A HYBRID BIOMETRIC TEMPLATE PROTECTION ALGORITHM IN FINGERPRINT BIOMETRIC SYSTEM

SHAJAL ERACHAMPAT

A project report submitted in partial fulfillment of the
requirements for the award of the degree of
Master of Computer Science (Information Security)

Faculty of Computing
Universiti Teknologi Malaysia

JUNE 2017

This project report is dedicated to my family, lecturers especially my supervisor and friends for their endless support and encouragement.

ACKNOWLEDGEMENT

First of all praise to Allah the Almighty God. I am grateful to express my sincere appreciation to my family, who always strengthen me and supported me emotionally and financially while I was away for my studies.

My sincere thanks to my project supervisor, Dr. Anazida Binti Zainal for motivation and encouragement. I would like to thank the staff of University Teknologi Malaysia and especially the Faculty of Computing, for their kind cooperation.

ABSTRACT

Biometric recognition has achieved a considerable popularity in recent years due its various properties and widespread application in various sectors. These include very top priority sectors like countries boundary security, military, space missions, banks etc. Due to these reasons the stealing of biometric information is a critical issue. To protect this user biometric template information there should be efficient biometric template transformation technique and thereby the privacy of user is preserved. Non-invertible transformation can keep the user template based transformed information maximum secure against the regeneration. But the performance of non-invertible template protection mechanism will be reduced by the increase in security. This limitation of non-invertible biometric transformation should be solved. This research aims to develop a hybrid biometric template protection algorithm to keep up a balance between security and performance in fingerprint biometric system. The hybrid biometric template protection algorithm is developed from the combination of non-invertible biometric transformation and biometric key generation techniques. To meet the research objective this proposed framework composed of three phases: First phase focus on the extraction of fingerprint minutiae and formation of vector table, while second phase focus on develop a hybrid biometric template protection algorithm and finally the third phase focus on evaluation of performance of the proposed algorithm.

ABSTRAK

Kebelakangan ini, *biometric recognition* telah mencapai popularity yang tinggi disebabkan kepelbagaian ciri dan aplikasi meluas dalam pelbagai sektor. Ini termasuk sektor keutamaan paling atas seperti negara-negara sempadan keselamatan, ketenteraan, misi angkasa, bank dan lain-lain. Oleh kerana sebab-sebab ini mencuri maklumat biometrik adalah isu yang kritikal. Untuk melindungi maklumat pengguna template biometrik ini perlu ada teknik transformasi biometrik template yang cekap dan dengan itu privasi pengguna akan terpelihara. Transformasi *non-invertible* boleh menyimpan template pengguna berasaskan perubahan maklumat yang maksimum yang selamat daripada dijana semula. Tetapi tahap ketepatan pengesahan dicapai oleh teknik transformasi *non-invertible* akan berkurang dengan peningkatan keselamatan. Batasan transformasi biometrik *non-invertible* perlu diselesaikan. Kajian ini bertujuan untuk membangunkan algoritma perlindungan template hibrid biometrik untuk mengikuti keseimbangan antara keselamatan dan prestasi dalam sistem cap jari. Biometrik. algoritma perlindungan template hibrid biometrik dibangunkan daripada gabungan transformasi biometrik *non-invertible* dan penjanaan kunci biometrik. Untuk mencapai objektif kajian, rangka kerja yang dicadangkan ini terdiri daripada tiga fasa: fasa pertama fokus kepada pengekstrakan perincian maklumat cap jari dan pembentukan jadual vektor, manakala fasa kedua fokus kepada membangunkan algoritma perlindungan template hibrid biometric dan akhir sekali fasa ketiga fokus kepada pengesahan dan penilaian prestasi algoritma yang dicadangkan.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF EQUATIONS

LIST OF ABBREVIATIONS

CN	-	Crossing Number
EER	-	Equal Error Rate
FAR	-	False Acceptance Rate
FRR	-	False Rejection Rate

CHAPTER 1

INTRODUCTION

1.1 Introduction

The future of identity depends fully on biometrics, and then the stealing of biometric information and thereby compromising the biometric system will be challenging issues. Biometric system process two main functions, they are Enrollment and Authentication. Enrollment is the process of capture the user biometric information and extraction of the features from it and this extracted feature called as template is stored in the database. Meanwhile Authentication is the process of user biometric information captured and extracted features or templates are compared with the ones already exists in the database. Due to the increase in biometric systems there is a huge dependency on biometric data; however this biometric data could have serious lifelong implications. The main reason for this is the biometric characteristics are unique for each individual and also with are not changeable though out the person lifetime. Whenever a biometric data is compromised form the database it can give an opportunity for attackers to misuse it various kind or even they can make artificial finger from that biometric raw data. Therefore the protection of biometric database is very important factor.

1.2 Background of the Problem

Millions of victims are infected by identity theft; it is possible to regenerate a new credit card or social security number. If bank social media accounts get hacked, it is possible to reset also. But when the biometric information is stolen, is there any solution to regenerate or reset? No they cannot because they are permanent identification markers. Once the biometric information is snagged by an attacker, they can control it forever (Goodman and Marc, 2015). Many of the attackers and thieves are already working diligently to circumventing these biometric systems. *"To reveal this issues (Matsumoto et al., 2002) conducted a study on recreating a mold using gelatin for the fingerprint image impression taken from the wineglass and they concluded that; there can be various dishonest acts using artificial fingers against the fingerprint systems. Manufacturers, vendors, and users of biometric system should carefully examine security of their system against artificial clones. How to treat such information should be an important issue."*

Due to the growth in biometric technologies there is demanding need for security mechanism in this area. Maltoni *et al.* (2009) analyzed various biometric technique and they concluded that fingerprint technology keep up the maximum balance between all the biometric properties. So, they have wide acceptance among the various biometric techniques like hand, iris, face, voice etc. Also due to the large application of fingerprint biometrics various sectors like banks, hospitals etc. there is increase in attacks against this stored fingerprint templates in the biometric database. So any compromise to the biometric information of the individuals stored in the database can cause critical damage to the individual forever. So there is a demanding need for biometric template security stored in the biometric database.

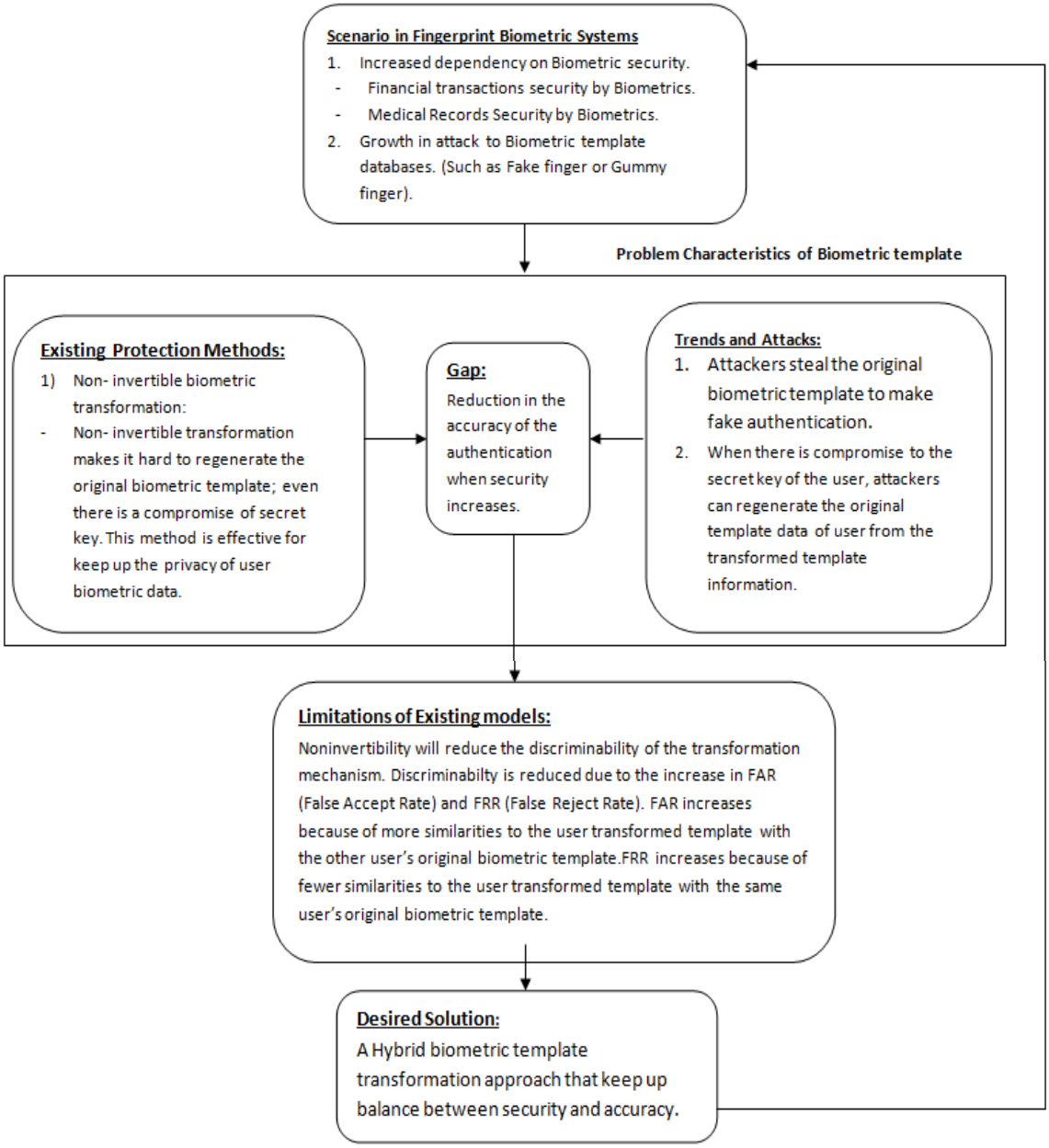

Figure 1.1: Problem characteristics of biometric template security

Identity of the individual is one of the important parameter in organization and government security systems, where any errors causing will be threaten the integrity of the overall security system. For example highly confidential and security areas like international border control, nuclear plant, airport, issuance of national passport and identity documents etc. where the integrity of the security system should be maximum. Current trend in the biometric security systems replaced most of the traditional ways of identity recognition and authentication. Biometric is

science of authenticating a user based on the physiological or behavioral features of an individual. These features include fingerprints, facial features, iris, voice, palm etc.

Biometric Recognition system basically have four modules: they are sensor module, feature extraction module, matching module and finally the decision module. Ratha *et al.* (2001) have pointed out several level of attacks that may be used against a biometric recognition system they are: 1) a artificial finger maybe introduced at the sensor, 2) there can be resubmission of illegally intercepted information to the biometric recognition system, 3) there can be replacement of feature information by a Trojan horse algorithms that creates pre-determined feature sets, 4) there can be replacement of original feature sets with synthetic feature sets, 5) there can be replacement of the matcher by Trojan horse algorithms that produces high scores thus ignoring system security, 6) there can be intentional modification to the template or deletion of information or addition of illegal template in the stored database, 7) there can be modification to the information in the communication channel between various modules of the biometric system (Jain *et al.*, 2005) and 8) the final outcome from the biometric system can be overruled.

There are various techniques proposed in the literature for the security of the biometric templates. Soutar (Bioscrypt) proposed use of coarsely quantized match score by the matcher to avoid the Hill- Climbing attack from successfully merging. Pankanti and Yeung (1999) come up with an invisible fragile watermarking technique to identify the tampering in the fingerprint image. Jain and Uludag (2003) proposed use of steganography to hide biometric fingerprint details in the face image and there by protect the biometric data when transmitted over non-secure communication channel. The main idea behind the use of watermarking and steganography is to prevent the sensitive template data from unauthorized modification and eavesdropping attacks. But there is an increased complexity and lack in overall security and privacy to the user biometric information which is stored in the database.

Biometric Cryptosystems and cancelable biometrics highlight so many advantages over the traditional generic biometric system. This technique helps to obscure the biometric template information, such that it is very difficult to obtain the original biometric template. In these techniques Pseudonymous Authentication is carried out (Authentication in the encrypted domain). Biometric Cryptosystems and cancelable biometrics have the property of Revocability of templates (many occurrence of secured biometric template can be generated). These two techniques increase the security against various traditional attacks, there by more social acceptance can achieved to the biometric applications.

Biometric Cryptosystems needs the storage of biometric dependent public data, which is used to retain or generate keys; these are called as helper data (Jain *et al.,* 2008). In Biometric Cryptosystems key release mechanism is done with the help of biometric template information also known as biometric dependent key-release. Boyen and Xavier (2004) described a vulnerability of secure sketches and fuzzy extractors while an attacker having multiple invocations of the given set of secrets that are used to reconstruct the original biometric template. Stoianov *et al.* (2009) point out a nearest imposter attacks in which specific parts of a large biometric template information is mixed to retain high matching scores. They also point out that successful encoding of chunks of biometric information is indeed need to bind sufficiently long keys may suffer from low entropy and are easily decoded. Keys used in fuzzy commitment schemes have suffer from low entropy, which reduces the difficulty for brute force attacks (Juels and Wattenberg, 1999).

Ignatenko and Willems (2010) conducted study to determine privacy and security weakness of fuzzy commitment scheme and results point out that fuzzy commitment schemes leak data in bound keys and non-uniform templates. Hong *et al.* (2008) pointed out vulnerabilities that can be caused when doing hardened fuzzy vaults. The fuzzy vault scheme does not hide the original biometric information but obscure it by helper data. More over in the key retrieval rates are given by the application, the attacker can still unlock vaults if the helper data does not obscure the original biometric template properly. Davida *et al.* (1998); Claus and Ralf (2004)

stated helper data based key generation schemes can be attacked via record multiplicity. If an imposter have access to several different types of helper data and its related secret keys of the same user, an association of these can help the attacker to reconstruct an possible biometric templates obtained at enrollment. Also key generation schemes likely to extract short keys which increase probability to be guessed in brute force attacks with in a sensible feature space. Key generation schemes likely to have less accuracy compared to key binding schemes, hence expected to be vulnerable to false acceptance attacks (Rathgeb and Uhl, 2011).

Cancelable biometrics is applied in order to make it very hard to recover the original biometric information. The individual characteristics of the biometric template should not be reduced (constraint on False Accept Rate), same time there should not be any tolerance to intra class variations (Constraint on False Rejection Rate) (Ratha *et al.,* 2001). Quan *et al.* (2008); Shin *et al.* (2009) point out attack against block re mapping and surface- folding techniques. Kong *et al.* (2006) states that most approaches to biometric salting becomes heavily vulnerable to attack if the biometric token is stolen. More over if the salting technique used is invertible; the template information can be regenerated and used in masquerade attacks. Lumini and Nanni (2007) point out that BioHashing techniques may exhibit low performance in case attackers are in control of secret tokens.

When considering the performance analysis of biometric systems commonly used factors are False Rejection Rate (FRR), False Acceptance Rate (FAR) and finally Equal Error Rate (EER). The FRR of Biometric cryptosystem is the rate of correct user rejected by the biometric system. The FAR of Biometric cryptosystem is the rate of wrong user accepts by the biometric system. In cancelable biometric transformation and alignment of transformed biometric information needed to be optimized in order to keep up the performance of the biometric recognition system. To achieve maximum privacy to user data the biometric template protection mechanism should be designed such a way that is very hard for the attacker to regenerate the original biometric information from the transformed template information. This can be achieved by non- invertible biometric transformation; here

the compromise of secret key will not help in generating the original biometric information of the user. Although non-invertible biometric transformation have this advantages, but there is imbalance between the non-invertibility and discriminability properties. These two properties should be keep up by a good non-invertible biometric transformation. The non-invertibility factor increases the security to the user biometric information. So many works proposed to keep up the security to user template information, but still the reduction in the discriminability factor or accuracy is an important research domain. Basically accuracy degradation is caused by increase in FAR and FRR rates, these rates should be limited to maximum to get better accuracy in authentication.

1.3 Statement of Problem

The user biometric information should be protected by good biometric transformation mechanism. The application of non-invertible biometric transformation can provide better security to biometric information, but the non-invertible transformation reduces the performance of the biometric identification system this is because of the increase in EER value. The main cause by which the EER value is increased is due to the usage of highly complex algorithms for transformation. On the other hand if too low complex algorithm usage can reduce security of the biometric information. Therefore there is a demanding need for non-invertible biometric template protection algorithm that can keep up both security and performance in balanced condition.

1.4 Aim

To develop a hybrid biometric template protection algorithm to balance security and performance in fingerprint biometric system.

1.5 Objectives

The objective of this research is to refine the security and balance it with the performance of non-invertible biometric protection technique in fingerprint biometric system by the application of hybrid biometric template protection algorithm. The objective are as stated below:

i. To extraction the fingerprint minutiae and formation of vector table.
ii. To develop a hybrid biometric template protection algorithm.
iii. To evaluation of performance of the proposed algorithm.

1.6 Scopes

For this research the following constraints are considered:

i. Fingerprint images taken from FVC2002 Database (http://bias.csr.unibo.it/fvc2002/).
ii. Algorithms generated by MATLAB coding.
iii. 256x 364 size TIFF images are used as Fingerprint image.
iv. False Accept Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER) are used to determine performance of algorithm.

1.7 Importance of the Research

This research importance is highlighted as follows.

i. The fingerprint uniqueness makes a demanding interest to adopt a strong security to the fingerprint image stored in the fingerprint biometric system database. As we know today most of the security authentication uses biometrics and fingerprint the most widely used biometric technique. So once a fingerprint is stolen from a database it can create a heavy damage to that fingerprint owner in current world. So there should be some good security mechanism for keep the fingerprint image not available to the attacker. This can be solved by template transformation technique or cancelable biometrics.

ii. Biometric information are permanently linked with users, such that it can be misused to perform an illegitimate tracking of the activities of the users enrolled to different databases.

iii. Disclosure of biometric template information of the users can be misused by the illegitimate users to produce artificial samples or gummy fingers for spoofing attack.

iv. This research work presumes to strengthen the security for the fingerprint biometric authentication system and keep up the accuracy to a satisfactory level.

1.8 Research Methodology

The research methodology consists of three phases they are shown in Figure 1.2. Detailed methodology for the work is explained in Chapter 3.

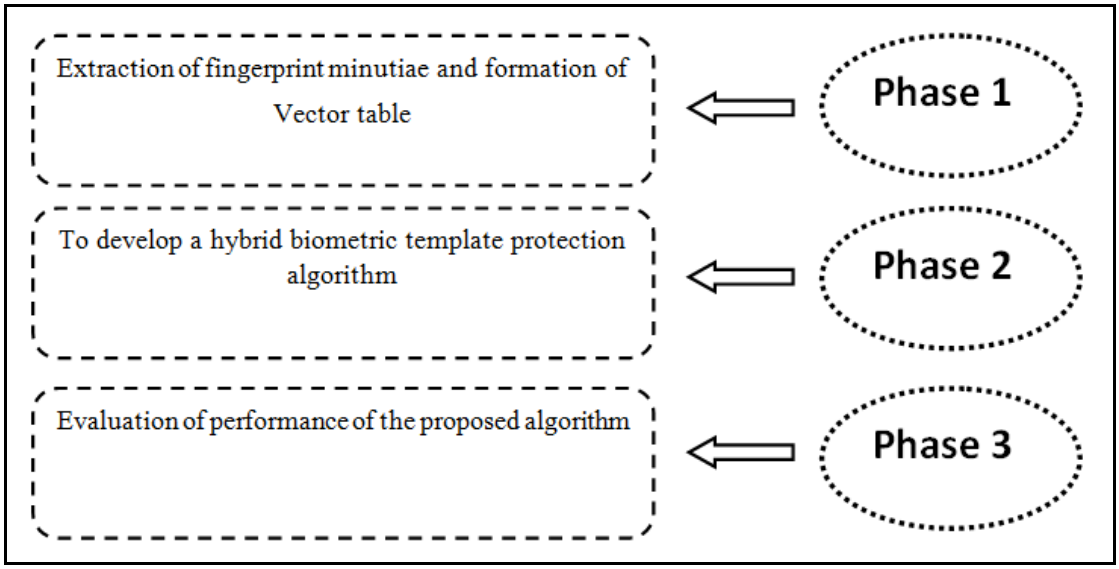

Figure 1.2: Research methodology

1.9 Organization of the Research

This research is made up of five chapters. Chapter 1 gives introduction to this research. Chapter 2 provides literature review about different biometric template security mechanisms used for protecting of user privacy. Chapter 3 provides the research methodology of this study. In Chapter 4 the extraction of fingerprint is done and finally a vector is created. In Chapter 5 the hybrid biometric template protection algorithm is designed and evaluation is done to achieve the final results. Finally Chapter 6 is the conclusion for this research work.

REFERENCES

Adams K. An Analysis Of Biohashing And Its Variants. *Pattern Recognition*. 2006. 36: 1359 - 1368.

Alessandra L. An Improved Biohashing For Human Authentication. *Pattern Recognition*. 2007. 40(3): 1057-1065.

Andrew T. Biophasor: Token Supplemented Cancellable Biometrics. *9th International Conference on Control, Automation, Robotics and Vision*. December 5-8, 2006. Singapore: IEEE. 2006. 1-5.

Anil K., Jain A. R. Biometric Template Security: Challenges and Solutions. *13th European Signal Processing Conference*. September 4-8, 2005. Antalya, Turkey: IEEE. 2005. 1-4.

Argyropoulos S. Gait Authentication Using Distributed Source Coding. *15th IEEE International Conference on Image Processing.* October 12-15, 2008. San Diego, CA, USA: IEEE. 2008. 3108-3111.

Boult T. Robust Distance Measures for Face-Recognition Supporting Revocable Biometric Tokens. *7th International Conference on Automatic Face and Gesture Recognition (FGR06).* April 10-12, 2006. Southampton, UK: IEEE. 2006. 560-566.

Boyen X. Reusable Cryptographic Fuzzy Extractors. *Proceedings of the 11th ACM conference on Computer and communications security*. October 25 - 29, 2004. Washington DC, USA: ACM. 2004. 82-91.

Buhan I. Fuzzy Extractors For Continuous Distributions. *Proceedings of the 2nd ACM symposium on Information, computer and communications security.* March 20-22, 2007. Singapore: ACM. 2007. 353-355.

Cavoukian A., Stoianov A. Biometric Encryption. In: *Encyclopedia of Biometrics*. US: Springer. 260-269; 2009.

Claus V. Handwriting: Feature Correlation Analysis for Biometric Hashes. *EURASIP Journal on Applied Signal Processing.* 2004. 2004(4): 542–558.

Daugman F. Combining Crypto with Biometrics Effectively. *IEEE Transactions on Computers*. 2006. 55(9): 1081-1088.

Davida G. On Enabling Secure Applications Through Off-Line Biometric Identification. *IEEE Symposium on Security and Privacy*. May 6-6, 1998. Oakland, CA, USA: IEEE. 1998. 148-157.

Davide M. *Handbook of Fingerprint Recognition*. Berlin, Germany: Springer. 2003.

Davide M. *Handbook of Fingerprint Recognition*. London: Springer. 2009.

Doktor M. (2007). Biometric Systems and Security Design Principles. http://wiki.cas.mcmaster.ca/index.php/Biometric_Systems_and_Security_Design_Principles. Available online 25 February, 2016.

Feng Q. Cracking Cancelable Fingerprint Template of Ratha. *International Symposium on Computer Science and Computational Technology*. December 20-22, 2008. Shanghai, China: IEEE. 2008. 572-575.

Goodman M. Future Crimes: Everything Is Connected, Everyone Is Vulnerable And What We Can Do About It. New York: Knopf Doubleday Publishing Group. 2015

Hämmerle-Uhl J. Cancelable Iris Biometrics Using Block Re-mapping and Image Warping. *Lecture Notes in Computer Science Information Security.* 2009. 5735: 135-142.

Hong S. The Vulnerabilities Analysis Of Fuzzy Vault Using Password. *Second International Conference on Future Generation Communication and Networking.* December 13-15, 2008. Hainan Island, China: IEEE. 2008. 76-83.

Ignatenko T. Information Leakage In Fuzzy Commitment Schemes. *IEEE Transactions on Information Forensics and Security*. 2010. 5(2): 337 – 348.

Jain A. K. Biometric Template Security. *EURASIP Journal on Advances in Signal Processing.* 2008. 2008(113): 1-20.

Jain A. K. Hiding Biometric Data. *IEEE Transactions on Pattern Analysis and Machine Intelligence.* 2003. 25(11): 1494-1498.

Juels A. A Fuzzy Commitment Scheme. *6th ACM conference on Computer and communications security*. November 01-04, 1999. Singapore: ACM. 1999. 28–36.

Juels A. A Fuzzy Vault Scheme. *Proceedings IEEE International Symposium on Information Theory*. June 30- July 5, 2002. Lausanne, Switzerland: IEEE. 2002. 408

Linnartz J. P. New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates. *Audio- and Video-Based Biometric Person Authentication*. 2003. 2688: 393-402.

Maiorana E. Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans.* 2010. 40(3): 525 – 538.

Manvjeet K. Fingerprint Verification System using Minutiae Extraction Technique. *International Journal of Computer, Electrical, Automation, Control and Information Engineering*. 2008. 2(10): 3405- 3410.

Matsumoto T. Impact Of Artificial "Gummy" Fingers On Fingerprint Systems. *Optical Security and Counterfeit Deterrence Techniques IV*. 2002.4677:1-15.

Ouda N. Tokenless Cancelable Biometrics Scheme for Protecting Iris Codes. *20th International Conference on Pattern Recognition.* August 23-26, 2010. Istanbul, Turkey: IEEE. 2010. 882-885.

Pabitha M. Efficient Approach for Retinal Biometric Template Security and Person Authentication using Noninvertible Constructions. *International Journal of Computer Applications*. 2013. 69(4): 28-34.

Pankanti S. Verification Watermarks On Fingerprint Recognition And Retrieval. *Security and Watermarking of Multimedia Contents.* 1999. 3657: 1-23.

Rabia J. A Survey of Face Recognition Techniques. *Journal of Information Processing Systems*. 2009.5(2):41-68

Ratha N. An Analysis of Minutiae Matching Strength. *Lecture Notes in Computer Science Audio- and Video-Based Biometric Person Authentication.* 2001. 2091: 223-228.

Ratha N. Enhancing Security And Privacy In Biometrics-Based Authentication Systems. *IBM Systems Journal*. 2001. 40(3): 614 – 634.

Ratha N. Generating Cancelable Fingerprint Templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2007. 29(4): 561-572.

Rathgeb C. A Survey On Biometric Cryptosystems And Cancelable Biometrics. *EURASIP Journal on Information Security*. 2011. 2011(3): 1-25.

Rocketcenter (2016). 101 Inventions. http://rocketcenter.com/forms/edu/101Inventions/101Enigma.pdf. Available online 15 May, 2016.

Saini R. Comparison of Various Biometric Methods. *International Journal of Advances in Science and Technology (IJAST).* 2014. 2(1): 24-30.

Savvides M. Cancelable Biometric Filters For Face Recognition. *17th International Conference on Pattern Recognition.* August 23-26, 2004. Cambridge, UK: IEEE. 2004. 922-925.

Shi J., and You Z. Privacy Trustworthy Biometrics Using Noninvertible And Discriminable Constructions. *19th International Conference on Pattern Recognition.* December 8-11, 2008. Tampa, FL, USA: IEEE. 2008. 1-4.

Shin S. Dictionary Attack on Functional Transform-Based Cancelable Fingerprint Templates. *ETRI J ETRI Journal.* 2009. 31(5): 628-630.

Soutar C. Bioscrypt. Retrieved from ttp://www.bioscrypt.com

Stoianov T. K. Security issues of Biometric Encryption. *IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH).* September 6-27, 2009. Toronto: IEEE. 2009. 34-39.

Tang F. Preprocessing And Postprocessing For Skeleton-Based Fingerprint Minutiae Extraction. *Pattern Recognition*. 2007. 40(4): 1270-1281.

Teoh A. Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs. *IEEE Transactions on Pattern Analysis And Machine Intelligence.* 2006. 28(12): 1892-1901.

Wang Y. Biometrics Symposium. Face Based Biometric Authentication with Changeable and Privacy Preservable Templates. *Biometrics Symposium.* September 11-13, 2007. Baltimore, MD, USA: IEEE. 2007. 1-6.

Wikipedia. (2016). Vigenère Cipher. https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher. Available online 13 August, 2016.

Woods R. *Digital Image Processing*. 3rd ed. New Jersey: Prentice Hall. 2002

Yagiz S. A Secure Biometric Authentication Scheme Based On Robust Hashing. *Proceedings of the 7th workshop on Multimedia and security.* August 01-02, 2005. New York, USA: ACM. 2005. 111-116.

Yang W. Cancelable Fingerprint Templates with Delaunay Triangle-Based Local Structures. *Cyberspace Safety and Security Lecture Notes in Computer Science*. 2013. 8300: 81-91.

Yevgeniy D. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM Journal on Computing*. 2008. 38(1): 97-139.

Zuo J. Cancelable Iris Biometric. *19th International Conference on Pattern Recognition.* December 8-11, 2008. Tampa, FL, USA: IEEE. 2008. 1-4.