of formats. The equipment approaches include enclosed acknowledgment framework where the biometric layouts never leave a physically secured module, for example, hand-held gadget. The card or gadget may contain just the layout and the matcher (coordinate – on – card) or the entire biometric framework including sensor, template, highlight extractor, format and matcher (framework–on–card). A key is released in this mechanism if the authentication of the biometric trait gets successful. A product based answer for format for security is stored as an altered adaptation of the layout, being ordered as 1) layout modification and 2) and biometric cryptosystems (Nagar et al., 2010). A template leakage is a serious issue because once a template is stolen it cannot be replaced with new one because biometric traits are irrevocable; there are two major approaches to secure a biometric template discussed in the content along with the solution like mixing of two fingers for protection of fingerprint template that will also prevent spoofing which is one of the major issue concerning the user interface of the system.

1.1. Problem statement

Spoof attacks at the user interface and template leakage of the user's biometric data are major issues concerned with the security of biometric authentication.

2. Biometric authentication

2.1. History of biometric

Allah has blessed all the individuals with some features that are specific to each individual. These features makes each of us distinct from each other, like shape of face, body stature, voice pitch and physical appearance etc. Paris was the first country to recognize criminals on the basis of these features in 19thcentury.As the idea became popular it was later on coupled with upcoming technologies and generates a way of technical identification known as biometric identification. Fingerprints readers were merged in it that totally changed the way of criminal

* Corresponding Author.
Email Address: noorulqamar@lgu.edu.pk (N. Ul-Qamar)
https://doi.org/10.21833/ijaas.2018.01.009
2313-626X/

investigation. This makes crime investigation much more reproductive as it was revealed that each person has a unique finger print. From this it was revealed that finger print of each living being is unique to them so data was compiled of each individual's fingerprints. However this capability was introduced in various corporations and institutions for security purposes and in mankind for e.g., to monitor the attendances of employees.

2.2. Biometric and its system operations

The word biometric has actually originated from Greek language bio (life) and metric (to measure). Biometric is basically a study of biological characteristics which can be statistically measured. In computer security biometric refers to authentications techniques, depending on measurable physical characteristics that can be automated checked. A biometric system refers to identify the person or biological organism by using the information about unique biological traits. It firsts captures the biometric property of the users using a suitable sensor such as face to face camera while enrolling. It then produce the noteworthy attributes such as finger print memory through a software from a biometric sample referred to as the feature extractor. These features are saved with other detectors such as name or identification traits. For the purpose of identification, another biometric sample is provided to the sensor. The properties taken out from this query is then matched to already stored identifiers in database through biometric matcher. Then a contest store is given back by the matcher that resembles the extent of resemblance between the query and the template (Robinson et al., 2017).

2.3. Types of biometrics

There are two main types of biometric techniques commonly used. These are:

- Physiological biometrics
- Behavioral biometrics

This various level of categorization of biometrics can be well understood with the help of Fig. 1.

Further details of the techniques are also mentioned.

2.3.1. Physiological biometric

a. Eye recognition: There are two methods used in eye recognition which are Iris recognition and Retina recognition. Retina recognition is more useful. The person sees into the lens or laser which scans the retina. The arrangement of blood vessels in retina is studied by the device. Each eye has significant arrangement so it is too risky to fool (De et al., 2016).

b. Fingerprints: This is the most common and oldest method used in physiological authentication. It is based on the authentication of the fingerprint of someone, analyzing the characteristics of finger prints. The impression left by the friction ridges is scan by the optical machine.

c. Face recognition: Face recognition technique makes a use of commonly used photo camera like a digital camera having low resolution. In this method the live capture or digital image is compared to the stored record for that person. It is not much useful as one only need a single capture (Scherhag et al., 2017).

d. Handprints recognition: The recognition of the handprints is a part of this mechanism. A scanner is used as a medium to extract a picture of a user's hand. It is similar to the finger print recognition. The ridges in the palm or the length of the fingers are unique to each person. They are then matched by the stored image. This may not help to recognize in the case of twins.

e. Voice recognition: This method evaluates on the recognition of voice of a person. The user verbalizes in a microphone, and his recorded voice is then computed. The frequency and pitch helps to identify the speaker as frequency and pitch are significant for the single speaker. This method is not much appreciated because there is not always 100 % accuracy.

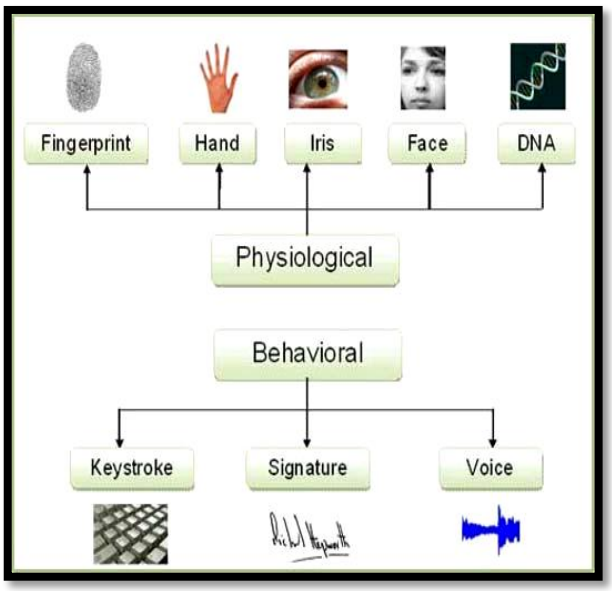

Fig. 1: Categorization of biometrics

2.3.2. Behavioural biometric

As mentioned above the examination of biological and physiological features of human beings are focal points of physical biometrics but opposing to that behavioral biometric mainly focus on studying non-physiological and non-biological features of human beings.

a. Signature verification: Each person has a unique signature. When the person does his signatures on the tablet or any touch screen these are matched to the already saved signatures. In this way identification is done.

b. Gait verification: It functions by analyzing the activity of an individual. The walking of an individual is scanned by a camera and by processing some numerical function on the inclination of the lower limbs and the rate of recurrence of the balancing of the body; it offers you a good authentication method.

It works by examining the movement of a man. A camera checks the client's gait and by figuring some scientific capacity on the variation of the legs walking, the recurrence of adjustment gives an appropriate verification strategy.

c. Keystrokes analysis: Keystroke analysis uses the rhythm and manner in which letters are being typed on the keyboard by the user, however a problem can occur when a person is doing a job in a different mode. Likewise if he is in stress mode his pattern may be different than the real one. This is considered the most reliable and easiest method of authentication to be implemented (Coakley et al., 2016).

3. Vulnerabilities of biometric system

When identification and authentication through physical or behavioral biometrics fails then a biometric framework becomes defenseless against two sorts of failures. A rejection of service happens when the machine doesn't identify a right consumer, while an intrusion points towards the taking possession of the property of another. Reasons of failure may be because of intrinsic restrictions. Authentication of biometric system is founded on corresponding of two biometric specimens.

Two types of authentication errors can be made by the system. False, Non-match is when there is low similarity between the two tests of the same person and the system could not recognize them. When two samples from different persons have close similitude then a false match occurs and the system erroneously proclaims them as a replica.

4. Biometric template security

4.1. What is a template?

A basic step in lessening the privacy and security threats related to biometric frameworks is the confirmation of the protection of biometric templates being stored in the database. A biometric layout is a computerized portrayal of the particular components that are removed from a biometric test and is then stored in a database.

The biometric sample with the aid of truly opposite engineering is proven in the Fig. 2.

Unlike passwords and identification playing cards, it is not viable to update stolen templates with new ones due to the fact biometric developments are irrevocable. So, the stolen biometric templates can be utilized for sakes like, to secretly track a person throughout multiple systems or acquire non-public facts.

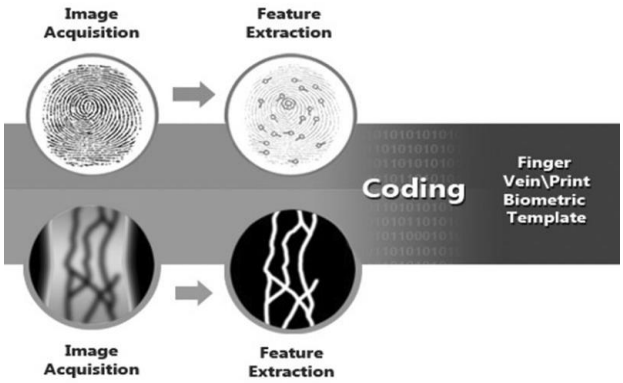

Fig. 2: Extracted features from the sample are stored as coded information in the data base

The escape of layout database implies a circumstance where a unique client's biometric format data winds up noticeably realistic to equal. This compounds the issue of spoofing in light of the fact that it makes it less demanding for the attacker to recoup the biometric design by just figuring out the layout.

Not at all like passwords and ID cards, is it therefore impractical to replace stolen formats with new ones keeping in view that the biometric qualities are unavoidable. Along these lines, the stolen biometric layouts can be utilized for purposes like, to track a man over numerous frameworks or get private data (Selwal and Gupta, 2017).

4.2. Requirements for template security

As templates are used in biometric authentication process so they must be secure. To create a scheme for biometric template protection it is important that these requirements should be achieved.

•**Non invertible -** It should recoup the biometric properties from the database. This continues the programmer from performing the biometric features gotten from the layout or making bodily spoofs of the biometric characteristic.

•**Hold accuracy**. The template safety scheme shouldn't degrade the authentication accuracy of biometric platform.

•**Revocability**- It must be conceivable to make numerous protected layouts from the synonymous biometric information that is not related to that information. This factor not just empowers the biometric framework to drop and reprints fresh biometric layouts if the database is compromised, however it likewise anticipates cross-matching over databases, thus protecting consumer's data and reclusiveness.

4.3. Approaches for template security

Two main approaches for securing a biometric template are:

i. Biometric Feature Transformation

ii. Biometric Cryptosystems

4.3.1. Biometric feature transformation

In this approach a secure template is created by applying a transformation function in a way that reconstructing of original template from it is computationally hard. This transformation is based on user-specific parameters. In recognition phase transformation occurs at input biometric template with same user-specific parameters and the transformed template is then matched with the transformed template stored in the database.

The main advantage of this technique is that if a person has transformed his biometric on a separate device and sends only the transformed template to biometric machine then the original template is never disclosed.

4.3.2. Biometric cryptosystems

Biometric cryptosystem is the coupling of cryptography technique and biometric system as the name of the topic suggests. It is actually combined to take advantages from the respective fields. Basically biometric ensures that the party they are in contact with should not be able to repudiate their signatures on the documents. While cryptography adjusts the level of security, helps in authentication and coding.

4.3.2.1. Key release based on biometric

A cryptographic key is kept in reserved as user documentation. After authentication is successfully authenticated, this key is used. Because of biometric discrepancy it is not practicable for most biometric properties to extricate key immediately. There are approaches of template security to verify biometric sample which is done by template comparison as shown in Fig. 3.

In key binding biometric cryptosystems high random keys are developed and are concealed by users biometric. This data is known as helper data. This helper data safely save the data during the phase of enrollment and use to recover key with biometric in recognition phase. In key generation biometric cryptosystem, helper data is acquired only from the biometric template (Zhou et al., 2016; Chuah et al., 2017).

4.3.3. Open issues and challenges

1. **Issue of adjustment:** This issue significantly affects the working of biometric system as there arises the dissimilarity between the results in enrollment phase and recognition phase.
2. **Not sufficient or well-founded information:** It is not clear that which biometric characteristic should be applied on which application.
3. **No optimal error correction:** Biometric data are severely noisy and many researches have to be done to discard noise. As biometric performs work in noisy data so error correction code is used.
4. **Securing biometric features:** Biometric data may not be secret. There are many chances that data may be stolen. Proper security must be provided to the unique biometric data to insure the safety of data.

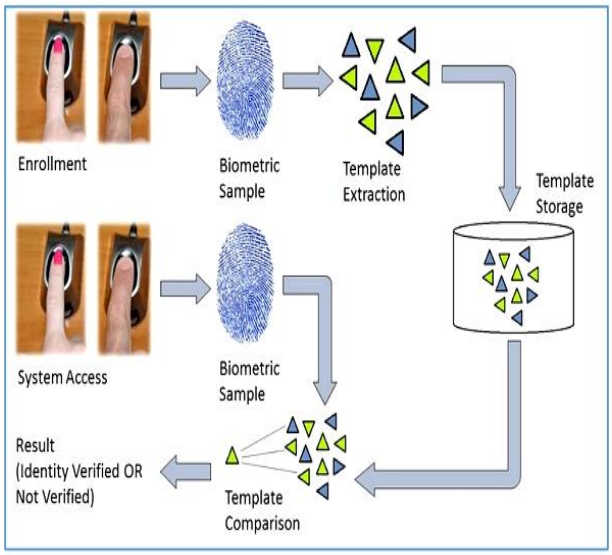

Fig. 3: Approaches of template security

5. Hacking of biometric authentication systems and its solutions

Biometric systems are the emerging technology of detection and investigating all sorts of crimes and it is a mean of ensuring security in all applicable areas of our daily life.

However, there are ways to hack the authentication techniques of biometric systems. Possible means of hacking and their preventions are discussed.

5.1. Key generation mode of biometric cryptosystem

To customize the security of all the above said approaches, it is recommended to join a few biometric to shape single multi-biometric format. Presently this multi-biometric layout can be utilized as a part of key era, key authoritative and in addition key discharge mode. To upgrade the security of all the above said approaches, it is proposed to join a few biometric to shape single multi-biometric format.

Presently this multi-biometric layout can be utilized as a part of key era, key authoritative and in addition key discharge mode. This key is not put away in the database. The significant issue with this framework is that key is not put away in database framework.

The larger amount of security in this framework can be pick up by sending the key code to a validated versatile number or mail ID for which likewise imperative can be offered identified with expiry of this key inside a particular time which will

additionally decrease chances for a man to get into the framework. Key generation by means of extraction of features and data is shown in Fig. 4.

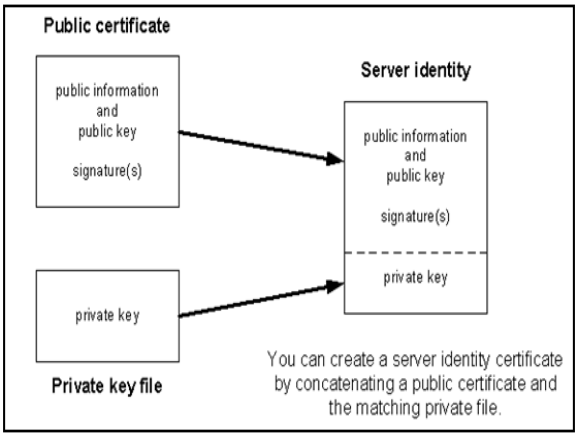

Fig. 4: Key generation

5.2. Attacks on biometric system

Biometric framework can be smacked by an encroacher with various sorts of assail on the framework. Biometric framework can be assaulted at different level. There are 8 unique pivots at biometric framework can be attacked violently. As a whole the decision is concerned by means of these attacking points as shown in Fig. 5.

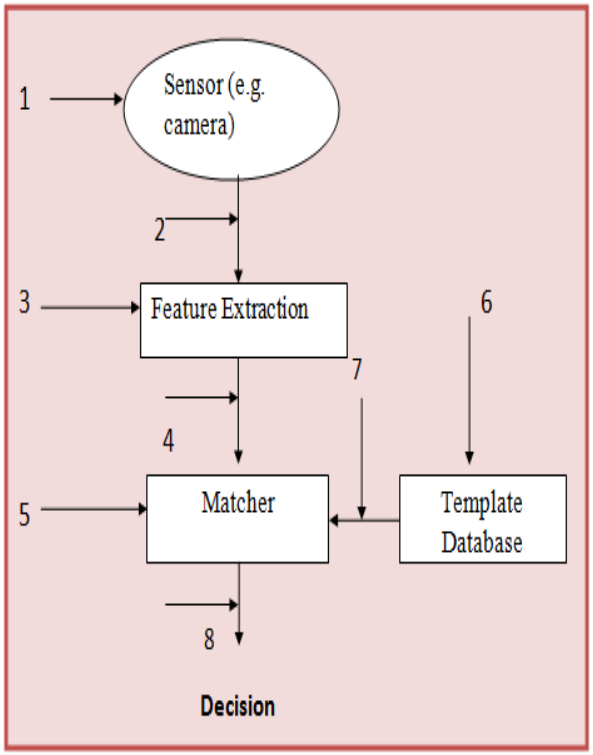

Fig. 5: Attacking points on biometric system

5.3. To overcome fake biometric attacks

Software's-based techniques for unique mark livens identification. They utilized a monetarily accessible sensor and the sole contribution to the livens identification module is a 5-second video of the fingerprints. The periodicity of sweat pores along the edges is utilized for livens identification.

Sweat distribution design after some time along the ridges is measured. Dummy fingerprints play uncooked. A back stimulator neural system classifier is used to recognize live fingers from dummy fingers.

- False acceptance attack
- Linkage attack.

5.3.1. False acceptance

At the point when the framework accepts the client accepting it is real despite the fact that it is definitely not. FA of 0.02% implies that out of 105 examples of a biometric any one may have identical constituents as that of enrolled biometric. FA attacks can be made on the off chance that one is approaching biometric database.

Prevention: This kind of attack can't be preventing by format insurance plans talked about above.

5.3.2. Linkage attack

It is otherwise called linkage attack. On the off chance that unique applications are making use of similar biometric for distinguishing proof, comparable personalities of same individual might be put away in various databases. Diverse application might be matched misusing the character.

Prevention: With a specific end goal to keep this attack, Template insurance plan can be utilized. In format assurance plot, distinctive pseudo (false) personalities are produced from same layout. These pretentious characters are self-governing and crooked as a result linkage can be stayed away from.

6. Cryptography

Cryptography is a technique of storing and transmitting records in a selected shape so that best the ones for whom it is supposed can study and method it. It is nearly associated with the fields of cryptanalysis and cryptology. Cryptography includes techniques of merging words with snapshot, different methods to hide statistics in garage or transit and techniques of microdots. But, in modern computer open-class world, cryptography is most usually related with scrambling plaintext (normal textual content, may be called clear text) into cipher text (a manner known as encryption), then returned again (called decryption). People practising this discipline are called cryptographers.

6.1. Current cryptography

Modern cryptography is extremely in panoramic view of software engineering rehearse and numerical hypothesis; cryptographic calculations are com computational hardness suppositions composes

of cryptographic calculations, making such calculations hard to soften up practice by means of any enemy. It's far hypothetically manageable to interrupt this type of framework, but it is impracticable to do as such through any recognized reasonable approach. Those designs are consequently named hypothetically advances and computationally cosy E.G. faster figuring invention and improvements in whole variety factorization calculations require these solutions for constant adjustment. There lie information with hypothetical plans that likely cannot earn back the original investment with infinite figuring energy—an example is the one-time cushion—yet these plans are greater difficult to represent than the first-class hypothetically brittle however computationally relaxed components of encryption keys for statistics applicable to an investigation (Sharma and Rajawat, 2016).

6.2. Cryptography use in copyright encroachment

Cryptography assumes a notable element in automatic rights management and copyright encroachment of advanced media. Symmetric-key cryptography eludes to encryption techniques wherein both the sender and recipient provide a comparable key (or, less typically, wherein their keys are exclusive, but associated in an efficiently calculable manner). This turned into the primary type of encryption freely recognized till June 1976. Intent chart indicating international records Encryption algorithm parent handle

One round (out of 8). Five of the idea determine, applied as part of a few sorts of PGP for fast encryption of as an example, email Symmetric key figures are carried out as either rectangular figures or movement figures.

A square figure enciphers contribution to pieces of plaintext in preference to person characters, the info frame utilized by a flow figure.

6.3. Symmetric key cryptography

Symmetric key cryptography makes use of a comparable key to scramble and decode data. Some everyday symmetric key calculations are the Triple DES, Blowfish, the superior Encryption general(AES) and records Encryption popular (DES), DES is insufficient in light of the fact that it makes use of a sixty four-bit key and has been broken. Be cautious, given that some crypto protection, much like Microsoft's home windows XP Encrypted document system (EFS), defaults to DES and should be modified to present extremely good safety. Pace is the primary preferred viewpoint of symmetric key cryptography. The rule troubles with this framework are key appropriation and flexibility. Keys ought to be disseminated competently, and every included channel desires a different key. Symmetric key frameworks give classification but don't give genuineness of the text, and having sent the message can be denied by the sender.

6.3.1. Asymmetric cryptography

A pair of mathematically associated keys is used by Asymmetric (public) key. Each key may be utilized for encryption or decryption. But, a key can only decode a message that has been encoded by the aid of the associated key. The important thing pair is referred to as the general public/private key pair. A few not unusual public key systems are virtual signature preferred (DDS), Diff-Hellman and Rivets-Shamir-Adelman (RSA). Uneven key frameworks supply a greater noteworthy scope of safety administrations than symmetric frameworks. They accommodate privacy, validity and non-repudiation. Speed is the usual problem with those frameworks. More computer belongings are fundamentally taken to encode and decode with awry frameworks than symmetric ones (Rani and Kaur, 2017).

6.3.2. Cryptographic hashing

The manner in the direction of developing a settled length string from a message of subjective length is known as cryptographic hashing. In this occasion the sender offers a cryptographic hashing of the message, the beneficiary can examine its erectness. Current cryptographic frameworks depend upon complicated numerical methods and connections

7. Conclusion

To identify an individual sharply and to make biometric template more secure double finger prints and 5 secs video software is also one of the best methods for prevention of spoofing because biometrics are restricted for an individual, it is required to be protected to be stolen or misused.

We were concerned about the spoof attacks at the user interface and template leakage of the users data as these are major issues concerned with the security of biometric authentication so this research has put forward some methods of protecting the biometric finger prints and templates to make it more safe keeping in consideration the covert acquisition of the protection schemes. The study also gives the solution to protect it more securely by means of cryptography thus possible attacks that can be prevented to make several biometric identities system more secure and safe are discussed as a whole.

References

Chuah CW, Deris MM, and Dawson E (2017). On the Security analysis of weak cryptographic primitive based key derivation function. In: Kim K and Joukov N (Eds.), Information Science and Applications 2017. ICISA 2017. Lecture Notes in Electrical Engineering, 424. Springer, Singapore. https://doi.org/10.1007/978-981-10-4154-9_27

Coakley MJ, Monaco JV, and Tappert CC (2016). Keystroke biometric studies with short numeric input on smartphones. In the IEEE 8th International Conference on Biometrics

Theory, Applications and Systems (BTAS), IEEE, Niagara Falls, NY, USA: 1-6. https://doi.org/10.1109/BTAS.2016.7791181

De P, Ghoshal D, and Deb T (2016). Dual authentication of a human being from simultaneous study of palm pattern and iris recognition. Indian Journal of Science and Technology, 9(35): 1-6.

Nagar A, Nandakumar K, and Jain AK (2010). Biometric template transformation: a security analysis. In the SPIE Media Forensics and Security, Electronic Imaging, San Jose, USA. https://doi.org/10.1117/12.839976

Rani S and Kaur H (2017). Technical review on symmetric and asymmetric cryptography algorithms. International Journal, 8(4): 182-186.

Robinson TL, Schildt BR, Goff TV, and Corwin DJ (2017). System and method for enrolling in a biometric system (U.S. Patent No. 9,544,309). U.S. Patent and Trademark Office, Washington, D.C., USA.

Scherhag U, Raghavendra R, Raja KB, Gomez-Barrero M, Rathgeb C, and Busch C (2017). On the vulnerability of face recognition systems towards morphed face attacks. In the 5th International Workshop on Biometrics and Forensics (IWBF), IEEE, Coventry, UK: 1-6. https://doi.org/10.1109/IWBF.2017.7935088

Selwal A and Gupta SK (2017). Low overhead octet indexed template security scheme for multi-modal biometric system. Journal of Intelligent and Fuzzy Systems, (Preprint), 32(5): 3325-3337.

Sharma S and Rajawat AS (2016). A review on possible attack in privacy model and modification technique. Imperial Journal of Interdisciplinary Research, 2(12): 1972-1975.

Zhou Y, Zhao B, Han J, and Zheng J (2016). An effective scheme for biometric cryptosystems. In 2nd IEEE International Conference on Computer and Communications (ICCC), IEEE, Chengdu, China: 241-244. https://doi.org/10.1109/CompComm.2016.7924701