© Universiti Tun Hussein Onn Malaysia Publisher's Office

IJIE

Journal homepage: http://penerbit.uthm.edu.my/ojs/index.php/ijie

The International Journal of Integrated Engineering

Security Features in Fingerprint Biometric System

Kamarul Zaman Panatik[1], Kamilia Kamardin[2,3*], Siti Nurhafizza Maidin[1], Ngu War Hlaing[2], Irfanuddin Shafi Ahmed[1], Noureen Taj[4], Hazilah Mad Kaidi[1]

[1]Razak Faculty of Technology and Informatics,
Universiti Teknologi Malaysia, Kuala Lumpur, MALAYSIA

[2]Malaysia-Japan International Institute of Technology,
Universiti Teknologi Malaysia, Kuala Lumpur, MALAYSIA

[3]Wireless Communication Center,
Universiti Teknologi Malaysia, Kuala Lumpur, MALAYSIA

[4]B. S Abdur Rahman Crescent Institute of Science and Technology,
Computer Science Engineering, Chennai, INDIA

DOI: https://doi.org/10.30880/ijie.2020.12.06.004
Received 08 April 2020; Accepted 28 May 2020; Available online 02 July 2020

Abstract: Nowadays, embedded systems run in every setting all around the globe. Recent advances in technology have created many sophisticated applications rich with functionality we have never seen. Nonetheless, security and privacy were a common issue for these systems, whether or not sensitive data can be protected from malicious attacks. These concerns are justified on the grounds that the past of security breaches and the resulting consequences narrate horrific stories concerning embedded systems. The attacks are now evolving, becoming more complex with technological advancements. Therefore, a new way of implementing security in embedded systems must be pursued. This paper attempts to demonstrate the incorporation of security features in fingerprint biometric system in the requirements analysis phase, ensuring the same throughout the system life cycle of embedded systems based on case study. The comparison of various biometric technologies such as face, fingerprint, iris, palm print, hand geometry gait, signature, and keystroke is presented. The aim of this paper includes analyzing, decomposing and transforming the threats and counter-measures identified during the requirements analysis using the abuse case into more specific safety requirements or functions. Furthermore, we have shown that the incorporation of security features into the biometric fingerprint system by analyzing the requirements of the system and providing the main steps for the protection of the biometric system in this paper.

Keywords: Threats, countermeasure, abuse case, fingerprint, information leaks

1. Introduction

An automated biometric system uses the characteristics of human beings such as behavioral, physiological, and biological characteristics for the authentication of individual identity based on a previous enrollment event. The reason that makes these characteristics ideal for human identification is due to several essential qualities such as universality, uniqueness, permanence and collectability [1]. These four qualities can be described as follow:

1. **Universality** – Every person possesses the same characteristic that a normal human being does.
2. **Uniqueness** – Every person has a unique characteristic. That is, no two individuals possess the same characteristic.
3. **Permanence** – The characteristic is time invariant. It does not change in time.
4. **Collectability** – The characteristic can be quantitatively measured and is easily available to collect.

**Corresponding author: kamilia@utm.my*

Biometrics have been part of impressive, ongoing research efforts to study their use and fitting application. These can be implemented in the current context. Some of the popular biometrics used today are voice, face, retinal scan, iris, ear, hand & finger geometry, imaging, DNA, infrared facial thermography, and fingerprints. Technological advancements have now led to the tremendous development of this domain.

Biometrical authentication [2] applies to human identification focused on the features of their physiological and behavioral characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc. It is more secure than password-based authentication, provided that biometric features cannot be missed or overlooked compared of passwords being lost or forgotten. Copying, sharing, and distribution is extremely difficult compared of passwords being announced in hacker websites. Moreover, the person authenticated shall be present at the time and location of authentication, as opposed to conniving users who dispute that the password has been exchanged. Biometrics are challenging to counterfeit and a customer is unlikely to repudiate the exposure to digital content through biometrics.

Eventually, biometrics for one user cannot crack faster than others; in other words, every user has a relatively equal level of safety. Thus, not many users can mount an attack against biometrics that are "easy to guess". Therefore, biometric authentication will substitute password authentication with either the full authentication method or the standard cryptographic keys that hold the multimedia file in the digital rights management (DRM) system [3].

Meanwhile, these technological advancements have not only spurred the advancement of fancy functional features of this technology, but have also welcomed the sophistication of security attacks. History has witnessed many instances of such security breaches in the hardware-software applications and these seem to evolve with time. Specifically, in biometrics using fingerprint authentication, any attacker could perform a brute-force attack or simply present the duplicate of a known person's biometric to the system [4].

The fact that makes biometric data unique is because of its ideal way of easy authentication that replaces passwords, or complements them. However, the impact of losing biometric data to malicious persons is something that is not recoverable. This is because they stand by our identification, part of something we are or have. A stolen password can easily be updated or changed but stolen biometric data such as fingerprints cannot be changed or removed [5]. Thus, this research will address the security concerns in biometric identification using fingerprint. Specifically, this paper will attempt to address the side-channel information leaks in fingerprint biometric.

In this paper, biometric system with comparison of different body traits in universality, uniqueness, permanence and collectability are presented in Section 2. The security features in Fingerprint Biometric in Section 3 and the requirements analysis based on the risk associated to each element of the biometric system together with direct attack and indirect attack in Section 4 are shown respectively. Moreover, in section 5, the results and discussions demonstrated the functional analysis and allocation of the threat and countermeasures and the design synthesis of the biometrics system in terms of physical elements. Then, finally, this paper is concluded in Section 6.

2. Biometric System

For different applications, a variety of biometric technologies have been used. The strengths and weaknesses of each biometrics depend on their application. No biometrics shall meet the demands (e.g., accuracy, practicality, cost) of all applications (e.g., DRM, access control, welfare distribution) effectively. In other terms, there is no "optimum" biometrics. Examples of body traits that can be used for biometric recognition are face, fingerprint, iris, palm print, hand geometry, and ear shape; while gait, signature, and keystroke [6].

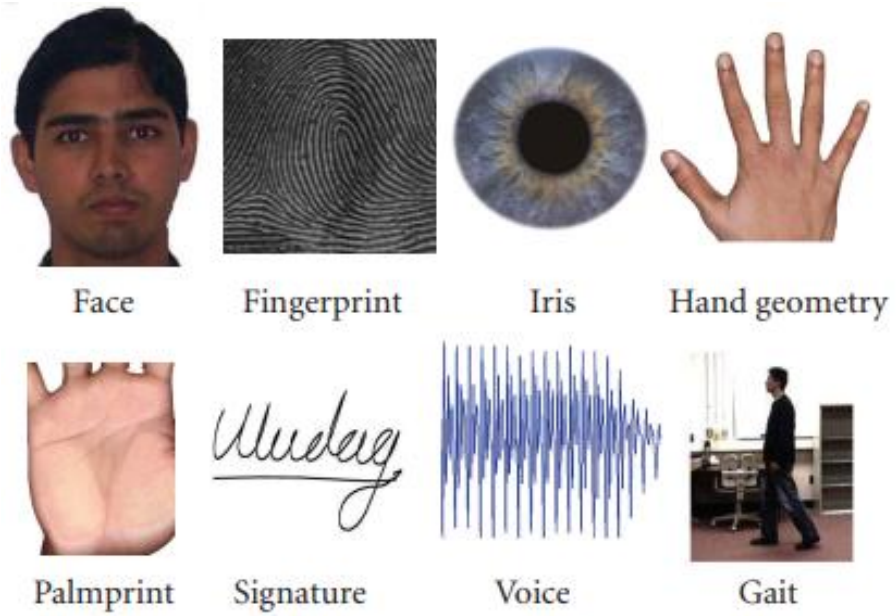

Fig. 1 - Examples of body traits that can be used for biometric recognition [6]

In Table 1, the comparison of various biometric technologies is categorized. High, Medium, and Low are denoted by H, M and L respectively. The match between a specific biometric and an application is determined depending upon the requirements of the application and the properties of the biometric characteristic.

Table 1 - comparison of various biometric technologies [7]

Biometric Identifier	**Universality**	**Uniqueness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**
Face	H	L	M	H	H	H
Fingerprint	**M**	**H**	**H**	**M**	**M**	**M**
Hand geometry	M	M	M	H	M	M
Iris	H	H	H	M	L	L
Keystroke	L	L	L	M	M	M
Signature	L	L	L	H	H	H
Voice	M	L	L	M	H	H

Biometric systems use pattern-recognition method to recognize a person based on specific behavioral and physiological characteristics. There are two operation modes of biometric system: recognition and verification. The former compares the captured biometric characteristic with the biometric template pre-stored in the database, whereas the latter performs a search on the entire database for a perfect match. Fig.2 shows the block diagram for the identification and verification of the user's data for enrollment.

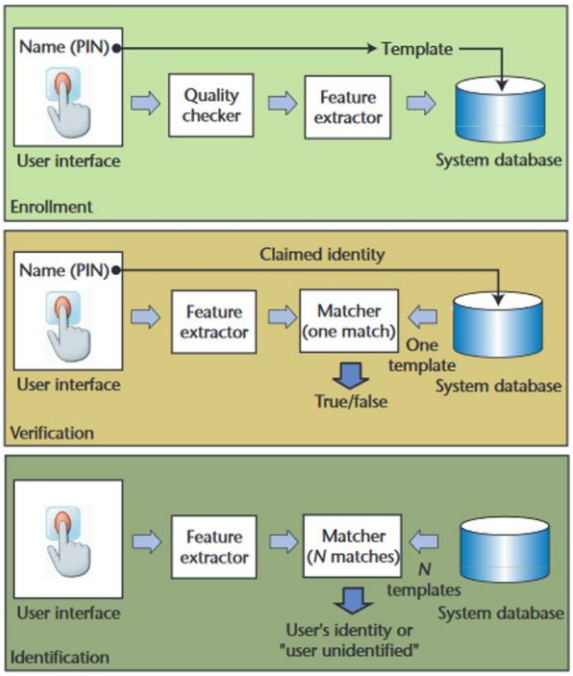

Fig. 2 - Block diagram for Enrollment, Verification and Identification Task

At the enrollment point, the customer applies his finger to the fingerprint sensor and the fingerprint picture is taken from the sensor panel. Some features of the fingerprint picture acquired are extracted and modified or transformed to create prototype data for comparison during verification. During verification, the sensor module collects the fingerprint image of an application. In order to obtain query data, the functional representations of the database fingerprint image follow the same process as the enrollment level. The test data are then reviewed for matching results with the template data. [8].

3. The security features in Fingerprint Biometric

In this paper, incorporation of the security design features of biometrics fingerprint authentication system will be attempted from the early stage in the system life cycle through the design stage based on a case study. The study is based on a system proposed by [9] which is "*Fingerprint Biometric Authentication System for Students Electronic Examination*". For this study, the only focus will be the fingerprint part of the system.

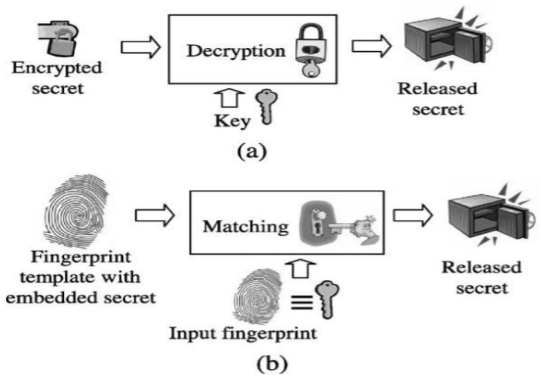

Fig. 3 - A generic instantiation of simple conventional and biometric-based DRM systems (a) password-based Authentication; (b) fingerprint-based authentication [10]

When it comes to biometrics, there are serious privacy issues which include some of the main problems of biometrics: Any collection of data could eventually get hacked. High-profile data can be particularly attractive for hackers. The good news is that high-profile data are more secure. Nevertheless, as biometrics are becoming more common, the biometrics may be accessible elsewhere that cannot use the same secure storage standard.

4. Requirements Analysis

In this stage, the requirements for implementing security of the fingerprint biometric system based on the risk associated to each element of the biometric system will be analyzed. The objective is to identify the possible attacks on the system and then come up with the corresponding countermeasures. According to [11], the possible security attacks for the fingerprint biometrics can occur at certain point of the fingerprint biometrics system as shown in Fig. 4.

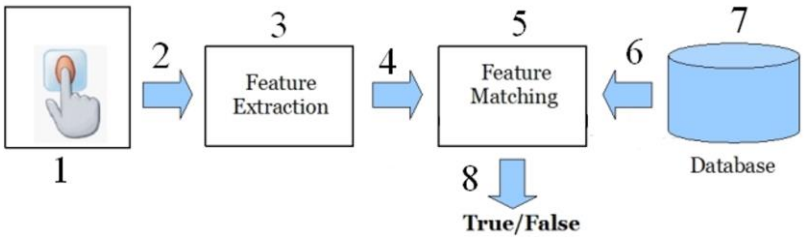

Fig. 4 - Possible attacks against fingerprint biometric [11]

Biometric technologies deliver major benefits over traditional schemes, but are vulnerable to attack [12]. In the biometric method, there are eight threat points which can be attacked as shown in Fig. 5. Such points of attack are classified into two different categories: direct and indirect threats.

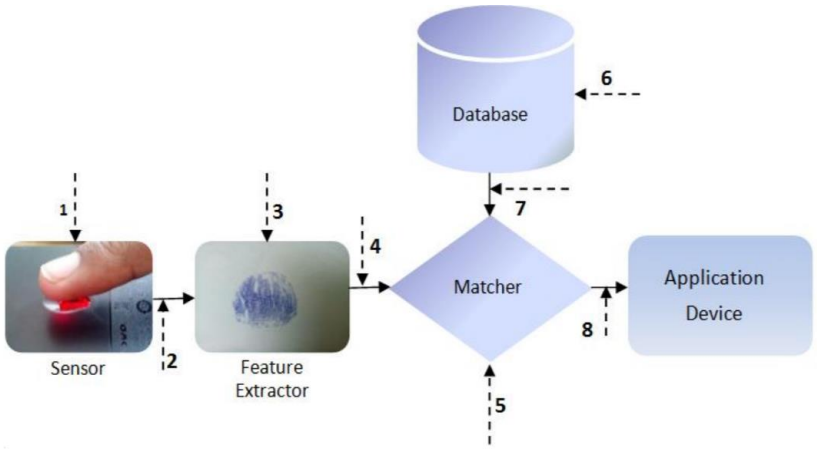

Fig. 5 - Threat points on biometric system [13].

4.1 Direct Threats

It refers to threats which need no special knowledge of the system function, such as the matching algorithm, the vector format function, etc. It contains only Threat 1 known as "Sensor Threat".

Threat 1: The sensor module is vulnerable to threat 1 which is known as “Threat to the sensor”. In this threat, an imposter to bypass recognition systems is shown to the sensor by a fake biometric feature such as an artificial finger or facial image [14]. An imposter may damage the system physically and flood the system with fake requests. Attacking the sensor is very simple because no particular knowledge is needed about device operation. Digital security mechanisms like watermarking are not available, cryptography at sensor level are used. The sensors cannot differentiate between a false and a real person and can easily be fooled by using fake fingerprints and a person's face image.

The flow diagram of direct and indirect attacks is shown in Fig. 6.

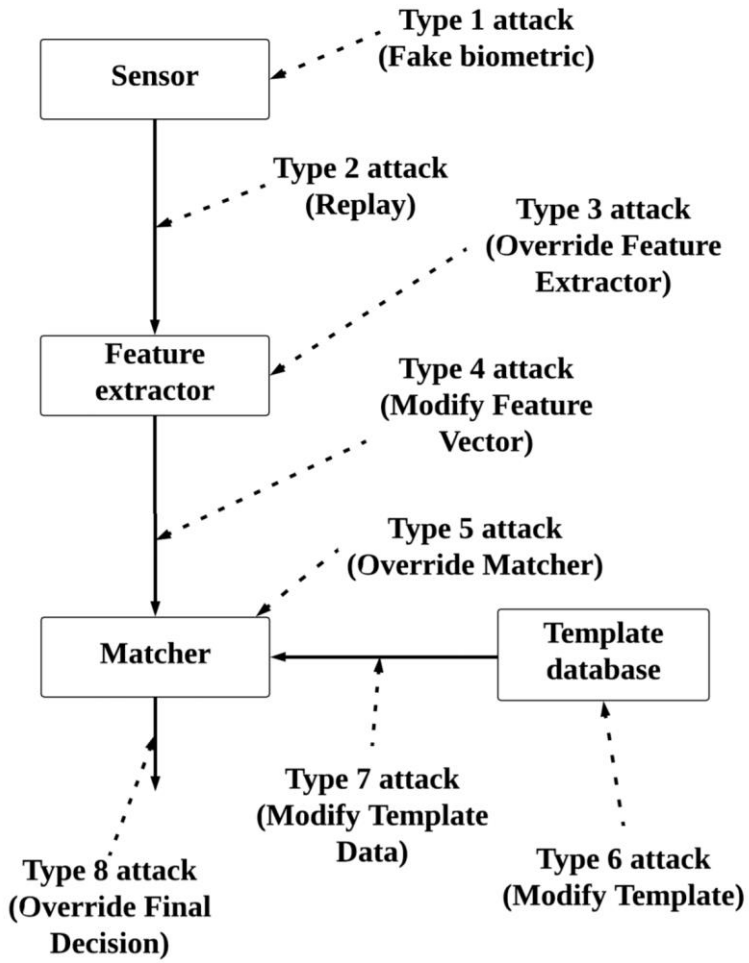

Fig. 6 - Flow Diagram of Direct and Indirect Attacks on biometric system

4.2 Indirect attacks

These are attacks that require information about how the authentication system operates internally, as opposed to direct attacks. It includes all the other seven threat points (2, 3, 4, 5, 6, 7, 8) that an impostor can attack in the biometric authentication system.

Threat 2: When a sensor obtains a raw biometric data, it sends raw data through a communication channel to the feature extractor module for pre-processing. The channel is located between the sensor and the extractor feature. The biometric feature is intercepted and stored somewhere. The biometric feature previously stored is replaced by the function extractor to bypass the sensor. This is known as "replay threat" [14].

Threat 3: The extractor module is vulnerable to Threat 3 called "Threat to the extractor module features". The raw data is sent to an extractor module when the sensor acquires a raw biometric data. The feature extractor module is pressurized in the imposter to generate the function values selected by the intruder, instead of the values extracted from the initial sensor data.

Threat 4: An impostor intercepts the communication channel between the function extractor and match modules and steals the feature values of a legitimate user this attack is equivalent to Threat 2 [14]. It is named "Threat to the channel between the extractor and the play".

Threat 5: A matcher module is vulnerable to threat 5 which is known as "Threat to the matcher module" [15]. The high matching score chosen by the imposter will be produced to bypass the biometrical authentication system irrespective of the input value.

Threat 6: This takes place when the impostor exploits database confidentiality by adding new templates, altering current templates and deleting old templates [15]. It is no easy task to attack system databases, for example by watermarking, and other digital mechanisms. Some knowledge of the internal working of the system must be necessary for successful attacks on the system database.

Threat 7: Threat can only be accomplished by transmitting the prototype via a channel contact between the device database and the match module. It happens when the importer modifies or tamps the content of the template transmitted. An impostor intercepts the canal to steal, substitute or alter the biometric template. It is referred to as "Attack on the communication channel between device and match database".
Threat 8: An impostor will override the result that the matching module declares. This attack can interrupt the match score transmitted via the channel of communication between the matching module and the application device. It modifies the match score to change the module's original decision (accept or reject). After examining these 8 attack points, it is found that opponents target models that are contained in the database most often. The templates contained in the database can be altered by adding new database templates, changing existing database templates and deleting all templates from the database [16].

4.3 Use Cases and Misuse Cases

Use cases are very useful in identifying the practical specifications of users and other stakeholders. The use case describes one or two people engaging with the program to get a job completed. The use case analysis of the program's technical specifications comprises of a well-organized set of use cases reflecting device interface information from the perspectives of members of the different user classes. Usually, any use case reflects how one consumer will communicate with the program. The concept of use case consists of a case diagram, and a sample definition for each scenario. A standard scenario and one or two alternate scenarios are usually presented in the case description.

Misuse cases reflect threats: the multitude of forms in which an intruder engages with the mechanism to circumvent, crack, harm, exploit or misuse the program. A case of misuse is a case of usage from the point of view of an agent averse to the program under design [17]. The aim of a misuse is not to provide system functionality, but to disrupt the system functionality of the consumer situations, which is a hostile agent. Furthermore, misuse incidents often include accidental or unintentional software mistakes and omissions.

Determining protection criteria typically begins with an overview of the properties to be covered, accompanied by risk management and risk analysis. Misuse case-based hazard recognition explicitly tackles this absence. We suggest a method for building threats and security requirements from use cases and misuse cases:

1. First define participants and create a robust framework (representing consumer classes).

2. For any use scenario, imagine and identify whether negative agents attempt to smash their intent or to thwart the measures in the definition of the use scenario; this helps in the most critical cases of misuse. The aim of the brainstorm sessions will be to recognize the various ways in which an attacker can damage the service offered by the aim event. Specifics of these attacks can be decided later. The aim is to define security threats against each feature, location, procedure, data and transaction in the use case from a variety of possible risks such as unwanted internal and external access, denial of service attacks, infringement of privacy, confidentiality and reputation breaches, and hackers. In addition to attack modes, the method will also try to track potential user failures and the device responses. Such errors may also create significant problems in the system's functionality or health.

3. Display the relationships between the usage cases and the relevant misuse situations as in Fig. 6. It will be easier to use terms like "threat" and "steal" to portray such relationships as depicted.

4. After misuse cases have been developed, define the usage of protection cases to combat or thwart the expected intent of will misuse case. According to the Fig. 7, it has shown that a new security use case called “Encrypt the Message” to thwart the “Tap Communication” misuse case. It is denoted that the new use cases “security use cases,” as they do not represent functional requirements of the system.

5. Proceed with steps (2) through (4) for each major use case until one is satisfied that (a) all appropriate risks to specific program functions and resources (as defined by the use case model) are listed and are described as cases of misuse and (b) each of these threats has been thwarted by one or more newly introduced “security use cases”. The new threat analysis approach used by Microsoft offers some valuable guidance to classify risks in usage cases.

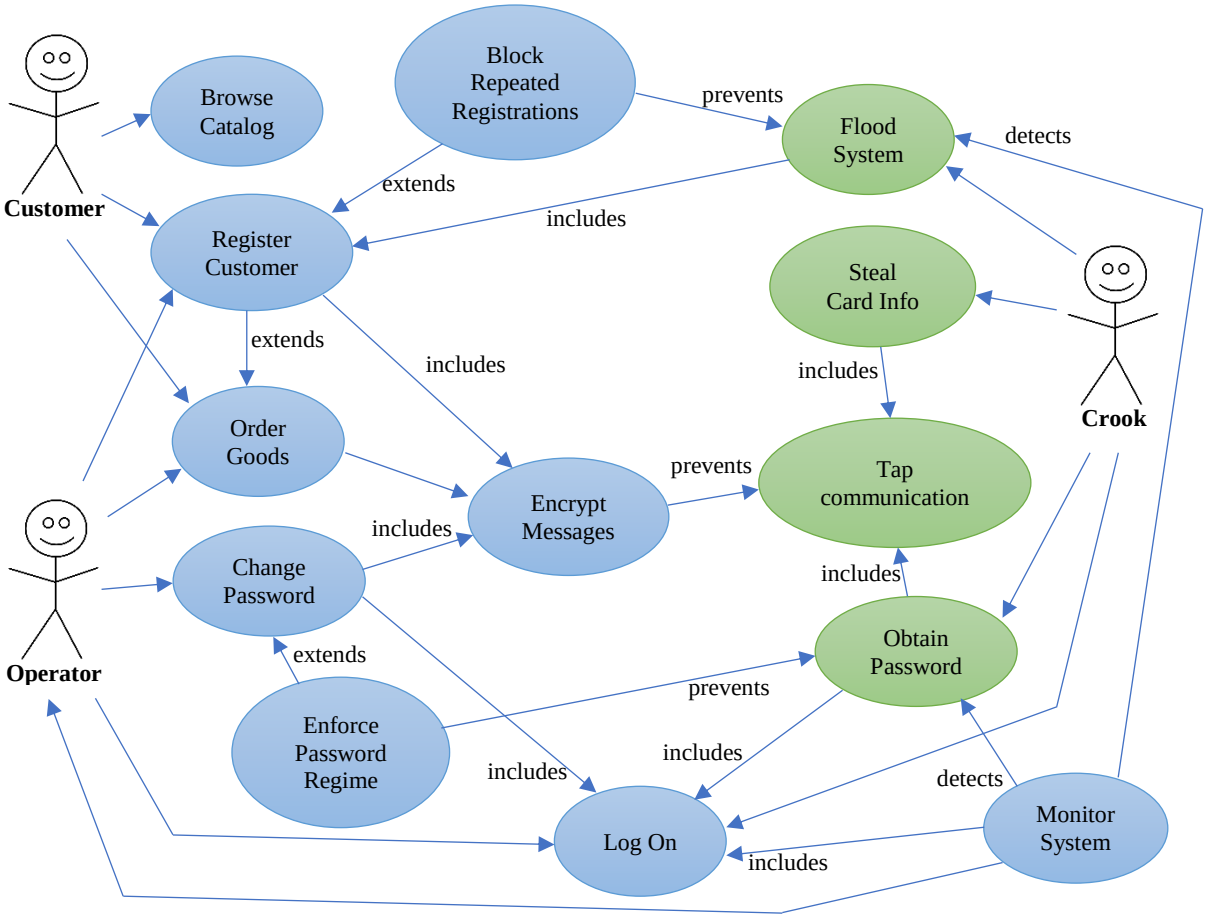

Fig. 7 - Flow Diagram of use and misuse cases

Security standards should be focused on identifying the assets and services that should be protected and the safety risks that should be protected from these assets and services. As shown in Fig. 8, specific relationships between assets and services are vulnerable to safety risks, require security requirements, require protection measures to resolve and thus secure assets and services.

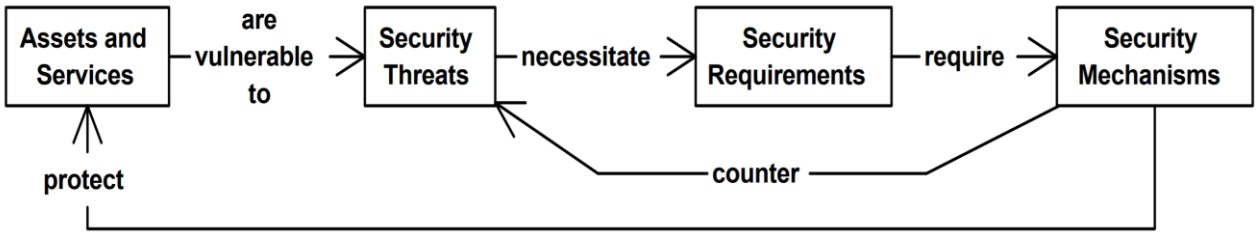

Fig. 8 - Security Threats, Requirements and Mechanisms

Security engineering has traditionally emphasized the creation and use of various protection measures to secure sensitive assets and resources by resolving identified security threats. Analysis and reporting of security risks and specifications received considerably less attention. Developing cases of abuse was a comparatively new approach to resolving security threat analysis. As stated as Fig. 9, misuse cases are specific cases used to examine and identify security risks.

Unlike typical use cases documenting encounters with an application and its users, misuse cases concentrate on encounters between the program and its abusers attempting to breach its protection. Since the success criteria for a case of misuse are a successful attack on an application, cases of misuse are highly useful ways to identify security risks but are inadequate for the study and definition of protection specifications. Instead, security use cases can be used to define specifications for the program to defend itself effectively against its specific security threats.

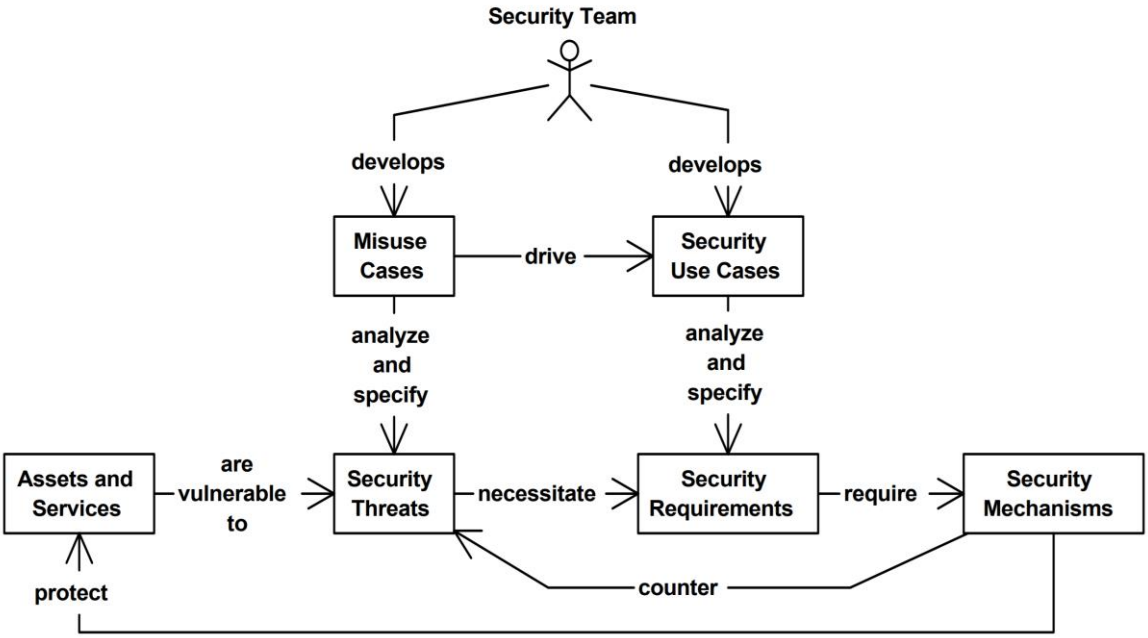

Fig. 9 - Misuse Cases and Security Use Cases

5. Results and Discussions

5.1 Functional Analysis and Allocation

This section aims to further analyses the threat and countermeasures identified during requirements analysis using abuse case, decomposes and transforms them into more specific security requirements or functions. For more about abuse case or security use case, see [18-19].

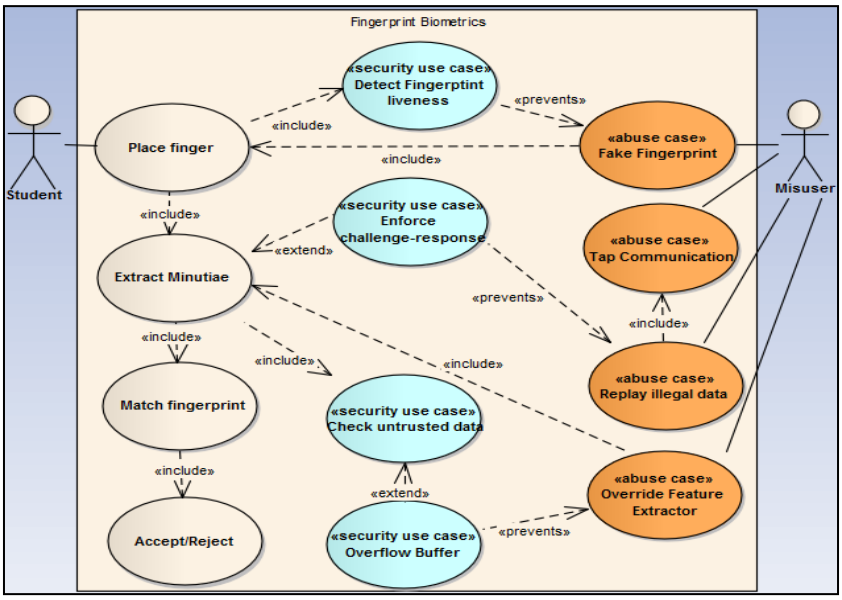

Fig. 10 - Abuse cases and security use cases (part 1)

The abuse cases that were developed based on the identified threat and countermeasures are shown in Fig. 10 and Fig. 11. The green use cases are security use cases needed to prevent the attacks from the Misuser. The orange use cases are the abuse cases which are the possible actions that can be performed by the Misuser in order to attack the system such as injecting a pre-selected feature that was stolen during the transmission between the feature extractor and the comparison component.

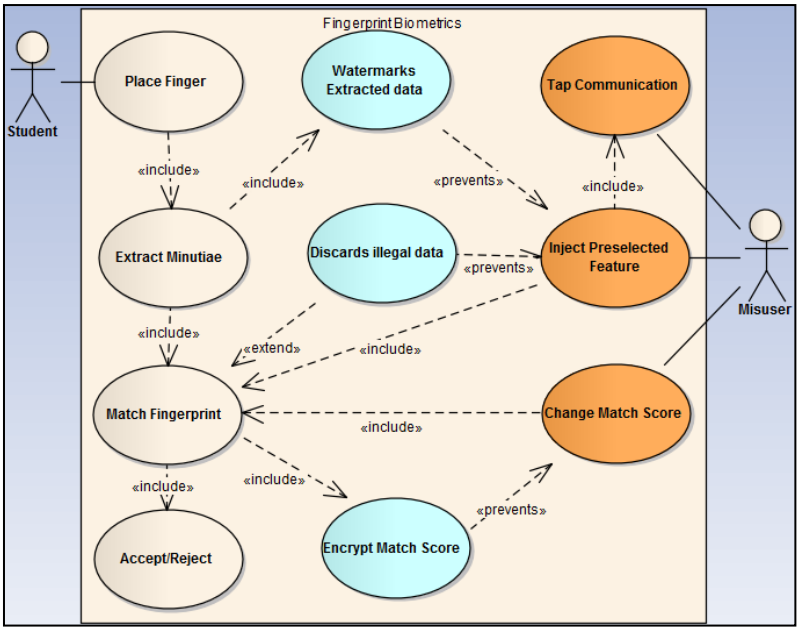

Fig. 11 - Abuse cases and security use cases (part 2)

5.2 Design Synthesis

This section demonstrates the abstract of the biometrics system in terms of physical elements that make up the whole fingerprint biometric system.

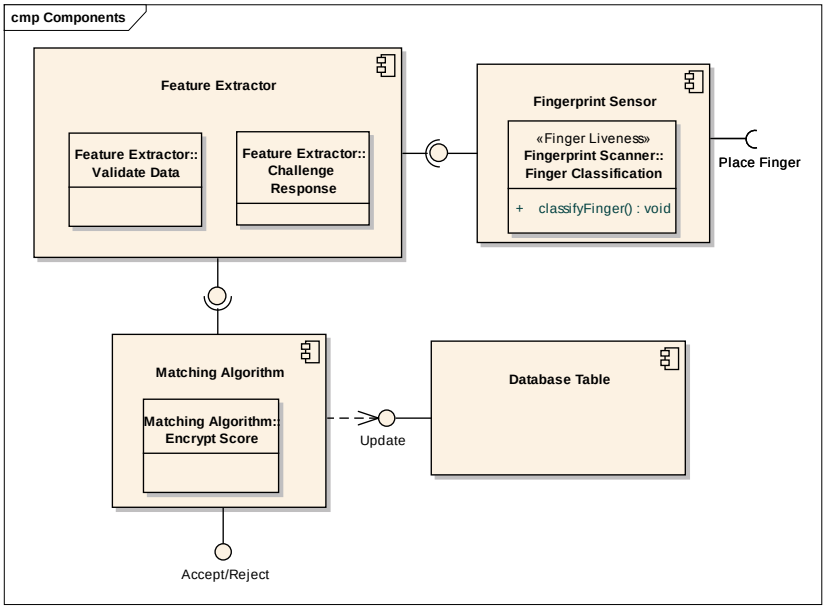

Fig. 12 - Component Diagram for Fingerprint Biometric system

Each component, modeled with its security element, implements the function allocated in the previous phase. The physical elements of the biometric system were modeled using component diagram with the elements of the feature extraction and matching algorithm, as shown in Fig. 12. Then, the architecture of the biometrics system was modeled as the deployment diagram which is shown in Fig. 13.

The enhancement of security features in the fingerprint biometric system, incorporated early in the system life cycle, was demonstrated based on the three stages of a common design process: Requirements analysis, Functional Analysis, and Design Synthesis. It was established how effective it is to design security for embedded systems along with other functional and performance requirements throughout the system life cycle. System development usually undergoes certain iterative processes, and perhaps, this case study might only represent the first iteration of the system life cycle

process. Through the successful research in this paper, the idea of incorporating security in the design process has been presented. The identification of possible attacks and the appropriate countermeasures taken early in the requirements analysis also potentially guides the progress not only by enhancing the security of the system but also by facilitating the tasks of the designers and engineers alike.

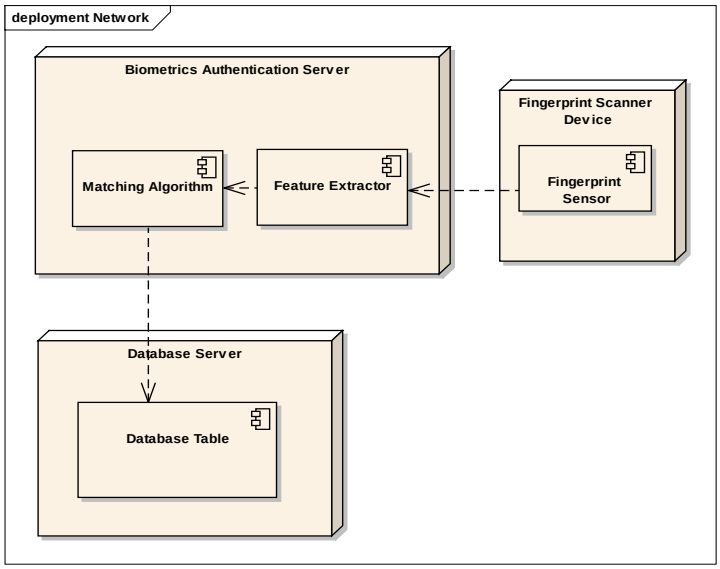

Fig. 13 - Deployment Diagram for fingerprint biometric system

By correlation based matching method, it is able to work with fingerprint of poor quality image. The functionality analysis of the host images guarantees a high degree of precision with fingerprint image authentication. When making the right option, the accuracy of a biometric device is strongly affected by falsified and falsifiable mistakes. The obstacle to scaling poses a concern about the effect of the number of registered users making the right decision. It is of utmost importance to protect the biometric device from attacks and user privacy.

Biometric security such as fingerprint authentication has proved to be both safer and more convenient than passwords, making fingerprint sensing feature in smartphones, tablets and PCs. Nevertheless, authentication of the fingerprint also poses security issues, which can best be solved with biometric protections. For the security purpose, there are three main steps can be considered [20].

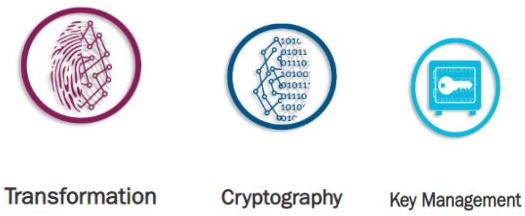

Fig. 14 - Three main steps of protection-built for biometrics [20]

i. Transformation

This single-way conversion of biometric data into a proprietary prototype format avoids recreation, reverse-engineering or accidental use, shielding the user against identity theft.

ii. Cryptography

Each biometric data is encrypted and digitally signed using 256-bit Advanced Encryption Standard and Transport Layer Protection to avoid eavesdropping, abuse or fraud.

iii. Key Management

Hardware-generated, one-time encryption keys make sure biometric data remains completely inside the secure execution environment of the host, where it is only accessible to so-called trusted processes.

5. Conclusion

Today the challenges of cyber security have been monumental. Due to the inevitable technological advancements, security sophistication also became more prevalent. Especially in the embedded system domain, security breaches cannot

be tolerated. The nature in which embedded systems usually operate covers certain sensitive data or information. Therefore, designing security in embedded systems early in development process or during system life cycle is very crucial. Thus, a thorough review of the biometric fingerprint system is carried out and looked at the different security features of the program. Moreover, Threat models with direct and indirect attacks on biometric system have been used to demonstrate the security vulnerabilities in a biometric framework. Then, we have pointed out the incorporation of security features in fingerprint biometric system by analyzing the requirements of the system and provided the main steps for protection for the biometric system. To be concluded, we have analyzed and transformed the threats and counter-measures identified during the requirements analysis using the abuse case into more specific safety requirements or functions. Therefore, we have shown that the incorporation of security features into the biometric fingerprint system by analyzing the requirements of the system and providing the main steps for the protection of the biometric system in this paper.

Acknowledgement

The authors fully acknowledged Ministry of Higher Education (MOHE) and Universiti Teknologi Malaysia (UTM) for the approved fund (16J46) which make this research possible.

Appendix A:

The description of the attacks against each point are summarized in Table 2.

Table 2 - Summary of the possible threats against fingerprint biometrics

No. of Threat	Description of Threat
Threat 1	Threat to biometric input devices
Threat 2	Threat to the process of transmitting biometric raw data to the signal-processing component
Threat 3	Threat to the extractor module features
Threat 4	Threat to the channel between the extractor and the play
Threat 5	Threat to the matcher module
Threat 6	Threat to the transition of biometric models from the registration portion to the storage component
Threat 7	Threat to biometric storage component
Threat 8	Threat to the connection between the matching module and the verification program

The next task is to identify the countermeasures for the threat that has been identified in Table 2. The corresponding countermeasures for such attacks are based on a survey done by [21] which are summarized in Table 3.

Table 3 - The attack and the identified countermeasure

Threat	Attack	Counter Measures
Threat 1	The most frequent attacks occur when the picture is recorded with fake fingerprint.	Fingerprint liveness detection [21-23]
Threat 2	The channel can be intercepted while the image is transmitted to the extractor device and therefore the fingerprint image can be stolen.	- Use encoding technique to validate data - Challenge-response authentication [24]
Threat 3	The extractor feature can be replaced by a Trojan horse, which can bypass the extractor feature and generate the artificial template for match.	Introduce data that overflows the buffer based on certain assumption criteria [24]
Threat 4	The transmission channel between the extractor and the matching function can also be intercepted and the fingerprint function can be saved later.	- Use encryption like watermarking - Enforce sequencing / timestamp
Threat 5	The same problem will occur in the matching module with the function extractor. The existence of Trojan horse can always produce the desired result regardless of the fingerprint input.	- Encrypt match score in the matching component - Limit the number of attempt
Threat 6	The database may also be attacked by the Trojan horse through which the matching module can be artificially recorded.	Encrypt template using parameters such as password
Threat 7	Through intercepting the communication channel between the database server and matching	- Apply sequencing / timestamp - Encryption such as watermarking

	equipment, the record of the legitimated user is stolen.	
Threat 8	Also susceptible to potential attacks is the channel between the corresponding module and the requesting verification.	Encrypt the decision before transmitting

References

[1] Willins, B., Sharony, J. and Wang, H., Symbol Technologies LLC. (2006). Cryptographic architecture for secure, private biometric identification. U.S. Patent 6,990,587

[2] Umer, S., Dhara, B.C. and Chanda, B. (2017). A novel cancelable iris recognition system based on feature learning techniques. Information Sciences, 406, pp.102-118

[3] Maltoni, D., Maio, D., Jain, A.K. and Prabhakar, S. (2003). Fingerprint Matching. Handbook of Fingerprint Recognition, pp.131-171

[4] Castiglione, A., Choo, K.K.R., Nappi, M. and Narducci, F. (2017). Biometrics in the cloud: challenges and research opportunities. IEEE Cloud Computing, 4(4), pp.12-17

[5] B. Schneier, "Stealing Fingerprints," Schneier on Security, (2015). Available: https://www.schneier.com/blog/archives/2015/10/stealing_finger.html.

[6] Nandakumar, K. and Jain, A.K. (2015). Biometric template protection: Bridging the performance gap between theory and practice. IEEE Signal Processing Magazine, 32(5), pp.88-100

[7] Jin, Z., Teoh, A.B.J., Goi, B.M. and Tay, Y.H. (2016). Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. Pattern Recognition, 56, pp.50-62

[8] Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), p.141

[9] Schaumont, P., Hwang, D., Yang, S. and Verbauwhede, I. (2006). Multilevel design validation in a secure embedded system. IEEE Transactions on Computers, 55(11), pp.1380-1390

[10] Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), p.141

[11] Kocher, P., Lee, R., McGraw, G. and Raghunathan, A. (2004), June. Security as a new dimension in embedded system design. In Proceedings of the 41st annual Design Automation Conference (pp. 753-760)

[12] Alaswad, A.O., Montaser, A.H. and Mohamad, F.E. (2014). Vulnerabilities of biometric authentication threats and countermeasures. International Journal of Information & Computation Technology, 4(10), pp.947-58

[13] Jain, R. and Kant, C. (2015). Attacks on biometric systems: an overview. International Journal of Advances in Scientific Research, 1(07), pp.283-288

[14] Latha, M.U. and Rameshkumar, K. (2013). A study on attacks and security against fingerprint template database. International Journal of Emerging Trends Technology in Computer Science (IJETTCS), 2, p.37

[15] Mwema, J., Kimwele, M. and Kimani, S., (2015). A simple review of biometric template protection schemes used in preventing adversary attacks on biometric fingerprint templates. International Journal of Computer Trends and Technology, 20(1), pp.12-8

[16] Akhtar, Z. (2012). Security of multimodal biometric systems against spoof attacks. Department of Electrical and Electronic Engineering, University of Cagliari, Cagliari, Italy, 6

[17] Ramesh, M.R. and Reddy, C.S. (2016). A survey on security requirement elicitation methods: classification, merits and demerits. Int. J. Appl. Eng. Res, 11(1), pp.64-70

[18] M. Damodaran. (2006). Secure Software Development using Use Case and Misuse Case, Issues Inf. Syst., vol. 7, no. 1, pp. 150–154

[19] I Park, J.H. and Park, J.H. (2017). Block chain security in cloud computing: Use cases, challenges, and solutions. Symmetry, 9, 164

[20] Ibrahim, M.B., Designing A Fingerprint Biometric Authentication System for Students Electronic Examination.

[21] Protecting Your Biometric Identity, Available: https://www.synaptics.com/technology/security-suite, 6th Feb, 2020

[22] Yang, W., Wang, S., Hu, J., Zheng, G. and Valli, C. (2019). Security and accuracy of fingerprint-based biometrics: A review. Symmetry, 11(2), p.141

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

[24] A. K. Jain, K. Nandakumar, and A. Nagar. (2008). Biometric template security. EURASIP J. Adv. Signal Process, 2008, 113:1–113:17