ISBN : 978-979-3793-73-3

ICOSET INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING and TECHNOLOGY "Sustainable Development in Developing Country"

UIR INTERNATIONAL CONFERENCE 2017

ICOSET

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY

"Sustainable Development in Developing Country"

PEKANBARU, 8-10 NOVEMBER 2017

PROCEEDING

YAYASAN LEMBAGA PENDIDIKAN ISLAM (YLPI) RIAU
UNIVERSITAS ISLAM RIAU

LPPM - UIR
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT UNIVERSITAS ISLAM RIAU
Jl. Kaharuddin Nasution No. 113, Marpoyan, Pekanbaru
Riau - Indonesia 28284

2017

PROCEEDING

International Conference on Science Engineering and Technology (ICoSET)
08 - 10 November 2017
Pekanbaru, Indonesia

"Sustainable Development in Developing Country

Editor :

Evizal Abdul Kadir

Ku Ruhana Ku Mahamud

Tole Sutikno

Organizer :

Co-Organizers :

PUBLISHER BY UNIVERSITAS ISLAM RIAU (UIR) PRESS
2017

UIR Press

Art Design, Publishing & Printing

LPPM, Rectorat Building 3rd Floor, Jl. Kaharuddin Nasution No.113, Marpoyan 28284 Pekanbaru, Indonesia.

Telp : 0761-674674, Fax : 0761-674834

uirpress.uir.ac.id

ISBN : 978-979-3793-73-3

Perpustakaan Nasional: Katalog Dalam Terbitan (KDT)

International Conference on Science Engineering and Technology (ICoSET)
08 - 10 November 2017, Pekanbaru, Indonesia.
Evizal Abdul Kadir, et al – Pekanbaru : UIR Press 2017

Xii, 261 p. ; ilus.; 29 cm

Bibliografi

ISBN : 978-979-3793-73-3

ISBN: 978-979-3793-73-3

ORGANIZING COMMITTEE

Conference Chair:
Dr. Evizal Abdul Kadir, ST., M.Eng

Conference Co-Chair Science:
Dr. Dedikarni, ST., M.Sc

Conference Co-Chair Social:
Dr. Sri Yuliani, M.Pd

Technical Program Chair:
Prof. Dr. Ku Ruhana Ku Mahamud
Assoc. Prof. Dr. Tole Sutikno

Technical Program Committees:

Prof. Dr. Detri Karya, SE., MA
(Islamic University of Riau, Indonesia)

Prof. Dr. Hasan Basri Jumin, M.Sc
(Islamic University of Riau, Indonesia)

Prof. Dr. Tengku Dahril, M.Sc
(Islamic University of Riau, Indonesia)

Prof. Dr. Syafrinaldi, SH., M.CL
(Islamic University of Riau, Indonesia)

Prof. Dr. Sugeng Wiyono, MMT
(Islamic University of Riau, Indonesia)

Prof. Dr. Seno Himala Putra, M.Pd (Islamic University of Riau, Indonesia)

Prof. Zainal A. Hasibuan, MLS., Ph.D
(University of Indonesia, Indonesia)

Prof. Josaphat Tetuko Sri Sumantyo, Ph.D
(Chiba University, Japan)

Prof. Dr. Usama Fauzi Juniansyah
(University of Tokyo, Japan)

Prof. Dr. Eko Supriyanto
(Universiti Teknologi Malaysia)

Prof. Dr. Zailuddin Arifin
(Universiti Teknologi MARA, Malaysia)

Prof. Jhon Lee, B.Sc, M.Sc., Ph.D
(Kyungdong University Korea)

Prof. Ahmed A. Al Absi
(Kyungdong University Korea)

Prof. Wisup Bae, Ph.D
(Sejong University, Korea)

Prof. Kazuhiko Nagatomo
(Dayeh University)

Assoc. Prof. Dr. Azhan Hashim Ismail
(Universiti Teknologi MARA, Malaysia)

Assoc. Prof. Dr. Shahrul Kamal Abdul Rahim
(Universiti Teknologi Malaysia)

Dr. Inkyo Cheong
(Inha University, Korea)

Ahn, Young Mee, Ph.D
(Inha University, Korea)

Dr. Montira Leelakriangsak
(Prince of Songkla University, Thailand)

Hitoshi Irie, Ph.D
(Chiba University, Japan)

Kuen-Song Lin, Ph.D
(Yuan Ze University, Taiwan)

Julie Yu-Chih Liu, Ph.D
(Yuan Ze University, Taiwan)

Liang Chih Yu, Ph. D
(Yuan Ze University, Taiwan)

ISBN: 978-979-3793-73-3

ISBN: 978-979-3793-73-3

TABLE OF CONTENTS

AN OVERVIEW OF FINGERPRINT TEMPLATE PROTECTION APPROACHES

Apri Siswanto,[1,] Ku Ruhana Ku-Mahamud, [1] and Evizal Abdul Kadir[2]
[1]*School of Computing, University Utara Malaysia, Malaysia*
[2]*Teknik Informatika, FakultasTeknik, Universitas Islam Riau, Indonesia*
Email: norliza@uum.edu.my, ruhana@uum.edu.my
aprisiswanto@eng.uir.ac.id, evizal@eng.uir.ac.id

Abstract

One possible attack in the biometric system is the template stored in the database. This attack can cause Biometric template information leakage, thus pose a serious privacy security threat. Most available template protection techniques fail to meet all the desired requirements of practical biometric systems such as diversity, revocability, security, and performance matching accuracy. This paper aims to review the various fingerprint template protection (ftp) approaches that have been proposed by researchers in recent decades. Some of the proposed schemes are standard encryption, biometric cryptosystem, template transformation, hybrid scheme and homomorphic encryption.

Keywords:*biometric system; fingerprint template protection; security, diversity, revocability*

1. INTRODUCTION

Biometric templates offer a reliable approach to user authentication issues in identity recognition systems.A wide range of biometric technologies are developed effectively that include fingerprint, iris, face, iris, palms, signature and hand geometry.Fingerprints are the most popular as they are easily captured, as well as low cost sensors and algorithms.The main purpose of using fingerprint biometric systems is to provide good authentication and can not be rejected.Authentication implies that only authorized users be able at access logical or physical resources protected by finger print systems and impostors are prohibited from accessing protected resources.From the user's perspective, there are two key requirements that fingerprint biometric system must be fulfilled. First, legitimate users should have timely and reliable access to protected resources / services. Second, biometric systems and personal data stored on it should be used only for the intended functionality, which is It is controlling access to certain resources and not for other unintentional purposes [1].

However, adversary attacks can make the biometric system not functioning properly according to the above requirements. To overcome and protect the biometric template information both in the process of registration/enrollment and authentication in the stored database, some techniques have been proposed by the researchers include standard encryption,

ISBN: 978-979-3793-73-3

biometric cryptosystem, template transformation, hybrid method and homomorphic encryption. This paper aims to summarize and present information on various fingerprint template protection techniques. The technique used is systematic literature review. The paper is organized in the following way. Section 2 of the paper discusses the attack on fingerprint template. Then, Section 3 presents desirable properties of fingerprint template protection. After that, Section 4 discusses fingerprint template protection approaches and Finally, Section 5 concludes the paper.

2. ATTACK ON FINGERPRINT TEMPLATE

The security ensured by the fingerprint biometric systems can itself be compromised. The general analysis of a fingerprint biometric system for vulnerability assessment determines the extent to which an imposter can compromise the security offered by the fingerprint biometric system. Many of the attacks are applicable to any information in fingerprint biometric system , the attacks can be using fake fingerprint biometrics and template modification are unique to biometric systems. According to Ratha, et al. [2] Biometric recognition system has some vulnerable point attacks. Attacks that may occur in the fingerprint verification system is as follows :

1. Attack at the sensor, A fake biometric sample can be presented in a sensor to gain access such as a fingerprint trace of an object touched by that person.
2. Replay Attack, There is a possibility of the adversary to interpret or obtain a digital copy of a stored biometric sample and replay this signal that passes through the biometric sensor.
3. Trojan horse attacks,The feature extractor can be replaced with a program that generates a set of desired features.
4. Spoofing the features, the features vector generated from biometric samples are replaced by a set of synthetic (fake) features created.
5. Attack on matcher, the matcher can also be subjected to Trojan horse attacks that always result in high or low match scores regardless of where the user presents the biometric on the sensor.
6. Attack on templates, the templates generated during the user enrollment can be stored locally or in network location that modify the saved template or replace it with a new template.
7. Attacks on communication channels, Data transferred through a communication channel can be intercepted for malicious reasons and modified and reinserted into the system.
8. Attack on the decision module, The final decision generated by the biometric system can be replaced by the Trojan horse program.

Biometric matching is usually only part of a larger information and information security management system. Thus the non-biometric module in the whole system can also introduce some security flaws. There are several techniques to disrupt attacks at various points. For example, sensing a finger conductivity or pulse can stop a simple attack on the sensor. Encrypted communication channel [3] can eliminate at least remote attack on synthesized feature factor and override final decision. The simplest way to stop attacks at override matcher, attacking the channel and modify template in database is to have the matcher and database reside in a secure location. Storing templates in a smartcard that a user brings with them to the point of service can also eliminate some attacks of type stored template [4].

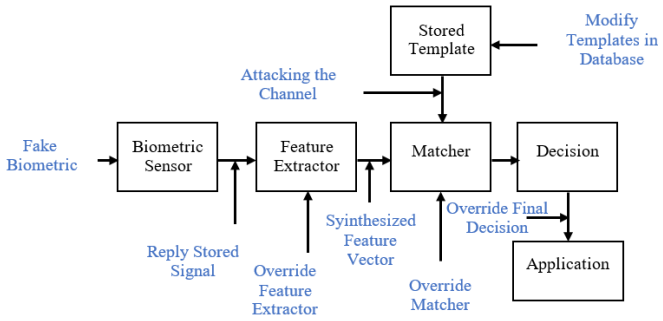

Fig. 1 Possible attack in fingerprint template protection

3. DESIRABLE PROPERTIES OF FINGERPRINT TEMPLATE PROTECTION (FTP)

The performance of biometric template protection systems can be evaluated by three categories namely,protection,operational and technical. Performance protectionincludesthe irreversibilitygandgdiversitygofgbiometric ginformation. Operational performance can be evaluated with the independence of modality, interoperability, and Quality of Performance. Technical performance can be evaluated with accuracy, throughput, storage requirements [5].There are four major requirement when a biometric template protection algorithm is design:[6]

A. Revocability: When the biometric template is compromised, it should be possible to revoke the compromised template and reissue a new template based on the biometric trait.
B. Diversity: The cross-matching of a secured templates should be ensured in such a manner that the privacy of the true owner of the template should be ensured.
C. Security - It should be extremely difficult to generate the original biometric feature set from the protected biometric templates.
D. Performance: The biometric template protection techniques developed should not decrease the accuracy of the recognition system.

4. FINGERPRINT TEMPLATE PROTECTION (FTP) APPROACHES

The major fingerprint template protection schemes can be categorized into standard encryption, biometrics cryptosystem, template transformation, hybrid methods, and homomorphic encryption such as shown in Figure 2. Each of schemes will discussed detail in the following sections.

A. Standard Encryption

The easiest way to secure fingerprint templates is by encrypting them using standard cryptographic techniques like RSA, DES and AES. This is the methodology used in most commercial biometric systems. However, it must be emphasized that some acquisitions with the same biometric properties do not produce the same feature set. Typically, the standard encryption function is not smooth function and a small difference in the feature set values extracted from raw biometric data will result in a huge difference in the resulting encrypted features. Consequently, one can not perform biometric matching directly in an encrypted domain. Instead, the template should be decrypted to match the query feature. As a result, the original biometric feature is exposed during each authentication attempt, irrespective of

ISBN: 978-979-3793-73-3

whether the authentication is eventually successful. Therefore, the encryption solution is secure revocable only under ideal conditions (key is kept secret and matching is done at a trusted location). If practical issues such as key management or susceptibility to template theft during a matching attempt are taken into account, the standard encryption technique is not good enough for securing biometric templates [6, 7].

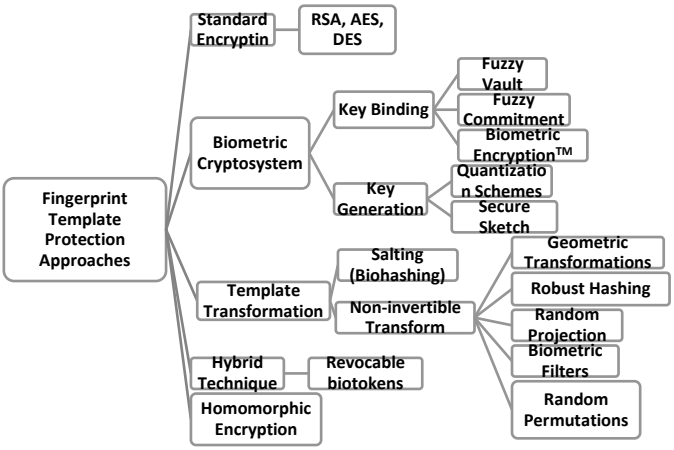

Fig. 2 A hierarchical taxonomy of FTP

B. *Biometric Cryptosystem*

In the biometric cryptosystems data information about the biometric template, called helper data , and stored in the database [8]. The data helper does not show important informationgabout the originalgbiometrictemplategbut is needed when matching the cryptographic key of the query biometric feature. Matching is done indirectly by verifying the truth of the extracted key. Errorgcorrectiongcoding techniques are usually used to handle intra-user variations. Biometric cryptosystemsgofferghigh security but, not designedgto provide diversitygand revocability. Cryptosystem biometrics are grouped into key bindinggand key generationg systems based on howgthe helper data derivedg[6].Some of the techniques in this category are fuzzy vault, biometric encryption and fuzzy commitments.

The first key binding fingerprint biometricgcryptosystem was developedgby[9], called BiometricEncryptionTM (mytec2). Thisgwasangcompleted versiongofgmytec1 [10]. Thisgbiometricgencryptiongwas not practical because of mismatch between accuracy and security. Then, the next key binding is fuzzy vault. Fuzzy vault is cryptography designed to work with biometric features that are represented as minutiae in fingerprints. The advantage of the fuzzy vault scheme is the ability to control the amount of security imparted to protected biometric templates by increasing the number of chaff points and consequently the difficulty of the polynomial reconstruction problem. Even though its popularity, analysis of the fuzzy vault scheme has indicated that this approach has several drawbacks. Chang, et al. [11] present observations to differentiate minutiae from chaffgpoints

attacking fuzzy vaults based on fingerprints. Since the chaff points are made one by one, it created later tend reveal smaller empty surroundingg areas which is verified experimentally, i.e., the security of a fuzzy vault highly relies on the methodologygof generating chaff points.

Scheirer and Boult [12] discussed the vulnerability of fuzzy vaults to three potential attacks, namely, surreptitious key-inversion (SKI) attacks , blended substitution attacks and attacks via record multiplicity (ARM). The authors suggest that a fuzzy vault is particularly vulnerable to ARM attacks, where access to two or more fuzzy vaults generated from the same biometric data, but with different keys and chaff points, would enable an adversary to easily identify the original points in the two vault and thus decode the vault.

Therefore, the fuzzy vault approaches does not gave diversity and revocability. This means that, if a fuzzy vault is compromised, a new vault cannot be created from the same biometric data by simply binding it with a different key. Furthermore, the vulnerability of fuzzy vaults to ARM attacks allows cross-matching of templates across different systems, thereby user privacy is not ensured [13]. In a stolen key-inversion attack, if an attacker is able to recover the secret key embedded in the fuzzy vault (for example, through snooping), the secret polynomial may be directly reconstructed; thereby, the unprotected biometric template can be easily separated from the chaff points. A blended substitution attack is straightforward if an adversary is able to modify an existing fuzzy vault. In this attack, an impostor takes advantage of the myriad chaff points existing in the fuzzy vault to substitute some of these random points with his or her own biometric data, in which case both the legitimate user and the impostor would be able to be identified using the same fuzzy vault. Kholmatov and Yanikoglu [14] extended Scheirer and Boult [12] presenting experimental evidence that confirms a fuzzy vault‟s vulnerability to record multiplicity (correlation) attacks.

Nandakumar, et al. [13] further mention the possibility of exploiting the non-uniform nature of biometric features to launch an attack on a fuzzy vault based on statistical analysis of points in the vault. The authors also note the vulnerability of a fuzzy vault to attacks during the authentication stage, where a genuine user‟s original template is temporarily exposed and therefore vulnerable to snooping [15].

Another liability of the fuzzy vault scheme is the considerable increase in biometric template size as a result of the addition of a large number of chaff points. This may be undesirable in recognition systems that require a small template size. Furthermore, recognition accuracy may be adversely affected as a result of the large number of false points or too few true points in the protected template. For example, Clancy, et al. [16] implementation of the fuzzy vault on minutiae fingerprint showed an unacceptably high FRR of 20-30%.

Furhermore, key binding Fuzzy commitment Simoens, et al. [5] is a biometric cryptosystemgthat can begused to secure biometric traits representedgin the form of binary vectors. This characteristic of fuzzy commitment scheme makes it useful for applications biometric authenticationgsystems, in which data is subject to random noise. Because thegscheme is tolerantgof error, it is capable of protecting biometric data such as conventional cryptographic techniques,

ISBN: 978-979-3793-73-3

such as hashgfunctions, are used to protect alphanumericgpasswords[17].

In the key generationgbiometricgcryptosystems,the helper data is generated only from biometric templates and cryptographic keys directly generated from helper data and query biometric features. The direct key generation of biometrics is an attractive template-protectiongapproach that can be very usefulgincryptographicgapplications. Nevertheless, it is problematic to generate a key that could funding at the same time high stability and entropy due to intra-usergvariationgin the template. It's hard to develop a scheme that generates the same key for different templates of the same person and at the same time very different keys for different persons. E.g. quantization schemes and secure sketch.
In the quantization scheme method, helpergdata is quantized togobtain a stablegkey. This scheme takes feature vectors from multiple biometric samples and gets feature element intervals. The interval is encodedgandgthengstored in helpergdata. Throughout authentication, biometricgfeaturesaregcalculated and mappedgtodeterminedgintervals. Several studies in this method such as [18] use the DividegandgConquermethodgforfingerprin tgimages, and bio keys are generatedgusingminutiag set. Yang, et al. [19] proposed a fingerprintgcryptosystem by modifyinggVoronoiNeighbor Structure (VNS). In the same year, Yang, et al. [20] focused on the using of "Delaunay Quadrangle-based fingerprint authentication system that uses topological code for local enrollment and security enhancements."

C. *Template Transformation*

In this approach, the transformation function algorithm (F) is applied to the biometric template (T) and the result is stored in the database. The transformation function parameter usually comes from a random key (K) or password. The matching process is performed on the transformed domain. The feature transformation approach scheme can be further categorized as *salting* or *non-invertible transforms*.The security of salting schemes is based on the secrecy of the key or password. While, the security of non-invertible transformation techniques uses one way functions computationally difficult to invert, even if the key is known. Nevertheless, the disadvantage of these techniques is that security of the system is very difficult to verify due there is no foundation of mathematical to perform a robust security analysis and it is assumed that the distribution of uniform biometric features [21] and enemies may be able to utilize non-uniform biometric properties to launch attacks that may require less effort to compromise system security.

- Salting

Salting is a an approach used two-factor authentication scheme, in which an unprotected biometric template is transformed into a protected template via a function Specified by an external key or a user-specific keyword. Because transformations can be reversed for the most part, keys must be kept or remembered securely by the user and presented during authentication. The need for additional information is the key to improving entropy from biometric templates and therefore making it difficult for opponents to guess templates [6].

The limitations of the salting approach is that the security of this scheme depend on the secrecy of the key or password [15, 22]. As a result, effective key management procedures must be put into place, or else the user is obliged to memorise the secret key; however, relying on users‟ memory for the protection of complex secret keys

re-introduces the weakness of password-based schemes that we are trying to circumvent . Since matching is performed directly in the transformed domain, the salting functions must be designed such that they do not have an adverse effect on the recognition performance. This becomes especially important in the presence of large intra-user variations. Salting methods generally use quantization to deal with intra-user variability during matching in the transformed domain.

Several studies related to fingerprint salting approach will be discussed below. Teoh et al [23] introduced the bio phasor technique. This method is the pseudo-randomgnumbergmixing iteration with the fingerprintgfeature. Thisgwork is considered a stolengkeyg scenario. Then, Jin, et al. [24] proposed salting biohashing. The biohashing procedure was initially proposed for the fingerprint modality, and it consists of two stages. Firstly, the extracted fingerprint feature vector is transformed into a translation, rotation, and scale invariant feature set, employing the Wavelet Fourier-Mellin Transform $(WFMT)^2$. Secondly, the resulting data is discretised via an inner product computation between the invariant feature vector and a tokenised pseudorandom number sequence. The second stage of this process produces the protected biometric template vector, which is referred to as a BioHash.

The Biohashing procedure has been proven to be advantageous in several ways. Firstly, biohashing simultaneously provides high intra-class variation and extremely low inter-class correlation, which essentially leads to an Equal Error Rate (EER) of zero (when the legitimate token is used). This means that the occurrence of a False Accept is eliminated without a corresponding increase in the FRR [25]. It has also been claimed that Biohashing has a high tolerance to data capture offsets, such that the same biometric trait acquired at different times will produce highly correlated bit strings (BioHashes) [24]. This is due to the invariance of the feature vector created during the first stage of the Biohashing process, as well as the subsequent discretization of the invariant feature vector in the second stage. Another advantage of Biohashing is that it addresses the problem of irrevocability of biometric features: a user‟s compromised BioHash can be easily revoked and replaced with a new one by using a different secret seed for enrolment.However, Biohasing schemes have weaknesses that have been presented by researchers. The most commonly analysed limitation of the Biohashing approach is the degradation in matching performance when an adversary has access to a user‟s secret key (seed) and uses the legitimate key with their own biometric features in order to fool the system into authenticating them [26].

Several researchers have presented methods for resolving performance degradation resulting from a stolen-token scenario, such as [27-29]. Beacuse a salting approach is by nature invertible, almost no any existing literary works focus on improving the non-invertibility property of Biohashing; however, there are two suggestions are presented in [30, 31]. In fact, Biohashing on its own technically cannot be made to be noninvertible. A hybrid protection scheme, incorporating techniques other than salting, would be required; for example, applying Biohashing to a non-invertible template. Other salting techniques, which do not adopt Biohashing, are also available in the literature; such as [32, 33].

ISBN: 978-979-3793-73-3

- *Non-Invertible Transform*

One-way functions applied to biometric data. To update biometric templates, function parameters must be changed. In case the transformed parameters are compromised the attacker can not reconstruct the original biometric template. Because of intra-class variations, transformations need to align biometric templates to perform effective comparisons and this leads to reduced authentication performance. A non-invertible transform shows the impossibility on obtaining the original biometric data from its transformed version. Thegparametersgofgthegtransformationgfunction are specified by a key, but knowledge of the key and/or the transformed template does not facilitate recovery of the original biometric template [6, 34].

The major advantage of the non-invertible transform scheme approach compared to the salting approach, and it means that biometric templates that are protected using non-invertible transforms are generally more secure than those protected using the salting approach. Then, a related advantage of the non-invertible transform approach is that, unlike salting, it does not require storage of any secret information. The next positive aspect of non-invertible transforms is that they tend to leave the protected biometric template in the same feature space s its unprotected counterpart. In this case, intra-user variations in the transformed biometric templates can be robustly handled by using existing, sophisticated matchers, thereby reducing the error rates of the biometric system [35]. Furthermore, the matching scores obtained are proportional to those obtained in the original space, and thus can be used in the design of a secure multibiometric system through a scoreline-level fusion method.

The main limitation of the non-invertible transformation method lies in the difficulty of designing a good one-way function. The transformation function must ensure that the biometric features from the same user maintain a high similarity in the transformed space, while features from different users are completely unrelated after transformation. However, the transformation must also be non-invertible, so that an adversary is unable to collect any information about the original biometric template from its protected counterpart. There is a trade-off between discriminability and non-invertibility, since it is challenging to design transform functions that satisfy both requirements simultaneously.

Consequently, often the greater the amount of distortion applied to the original biometric data by the transformation, the worse the recognition performance among the protected biometric templates. This means that the non-invertible transform approach typically suffers from a security versus performance trade-off. Furthermore, the transformation function relies heavily on biometric features to be used in specific applications. This analysis makes evident a clear comparison between the salting and non-invertible transform approaches. While salting schemes (such as BioHashing) generally tend to either preserve or improve the recognition performance of the biometric system into which they are incorporated, non-invertible transforms often have the effect of degrading the recognition accuracy somewhat. On the other hand, non-invertible transforms tend to impart more security to the protected biometric templates compared to salting approaches, which are invertible with the revelation of the user-specific key.

In this scheme,the most influential researcher are Ratha, et al. [36]. They proposed and analyzed cancelable biometrics fingerprint using non-invertible transforms for generating fingerprint templates. The scheme of cancelable biometrics is to change the raw biometric templates by using either feature or signal domain transformations. Cartesian, polar and functional are the three functions of the transformation. These functions used to transform fingerprint minutiae data so that a minutiae matcher can still be applied to the transformed minutiae.

For the functional transformation, Ratha, et al. [37] used a mixture of 2D Gaussians and electric potential field in a 2D random charge distribution as a means to translate the minutia points. Research with the same technique is also done by Yang, et al. [38] who developed a non-invertible transformation for fingerprints by considering local and global features of minutia points. The distance between the minutiae pair is projected vertically to the circle. Later, Lee and Kim [39] proposed a new representation of the minutiae points of the fingerprint image made using bit strings. Minutia points of the fingerprint image are mapped to a 3D array that is divided into small cells. A string of bits is generated by finding which cells include minutiae points. Subsequent research conducted by Zhe and Jin [40], they proposed the protection of a fingerprint template obtained using a projected MVD feature at random. Ahmad, et al. [41] introduced a pair of polar relationships of minutiae. The correlation-based filter method using chip matching was proposed by Takahashi and Hirata [42]. Wang and Hu [43] proposed the Densely Infinite To One Mapping (DITOM) approach use of Correlation Invariant Random Filtering (CIRF). Das, et al. [44] meant a method based on the Minimum Distance graph. The hashing algorithm is constructed using this graph and an appropriate search algorithm is used to match the resulting hash. Ferrara, et al. [45] making the non-invertible Cylinder Minutiae Code (pMCC) for fingerprints as a fingerprint enhancement enhancement fingerprint..

D. ***Hybrid Methods***

Several fingerprint template protection schemes used combination of feature transformation and biometric cryptosystems. Usually it called hybrid methods. Several hybrid system examples are presented in the literature, some of which even incorporate traditional cryptographic hashing functions into the hybrid protection system. For Example hardening a fingerprint-based fuzzy vault with a user-specific password, combined key binding with salting [13]. An application-specific key release scheme that retrieves a cryptographic key bound to a BioHashed fingerprint, combined salting with key binding methods [46].

In addition, Several studies that have been done in fingerprint template protection based on hybrid scheme are Boult, et al. [47] presented revocable biotokens for fingerprint biometrics. This technique divides data into two parts fractional and integer parts. The fractional part performs the transformation and the integer part is encrypted.. The fractional part does the transformation and integer part is encrypted. Then, Feng, et al. [48] also developed a three-step hybrid algorithm based on random projection, discriminability-preserving (DP) transform, and fuzzy commitment scheme. In similar way, Nagar, et al. [30] constructing a hybrid cryptosystem with minutiae descriptors for fingerprints. This work used both fuzzy vault and fuzzy commitment scheme to build the cryptosystem. The helper data extraction involves fuzzy vault encoding and the ordinate values secured by fuzzy commitment.

ISBN: 978-979-3793-73-3

Furthermore, Chin, et al. [49] proposed a hybrid system using fingerprint and palmprint features, then Sandhya and Prasad [50] constructed Delaunay triangles from fingerprint minutiae. The features are transformed and then a cryptosystem was built using fuzzy commitment scheme. Convolution code was used to generate the error correction code. Finally, Jin, et al. [51] proposed a long ECC free key-binding scheme with a cancelable transforms for minutia-based fingerprint biometrics. The minutiae information is secured by a strong noninvertible cancelable transform called modified Randomized Graph based Hamming Embedding. The advantage of hybrid protection schemes is that they can combine the high revocability and diversity properties characteristic of feature transformation approaches with the high security offered by biometric cryptosystems [6].After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your conference for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper; use the scroll down window on the left of the MS Word Formatting toolbar.

E. Homomorphic Encryption

Another alternative, apart from the above 4 methods is homomorphic encryption. This technique allows a limited subset of calculations on encrypted data. Combining Homomorphic Encryption with a biometric recognition system will meet the requirements of Biometric Template Protection without degrading the accuracy [52]. The fingerprint template protection study under the Homomorphic Encryption scheme was developed at Rane et al. [53] They presented the calculation of Hamming distance for fingerprint applications. Then, Barni, et al. [54] shows distributed biometric systems by utilizing cryptosystems, homomorphic encryption on Fingercode templates in a semi-honest model.

5. CONCLUSION AND FUTURE WORK

This paper provides and summarizes information about research issues related to fingerprint template protection. Based on a survey of 54 papers conducted it can be concluded that there are 5 techniques that can be done to solve the problem of fingerprint template protection that is encryption standard, biometric cryptosystem, template transformation, hybrid methods and homomorphic encryption. Then there has not been the best approach to template protection that actually meets the main requirements of template security, revocability. diversity and performance matching accuracy. Application requirements and user-desired scenarios play a key role in the selection of template protection schemes.

REFERENCES

[1] A. K. Jain, K. Nandakumar, and A. Nagar, "Fingerprint template protection: From theory to practice," in *Security and Privacy in Biometrics*, ed: Springer, 2013, pp. 187-214.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *International Conference on Audio-and Video-Based Biometric Person Authentication*, 2001, pp. 223-228.

[3] B. Schneier, "Security pitfalls in cryptography," 1998.

[4] N. K. Ratha and R. Bolle, "IO SMARTCARD BASED AUTHENTICATION," *Biometrics:*

Personal Identification in Networked Society, vol. 479, p. 369, 1999.

[5] K. Simoens, B. Yang, X. Zhou, F. Beato, C. Busch, E. M. Newton, *et al.*, "Criteria towards metrics for benchmarking template protection algorithms," in *Biometrics (ICB), 2012 5th IAPR International Conference on*, 2012, pp. 498-505.

[6] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 2008, p. 113, 2008.

[7] H. Al-Assam, H. Sellahewa, and S. Jassim, "A lightweight approach for biometric template protection," in *SPIE Defense, Security, and Sensing*, 2009, pp. 73510P-73510P-12.

[8] A. Vetro and N. Memon, "Biometric system security," in *Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea*, 2007.

[9] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. V. Kumar, "Biometric Encryption: enrollment and verification procedures," in *Aerospace/Defense Sensing and Controls*, 1998, pp. 24-35.

[10] G. J. Tomko, C. Soutar, and G. J. Schmidt, "Fingerprint controlled public key cryptographic system," ed: Google Patents, 1996.

[11] E.-C. Chang, R. Shen, and F. W. Teo, "Finding the original point set hidden among chaff," in *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*, 2006, pp. 182-188.

[12] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in *Biometrics Symposium, 2007*, 2007, pp. 1-6.

[13] K. Nandakumar, A. Nagar, and A. K. Jain, "Hardening fingerprint fuzzy vault using password," in *International conference on Biometrics*, 2007, pp. 927-937.

[14] A. Kholmatov and B. Yanikoglu, "Realization of correlation attack against the fuzzy vault scheme," in *Proc. SPIE*, 2008, pp. 1-7.

[15] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*: Springer Science & Business Media, 2009.

[16] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure smartcardbased fingerprint authentication," in *Proceedings of the 2003 ACM SIGMM workshop on Biometrics methods and applications*, 2003, pp. 45-52.

[17] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," 2013.

[18] R. Ranjan and S. K. Singh, "Improved and innovative key generation algorithms for biometric cryptosystems," in *Advance Computing Conference (IACC), 2013 IEEE 3rd International*, 2013, pp. 943-946.

[19] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor

ISBN: 978-979-3793-73-3

structures," *Pattern Recognition*, vol. 47, pp. 1309-1320, 2014.

[20] W. Yang, J. Hu, and S. Wang, "A Delaunay quadrangle-based fingerprint authentication system with template protection using topology code for local registration and security enhancement," *IEEE transactions on Information Forensics and Security*, vol. 9, pp. 1179-1192, 2014.

[21] M. Kaur, S. Sofat, and D. Saraswat, "Template and database security in Biometrics systems: A challenging task," *International Journal of Computer Applications*, vol. 4, pp. 1-5, 2010.

[22] L. Nanni and A. Lumini, "Cancellable biometrics: problems and solutions for improving accuracy," *Biometrics: Methods, Applications and Analyses*, 2010.

[23] A. B. Teoh and D. C. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *Control, Automation, Robotics and Vision, 2006. ICARCV'06. 9th International Conference on*, 2006, pp. 1-5.

[24] A. T. B. Jin, D. N. C. Ling, and A. Goh, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern recognition*, vol. 37, pp. 2245-2255, 2004.

[25] A. Lumini and L. Nanni, "An improved biohashing for human authentication," *Pattern recognition*, vol. 40, pp. 1057-1065, 2007.

[26] H. Al-Assam, H. Sellahewa, and S. Jassim, "Multi-Factor Biometrics for Authentication: A false sense of security," in *Proceedings of the 12th ACM Workshop on Multimedia and Security*, 2010, pp. 81-88.

[27] D. Maio and L. Nanni, "Multihashing, human authentication featuring biometrics data and tokenized random number: A case study FVC2004," *Neurocomputing*, vol. 69, pp. 242-249, 2005.

[28] A. B. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern recognition*, vol. 41, pp. 2034-2044, 2008.

[29] A. B. J. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 37, pp. 1096-1106, 2007.

[30] A. Nagar, K. Nandakumar, and A. K. Jain, "A hybrid biometric cryptosystem for securing fingerprint minutiae templates," *Pattern Recognition Letters*, vol. 31, pp. 733-741, 2010.

[31] Y. Wang and K. Plataniotis, "Face based biometric authentication with changeable and privacy preservable templates," in *Biometrics Symposium, 2007*, 2007, pp. 1-6.

[32] S. Hirata and K. Takahashi, "Cancelable biometrics with perfect secrecy for correlation-based matching," *Advances in Biometrics*, pp. 868-878, 2009.

[33] M. Elmezain, A. Al-Hamadi, J. Appenrodt, and B. Michaelis, "A

hidden markov model-based continuous gesture recognition system for hand motion trajectory," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, 2008, pp. 1-4.

[34] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, "Securing Fingerprint Systems," *Handbook of Fingerprint Recognition*, pp. 371-416, 2009.

[35] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: a security analysis," in *IS&T/SPIE Electronic Imaging*, 2010, pp. 75410O-75410O-15.

[36] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM systems Journal*, vol. 40, pp. 614-634, 2001.

[37] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, 2007.

[38] H. Yang, X. Jiang, and A. C. Kot, "Generating secure cancelable fingerprint templates using local and global features," in *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, 2009, pp. 645-649.

[39] C. Lee and J. Kim, "Cancelable fingerprint templates using minutiae-based bit-strings," *Journal of Network and Computer Applications*, vol. 33, pp. 236-246, 2010.

[40] J. Zhe and A. T. B. Jin, "Fingerprint template protection with minutia vicinity decomposition," in *Biometrics (IJCB), 2011 International Joint Conference on*, 2011, pp. 1-7.

[41] T. Ahmad, J. Hu, and S. Wang, "Pair-polar coordinate-based cancelable fingerprint templates," *Pattern Recognition*, vol. 44, pp. 2555-2564, 2011.

[42] K. Takahashi and S. Hirata, "Cancelable biometrics with provable security and its application to fingerprint verification," *IEICE transactions on fundamentals of electronics, communications and computer sciences*, vol. 94, pp. 233-244, 2011.

[43] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (DITOM) approach," *Pattern Recognition*, vol. 45, pp. 4129-4137, 2012.

[44] P. Das, K. Karthik, and B. C. Garai, "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs," *Pattern Recognition*, vol. 45, pp. 3373-3388, 2012.

[45] M. Ferrara, D. Maltoni, and R. Cappelli, "Noninvertible minutia cylinder-code representation," *IEEE Transactions on Information Forensics and Security*, vol. 7, pp. 1727-1737, 2012.

[46] T. S. Ong, A. T. B. Jin, and D. C. L. Ngo, "Application-Specific Key Release Scheme from Biometrics,"

ISBN: 978-979-3793-73-3

IJ Network Security, vol. 6, pp. 127-133, 2008.

[47] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy and security analysis," in *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on*, 2007, pp. 1-8.

[48] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE transactions on information forensics and security*, vol. 5, pp. 103-117, 2010.

[49] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," *Information Fusion*, vol. 18, pp. 161-174, 2014.

[50] M. Sandhya and M. V. Prasad, "Cancelable fingerprint cryptosystem based on convolution coding," in *Advances in Signal Processing and Intelligent Recognition Systems*, ed: Springer, 2016, pp. 145-157.

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

[52] S. Ye, Y. Luo, J. Zhao, and S.-C. Cheung, "Anonymous biometric access control," *EURASIP Journal on Information Security*, vol. 2009, p. 865259, 2009.

[53] S. D. Rane, W. Sun, and A. Vetro, "Secure distortion computation among untrusting parties using homomorphic encryption," in *Image Processing (ICIP), 2009 16th IEEE International Conference on*, 2009, pp. 1485-1488.

[54] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. D. Labati, P. Failla, *et al.*, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in *Biometrics: theory applications and systems (BTAS), 2010 Fourth IEEE International Conference on*, 2010, pp. 1-7.

Certificate Number: 014/Certificate/ICoSET/2017

YAYASAN LEMBAGA PENDIDIKAN ISLAM (YLPI) RIAU
UNIVERSITAS ISLAM RIAU

UIR INTERNATIONAL CONFERENCE 2017

ICOSET

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY

CERTIFICATE

This is to certify that

EVIZAL ABDUL KADIR

has participated in International Conference on Science, Engineering and Technology (ICOSET)
"Sustainable Development in Developing Country" as

PRESENTER

held by Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Islam Riau, Indonesia

Pekanbaru, 8-10 November 2017

University Partners:

UUM Universiti Utara Malaysia
CHIBA UNIVERSITY
NGUYEN TRAI UNIVERSITY

Prof. Dr. H. Syafrinaldi, SH., M.C.L
Rector of Universitas Islam Riau

Dr. Evizal Abdul Kadir, M. Eng
Conference Chair

Certificate Number: 043/Certificate/ICoSET/2017

YAYASAN LEMBAGA PENDIDIKAN ISLAM (YLPI) RIAU
UNIVERSITAS ISLAM RIAU

UIR INTERNATIONAL CONFERENCE 2017

ICOSET

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING AND TECHNOLOGY

CERTIFICATE

This is to certify that

EVIZAL ABDUL KADIR

has participated in International Conference on Science, Engineering and Technology (ICOSET)
"Sustainable Development in Developing Country" as

CHAIR

held by Lembaga Penelitian dan Pengabdian Masyarakat (LPPM) Universitas Islam Riau, Indonesia

Pekanbaru, 8-10 November 2017

University Partners:

UNIVERSITAS ISLAM RIAU
PEKANBARU
REKTOR

Prof. Dr. H. Syafrinaldi, SH., M.C.L
Rector of Universitas Islam Riau

UNIVERSITAS ISLAM RIAU
PEKANBARU
LEMBAGA PENELITIAN DAN PENGABDIAN KEPADA MASYARAKAT

Dr. Evizal Abdul Kadir, M. Eng
Conference Chair