Journal of Theoretical and Applied Information Technology
31st May 2018. Vol.96. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FINGERPRINT TEMPLATE PROTECTION SCHEMES: A LITERATURE REVIEW

[1]APRI SISWANTO, [2]NORLIZA KATUK, [3]KU RUHANA KU-MAHAMUD

[1]Department of Informatic, Faculty of Engineering, Universitas Islam Riau, 28284, Perhentian Marpoyan, Pekanbaru, Indonesia

[2,3]School of Computing, College of Arts and Sciences, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah, Malaysia

E-mail: [1]aprisiswanto@eng.uir.ac.id, [2]k.norliza@uum.edu.my, [3]ruhana@uum.edu.my

ABSTRACT

The fingerprint is the most widely used technology for identification or authentication systems, which can be known as fingerprint authentication systems (FAS). In addition to providing security, the fingerprint is also easy to use, very reliable and has a high accuracy for identity recognition. FAS is still exposed to security attacks because fingerprint information is unencrypted. Therefore, fingerprint information requires protection known as fingerprint template protection (FTP). This paper aims to provide an organized literature on FTP. Three research questions were formulated to guide the literature analysis. First, this analysis focuses on the types of FTP schemes; second, the metrics used for evaluating the FTP schemes; and finally, the common datasets used for evaluating the FTP schemes. The latest information and references are analysed and classified based on FTP methods and publication year to obtain information related to the development and application of FTP. This study mainly surveyed 62 documents reported on FTP schemes between the year 2000 and 2017. The results of this survey can be a source of reference for other researchers in finding literature relevant to the FTP.

Keywords: *Biometric Authentication, Fingerprint Template Protection, Template Transformation, Fingerprint Cryptosystem, Authentication Systems*

1. INTRODUCTION

Biometric technology is used widely as an authentication mechanism to overcome the weaknesses found in traditional methods such as password and security code [1]. Unlike the traditional methods, an individual user must be physically present during the authentication process; hence, the risk of impersonation is very low. Further, authentication using biometric technology does not require users to remember the password or carry such tokens (e.g., smart card, and keys) which makes it a mobile and practical solution for authentication.

One of the most widely used biometric technology is fingerprint such those found in attendance systems, personal identification systems, smart home systems, payment systems, crime detection systems and border security control systems [2]. Fingerprints have a unique shape for everyone. That is, each person has a different form of fingerprint despite being born twin. The reduction in the size and cost of modern fingerprint scanners makes fingerprints very likely to continue as a prominent authentication method in the future.

Although fingerprints are unique and hard to forge, the current fingerprint authentication systems are still exposed to security attacks. Unencrypted fingerprint information (i.e., fingerprint templates (FT)) stored in the database could be stolen or captured during its transmission in the communication line. The method for securing the fingerprint information is called as fingerprint template protection (FTP). To date, various methods and techniques have been developed by researchers in this field including fingerprint cryptosystem (FC), cancellable fingerprint (i.e., template transformation), hybrid methods, and homomorphic encryption [3].

Recent and previous studies by other researchers have reported the great amount of enhancements on FTP which cause an emerging of many new FTP schemes. However, to our knowledge, there is no specific work surveying the FTP schemes in the literature. Surveying those FTP schemes may provide

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

researchers with state-of-the-art in the field and could encourage further developments. Therefore, this paper aims to fill the gap by reviewing the literature related to FTP schemes. Three research questions (RQ) were formulated as below:

RQ1: What are the types of FTP schemes that researchers studied?
RQ2: What are the metrics used for evaluating the FTP schemes?
RQ3: What are the common datasets used for evaluating the FTP schemes?

The paper is organized in the following way. Section 2 discusses the method for conducting the study. Then, Section 3 presents the results of the study based on the specified RQs. Finally, Section 4 discusses the limitation of the study and concludes the finding.

2. METHOD

A comprehensive electronic document search was done using the main keyword 'fingerprint template protection' to get the key findings, the types of FTP schemes, the performance measures, and the dataset. In addition, there are other several key terms such as cancellable fingerprint, transformation template, feature transformation, biometric cryptosystem, fingerprint cryptosystem, fingerprint cryptography, and homomorphic encryption were used in the search. The search focused on English documents published between January 2000 and December 2017. It was conducted using academic search engine Google Scholar.

In the first phase, the search was done using the main keyword 'fingerprint template protection'. At this stage, there were more than 3600 documents found in Google Scholar. After the results were filtered, only 20 relevant documents were selected. It comprises two e-books, two doctoral theses, eleven articles from journals and five conference articles [4-23].

In the second phase, an extended searching was done using supporting keywords including cancellable fingerprint, transformation template, feature transformation, biometric cryptosystem, fingerprint cryptosystem, fingerprint cryptography, and homomorphic encryption. The search returned more than a thousand documents. After the results were filtered, 42 relevant documents were selected. These documents comprise 25 articles in journals and 17 conference articles.

Figure 1 illustrates the literature review process. The total of 62 documents were analysed by extracting information on the key findings of the FTP schemes that the researchers proposed, the evaluation metric, and the dataset used for evaluating the schemes. Table 1 shows the information of the 62 documents included in the study. It covers the year, the number of citations received in Google Scholar (as of February 2018) authors, titles, and types of document.

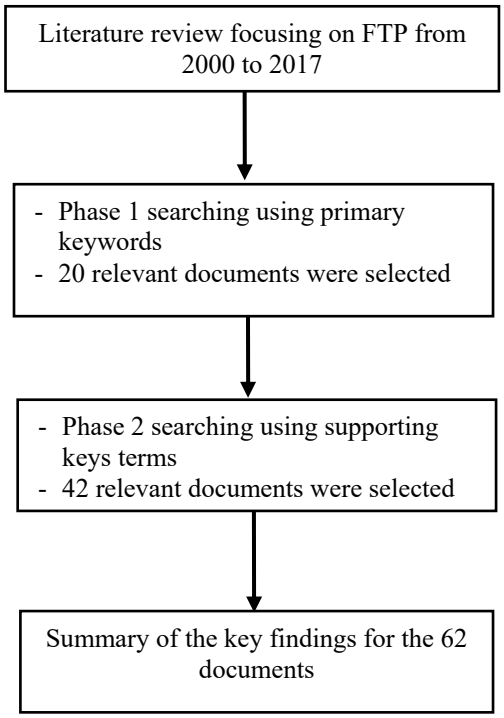

Figure 1: The literature review process

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: List of the 62 documents included in this study

Num.	Year	Number of citations	Authors	Title	Type of document
1	2012	61	Jin, et al.	Fingerprint Template Protection with Minutiae-Based Bit-String for Security and Privacy Preserving [4]	Journal
2	2010	33	Yang, et al.	Robust Minutiae Hash for Fingerprint Template Protection [5]	Conference article
3	2012	7	Yang, et al.	Performance Evaluation of Fusing Protected Fingerprint Minutiae Templates on The Decision Level [6]	Journal
4	2014	1	Subban	Fingerprint Template Protection Techniques- A Survey and Analysis [7]	Conference article
5	2015	1	Krivokuca	Fingerprint Template Protection Using Compact Minutiae Patterns [8]	Ph.D. thesis
6	2011	1	Choi, et al.	Fingerprint Template Protection Using One-Time Fuzzy Vault [9]	Journal
7	2016	-	Krivokuća and Abdulla	Cancellability and Diversity Analysis of Fingerprint Template Protection Scheme Based on Compact Minutiae Pattern [10]	Journal
8	2017	-	Stanko and Skoric	Minutia-Pair Spectral Representations for Fingerprint Template Protection [11]	Journal
9	2016	-	Poonguzhali and Ezhilarasan	A Hybrid Template Protection Technique for Fingerprint Biometric Authentication System [12]	Conference article
10	2015	10	Tams, et al.	Improved Fuzzy Vault Scheme for Alignment-Free Fingerprint Features [13]	Conference article
11	2015	-	Jin	Privacy-Preserving Minutia-Based Fingerprint Template Protection Techniques [14]	Ph.D. thesis
12	2016	-	Kumar and Garg	A Fingerprint Template Protection Using Watermarking [15]	Journal
13	2017	-	Nazmul, et al.	Alignment-Free Fingerprint Template Protection Technique Based on Minutiae Neighbourhood Information [16]	Conference article
14	2005	373	Tuyls, et al.	Practical Biometric Authentication with Template Protection [17]	Conference article
15	2013	25	Jain, Nandakumar, and Nagar	Fingerprint Template Protection: From Theory to Practice [18]	E-book
16	2014	-	Fernandez	Fingerprint Template Protection Scheme, Security and Vulnerabilities: A Survey [19]	Conference article
17	2016	1	Ashish and Sinha	Biometric Template Protection [20]	Journal
18	2011	17	Takahashi and Hirata	Cancelable Biometrics with Provable Security And Its Application To Fingerprint Verification [21]	Conference article
19	2009	4676	Maltoni, et al.	Handbook of Fingerprint Recognition [22]	E-book
20	2006	268	Uludag and Jain	Securing Fingerprint Template: Fuzzy Vault With Helper Data [23]	Conference article
21	2007	22	Moon, et al.	Fingerprint Template Protection Using Fuzzy Vault [24]	Conference article
22	2006	47	Teoh and Ngo	Biophasor: Token Supplemented Cancellable Biometrics [25]	Conference article

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

23	2007	767	Ratha, Chikkerur, Connell, and Bolle	Generating Cancelable Fingerprint Templates [26]	Conference article
24	2008	144	Nagar, Nandakumar, and Jain	Securing Fingerprint Template: Fuzzy Vault With Minutiae Descriptors [27]	Conference article
25	2007	52	Teoh and Kim	Secure Biometric Template Protection in Fuzzy Commitment Scheme [28]	Journal
26	2008	100	Kholmatov and Yanikoglu	Realization of Correlation Attack Against The Fuzzy Vault Scheme [29]	Conference article
27	2007	152	Boult, Scheirer, and Woodworth	Revocable Fingerprint Biotokens: Accuracy and Security Analysis [30]	Conference article
28	2008	47	Chikkerur, Ratha, Connell, and Bolle	Generating Registration-Free Cancelable Fingerprint Templates [31]	Conference article
29	2009	43	Yang, Jiang, and Kot	Generating Secure Cancelable Fingerprint Templates Using Local and Global Features [32]	Conference article
30	2010	75	Nandakumar	A Fingerprint Cryptosystem Based on Minutiae Phase Spectrum [33]	Conference article
31	2010	100	Lee and Kim	Cancelable Fingerprint Templates Using Minutiae-Based Bit-Strings [34]	Journal
32	2010	24	Liu, Liang, Pang, Xie, and Tian	Minutiae and Modified Biocode Fusion for Fingerprint-Based Key Generation [35]	Journal
33	2010	130	Nagar, Nandakumar, and Jain	A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates [36]	Journal
34	2011	3	Zhou, Opel, Merkle, Korte, and Busch	Enhanced Template Protection with Passwords for Fingerprint Recognition [37]	Conference article
35	2011	15	Zhe and Jin	Fingerprint Template Protection with Minutia Vicinity Decomposition [38]	Conference article
36	2011	112	Ahmad, Hu, and Wang	Pair-Polar Coordinate-Based Cancelable Fingerprint Templates [39]	Journal
37	2012	98	Wang and Hu	Alignment-Free Cancelable Fingerprint Template Design: A Densely Infinite-To-One Mapping (DITOM) Approach [40]	Journal
38	2012	46	Das, Karthik, and Garai	A Robust Alignment-Free Fingerprint Hashing Algorithm Based on Minimum Distance Graphs [41]	Journal
39	2012	89	Ferrara, Maltoni, and Cappelli	Noninvertible Minutia Cylinder-Code Representation [42]	Journal
40	2012	50	Li, et al.	An Effective Biometric Cryptosystem Combining Fingerprints with Error Correction Codes [43]	Journal
41	2013	27	Imamverdiyev, Teoh, and Kim	Biometric Cryptosystem Based On Discretized Fingerprint Texture Descriptors [44]	Journal
42	2013	9	Ranjan and Singh	Improved and Innovative Key Generation Algorithms for Biometric Cryptosystems [45]	Conference article
43	2014	31	Prasad and Kumar	Fingerprint Template Protection Using Multiline Neighboring Relation [46]	Journal
44	2014	31	Yang, Hu, and Wang	A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Using Topology Code for Local Registration and Security Enhancement [47]	Journal

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

45	2015	12	Nguyen, Wang, Ha, and Li	Performance and Security-Enhanced Fuzzy Vault Scheme Based on Ridge Features for Distorted Fingerprints [48]	Journal
46	2015	6	Bansal, Sofat, and Kaur	Fingerprint Fuzzy Vault Using Hadamard Transformation [49]	Conference article
47	2016	22	Li and Hu	A Security-Enhanced Alignment-Free Fuzzy Vault-Based Fingerprint Cryptosystem Using Pair-Polar Minutiae Structures [50]	Journal
48	2015	26	Murillo-Escobar, Cruz-Hernández, Abundiz-Pérez, and López-Gutiérrez	A Robust Embedded Biometric Authentication System Based on Fingerprint and Chaotic Encryption [51]	Journal
49	2015	11	Sandhya and Prasad	K-Nearest Neighborhood Structure (K-NNS) Based Alignment-Free Method for Fingerprint Template Protection [52]	Conference article
50	2016	17	Wang and Hu	A Blind System Identification Approach to Cancelable Fingerprint Templates [53]	Journal
51	2016	4	Sandhya and Prasad	Cancelable Fingerprint Cryptosystem Based on Convolution Coding [54]	Journal
52	2016	19	Jin, Teoh, Goi, and Tay	Biometric Cryptosystems: A New Biometric Key Binding and Its Implementation for Fingerprint Minutiae-Based Representation [55]	Journal
53	2010	79	Barni, et al.	A Privacy-Compliant Fingerprint Recognition System Based on Homomorphic Encryption and Fingercode Templates [56]	Conference article
54	2016	-	Guo, Mao, and Guo	Non-Invertible Fingerprint Template Protection with Polar Transformations [57]	Conference article
55	2016	21	Wong, Teoh, Kho, and Wong	Kernel PCA Enabled Bit-String Representation for Minutiae-Based Cancellable Fingerprint Template [58]	Journal
56	2017	-	Gao	Toward Constructing Cancellable Templates Using K-Nearest Neighbour Method [59]	Journal
57	2017	13	Gomez-Barrero, Maiorana, Galbally, and Campisi	Multi-Biometric Template Protection Based on Homomorphic Encryption [60]	Journal
58	2017	-	Sadhya and Singh	Design of A Cancelable Biometric Template Protection Scheme for Fingerprints Based on Cryptographic Hash Functions [61]	Journal
59	2017	3	Wang, Yang, and Hu	Design of Alignment-Free Cancelable Fingerprint Templates With Zoned Minutia Pairs [62]	Journal
60	2017	-	Jin, Lai, Hwang, Kim, and Teoh	A New and Practical Design of Cancellable Biometrics: Index-Of-Max Hashing [63]	Journal
61	2007	172	Nandakumar, Nagar, and Jain	Hardening Fingerprint Fuzzy Vault Using Password [64]	Conference article
62	2009	25	Rane, Sun, and Vetro	Secure Distortion Computation Among Untrusting Parties Using Homomorphic Encryption [65]	Conference article

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The 62 documents that have been selected in this survey were classified based on the year of publication as visualized in Figure 2.

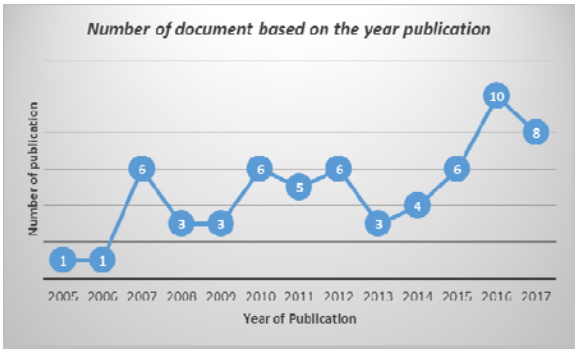

Figure 2: Number of documents based on the year of publication

3. RESULTS

3.1 What are the types of FTP schemes that researchers studied?

FTP schemes can be categorized into four major groups that are fingerprint cryptosystem, template transformation, hybrid methods, and homomorphic encryption such as shown in Figure 3.

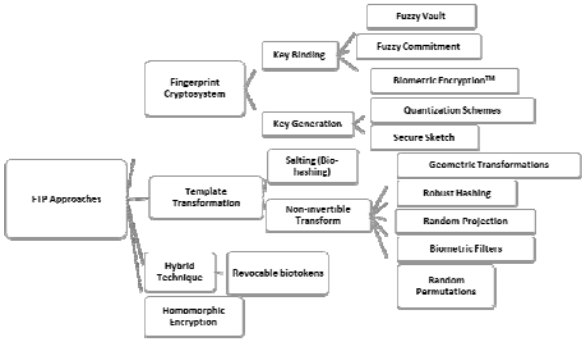

Figure 3: Categorization of FTP schemes

In the first category that is fingerprint cryptosystems (FC), helper data is used to describe additional information of FT stored in the database [66]. The helper data is required to extract a cryptographic key from the query fingerprint features during matching. It does not expose significant information about the original fingerprint. Matching is done indirectly by verifying the truth of the extracted key. Typically, error correction coding techniques are used to handle intra-user variations. Based on how the helper data derived, the FC are divided into key binding and key generation system.

The helper data is acquired by binding a key, that is free from the fingerprint features of the FT. Computationally, it is difficult to decode the key or the template with no knowledge of the user's fingerprint data. Techniques of error correction coding are employed to provide tolerance to intra-user variations in fingerprint data. However, the application precludes the use of sophisticated matcher, which leads to a reduction in the matching accuracy. In general, a key-binding FC is not designed to provide diversity and revocability in fingerprint protected templates [67]. This approach may be improved to take these two properties into account, and indeed some efforts in this direction have already been made with hybrid system. Some of the techniques in this category are fuzzy vault, fingerprint encryption, and fuzzy commitment.

In key generation FC, the based idea is to directly produce a cryptographic key from the fingerprint data, instead of binding an existing key with the FT as in key binding fingerprint cryptosystems [67]. This means the helper data is derived only from the FT, and the cryptographic key is directly generated from the helper data and the query fingerprint features [68]. Direct key generation of fingerprints is an attractive FTP approach that can also be very useful in cryptographic applications. However, it is difficult to generate keys that can provide stability and entropy along with intra-user variations in templates. It is difficult to develop a scheme generating the same key for different templates of the same individual, and at the same time has a very different key for different individuals, for example, quantization schemes and secure sketch.

In the second category that is the template transformation approach, transformation function is used to convert user templates (T) listed in the system into a protected template (T'). The transform function (F) is characterized by a set of user-specific parameters, which usually come from a random external keys or random password (K). After that, only the protected template, F (T, K), is stored in the system database. Matching process is performed in the transformed domain. *Salting* and *non-invertible* transforms are the two most popular schemes in feature transformation approaches. Schematically, the authentication process in a FTP based on feature transformation is depicted in Figure 4.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Figure 4: The authentication process in a fingerprint recognition system employing feature transformation [68]

Salting is one of FTP approaches that uses a two-factor authentication scheme, where an unprotected FT is converted to a protected template through a function defined by an external key or a specific user key. As long as key authentication should be kept or remembered safely by the user because the transformation can be reversed, for the most part. This requires additional information on the form of keys that increase the entropy of the FT and hence make it difficult for the opponent to guess the template [68]. The salting approach has a particular limitation in that the security depends on the secrecy of the password or key [22, 69]. However, using the memory of users for protecting complex secret keys reveals the weakness of password-based schemes. Because matching is directly performed in the transformed domain, the salting functions must not have an adverse effect on the performance of recognition. This is important, specifically when there are large intra-user variations. Generally, salting methods employ quantization to handle intra-user variability during matching in the transformed domain.

Meanwhile, in non-invertible transform approach, a one-way function non-invertible transform applying to secure the FT. The intruder cannot reconstruct the original FT if the transformation parameters are compromised. Due to intra-class variations, the transformation has to align FT to run an effective comparison. This reduces the authentication performance. A non-invertible transform indicates the impossibility of obtaining the original data of fingerprint from the transformed version. The transformation function parameters are specified by a key; however, knowledge of the key and/or the transformed template does not promote the recovery of the original template of fingerprint [67, 68]. The non-invertible transformation method has a limitation related to the difficulty in the design of a good one-way function. The function of transformation has to ensure that the features of a fingerprint from the same user maintain a high similarity in the transformed space. Meanwhile, features from different users are unrelated after transformation. However, the transformation must also be non-invertible. Thus, an adversary is not able to collect any information about the original FT from its protected counterpart.

Ratha, et al. [70] proposed a cancellable fingerprint using non-invertible transforms for producing cancellable FT. It can change the raw FT by using either feature or signal domain transformations. The three transformation functions include Cartesian transformation, polar transformation, and functional transformation. Figure 5 shows Ratha, et al.'s scheme.

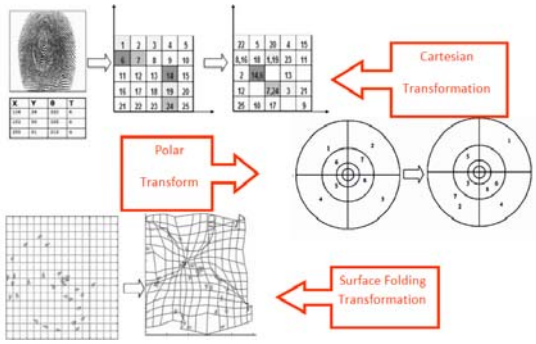

Figure 5: Ratha, et al.'s schemes using Cartesian, polar and functional transformation

The third category is hybrid techniques that can be designed by combining feature transformation and FC. Some of the systems incorporate the functions of traditional cryptographic hashing into the FTP, such as an application-specific key releases scheme that retrieves a cryptographic key bound to a biohashed fingerprint, combining salting with keybinding methods [71]. Nandakumar, et al. [64] proposed hardening a fingerprint-based fuzzy vault with a user-specific password, combined key binding with salting approach.

The last category is homomorphic encryption. This technique allows calculations on encrypted data. It combines homomorphic encryption with fingerprint recognition system [72]. Rane, et al. [65] presented Hamming distance calculation for their FTP scheme. Exploiting cryptosystems, Barni, et al. [56] revealed a distributed biometric system, homomorphic encryption on FT in a semi-honest model.

The detail information about the all studies categorized into these four groups is shown in Table 2.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Summary of the types of FTP schemes

Authors	FTP categories	Dataset	Key findings
Jin, et al. [4]	Non-Invertible Transform	FVC2002 DB1, DB2 and FVC2004 DB1, DB2	The stage techniques used in this scheme can prove the nature of diversity, revocability, and performance, but have the disadvantage of the Equal Error Rate (EER) evaluation in the token scenarios that reach 15%.
Yang, et al. [5]	Non-Invertible Transform	FVC2002DB2	This scheme achieves self-geometric alignment in the local minutiae area and imparts randomness around minutia to achieve diversification and encryption effects. This scheme also has a high security and compact template size.
Yang, et al. [6]	Hybrid Technique	multi-sensor fingerprint database with 71,994 samples	This scheme provides a multi-biometric template protection system employing decision level fusion of multiple protected fingerprint templates.
Pradheeba and Subban [7]	Review paper		This paper reviewed the pitfalls in the existing FTP algorithms and suggested for research development in hybrid methodologies to achieve better results.
Krivokuca [8]	Non-Invertible Transform	fingerprint database was constructed using fingerprints provided 100 volunteers	This work proposed a single N-node pattern constructed using a small subset of N minutiae from the corresponding minutiae template. The scheme fulfilled the FTP properties that are non-invertibility, cancellability, diversity, and performance
Choi, et al. [9]	Fuzzy Vault	DB1 of FVC2002	The study employed One Time Fuzzy Vault (OTFV) and add chaff minutiae to improve fingerprint fuzzy vault security and prevent correlation attack. The security level of this scheme increases 10^{34} times as compared to the counterpart.
Krivokuca and Abdulla [10]	Non-Invertible Transform	Fingerprint database was constructed using fingerprints provided 100 volunteers	The research produced a new fingerprint construction, based on the presentation of fingerprints with a compact minutiae pattern, meeting the cancellation and diversity characteristics of the ideal FTP scheme.
Stanko and Scoric [11]	Non-Invertible Transform	Verifinger database and the MCYT database	This scheme has the advantage that it does not discard the phase information of the spectral functions, then the speed also improved and the EER is comparable to that of the original spectral minutiae representation.
N. Poonguzhali and M. Ezhilarasan [12]	Hybrid Technique	FVC2002 DB_1A, DB_2A and DB_3A	This scheme provides FT protection and also enables template discriminability.
Tams, et al. [13]	Fuzzy Vault	FVC 2002 DB1	This scheme improved fuzzy vault scheme for three fusions of alignment-free fingerprint feature types.
Jin Zhe [14]	Non-Invertible Transform	FVC2002 DB1, DB2 and FVC2004 DB1, DB2	This scheme implemented the cancellable biometrics and biometric encryption to transform fingerprint data into irreversibly transformed FT. The scheme resolved FT reissue problem.
Kumar, et al. [15]	Hybrid Technique	PSNR and NC	The scheme employed watermarking techniques for FT using Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD). The scheme is imperceptible, more secure, and robust.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Nazmul, Islam, and Chowdhury, [16]	Non-Invertible Transform	FVC2002 DB1-B	This scheme proposed an alignment-free FTP which extracts the rotation and translation invariant features from the neighbouring region of each minutia and then exploits the neighbourhood information to achieve the non-invertible property.
Tuyls, et al. [17]	Fuzzy Commitment	FVC2000	This scheme applied Gabor filtering to make a fixed length FT, then converted the FT to binary used quantize scheme. Finally, error correction coding is applied to the binary representation. The scheme achieved an EER of approximately 4.2% .
Jain, et al. [18]	Review paper		The study reviewed three basic theoretical frameworks for FTP that are encryption, template transformation, and biometric cryptosystems and addressed the practical problems involved in applying these techniques to secure FT.
Fernandez [19]	Review Paper		The analysed the types of attacks on FT to obtain the original FT and the security provided for the fuzzy vault and non-invertible template protection model.
Ashish and Sinha [20]	Hybrid Technique	FVC2004DB1	The study proposed an FTP method using the Gabor filter processing approach and the orientation estimation algorithm in finding the ridge tip and bifurcation estimation.
Takahashi [21]	Non-Invertible Transform	Veridicom 5th Sense	This scheme focuses on the revocability properties; the algorithm used to overcome this issue is correlation-invariant random filtering (CIRF) and chip matching algorithm.
Maltoni, et al. [22]	Handbook of Fingerprint Recognition		The book provides general information for FTP and evaluation metrics.
Uludag and Jain [23]	Fuzzy Vault	DB2 database of FVC 2002	This scheme has the advantage of tolerant to intra-user variations. However, it has low matching accuracy.
Moon, et al. [24]	Fuzzy Vault	The dataset was collected from 400 individuals by using the optical fingerprint sensor	This scheme modifies the fuzzy vault to protect fingerprint templates and to perform fingerprint verification with the protected template at the same time.
Teoh and Ngo [25]	Salting	FVC 2002 (Set A), DB1 and DB2	This scheme excels in the false accept rate (FAR) measure context, but the template is no longer secure if the user key is compromised.
Ratha, et al. [26]	Non-Invertible Transform	IBM-99 optical database	This study proposed feature-level cancellable biometric construction by comparing the performance of Cartesian, polar, and surface folding transformations of the minutiae positions. It achieved revocability and prevented cross-matching of biometric databases.
Nagar, et al. [27]	Fuzzy Vault	FVC2002 DB2	The study proposed a fuzzy commitment scheme that encrypts FT using minutiae descriptors which capture orientation and ridge frequency information in a minutia's neighbourhood. In overall, it improved FT security and matching accuracy.
Teoh and Kim [28]	Fuzzy Commitment	FVC2002 DB1	Based on the false rejection rate (FRR) evaluation, this scheme indicated that only 9 out of 1000 correct Id are failed to be generated, and the recovery success rate is up to 99.10%.
Kholmatov and	Fuzzy Vault	Database of 400 fuzzy	This scheme unlocked 59% of the vaults

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Yanikoglu [29]		vaults	created using different impressions of the same fingerprint.
Boult, et al. [30]	Hybrid Method	FVC2000, 2002 and 2004, DB1 and DB2	This scheme provided privacy and security and improve the accuracy of the underlying biometrics.
Chikkerur, et al. [31]	Non-Invertible Transform	Database of 188 fingerprint images acquired from an optical sensor	This scheme provided a viable solution to address the privacy and security concerns around biometric authentication.
Yang, et al. [32]	Non-Invertible Transform	FVC 2002	This scheme achieved revocability and security properties.
Nandakumar [33]	Fuzzy Commitment	FVC2002-DB1 and DB2	This scheme provided high fingerprint matching accuracy.
Lee and Kim [34]	Non-Invertible Transform	FVC2004 database	This study proposed a method to produce bit-strings by mapping minutiae into a predefined 3D array using the coordinates of each minutia.
Liu, et al. [35]	Key Generating	FVC2002 DB1 and DB2	This scheme changed features of fingerprint into the features that can be handled by some known secure sketch construction.
Nagar, et al. [36]	Hybrid Method	FVC2002 DB2	The performance and security matching of the fingerprint fuzzy vault can be enhanced by combining minutiae descriptors.
Zhou, et al. [37]	Fuzzy Vault	NIST SD 14 database	The proposed scheme reduced false match rate (FMR) and significantly improved resistance against polynomial reconstruction attacks.
Zhe and Jin [38]	Non-Invertible Transform	FVC2002 DB2	This scheme achieved performance accuracy, revocation and template irreversibility.
Ahmad, et al. [39]	Non-Invertible Transform	FVC2002DB1, FVC2002DB2 and FVC2002DB3	This scheme met the requirements for FTP. On the other hand, performance degradation happenned in the case of very low transformation.
Wang and Hu [40]	Non-Invertible Transform	FVC2002 DB1, DB2 and DB3	This scheme provided FT security because the transformation and stored templates remain, and the raw FT cannot be recovered. But cancellable properties have not been reached.
Das, et al. [41]	Non-Invertible Transform	FVC2002-DB1a and FVC2002-DB2a	This scheme captured the minutia positional variations across users. However, fingerprint hash generation and matching processes were relatively low.
Ferrara, et al. [42]	Non-Invertible Transform	FVC2002 datasets and on FVC2006 DB2	This scheme proposed a reverse Minutia Cylinder-Code (MCC) that is recovering original minutiae positions and angles. It provided acceptable accuracy, protection for minutiae information, and robust against masquerade attacks.
Li, et al. [43]	Fuzzy Commitment	FX3000 database, FVC2002 DB1, FVC2002 DB2	This scheme used binary length-fixed feature generation method of fingerprint for fuzzy commitment. The scheme outperformed most of the existing scheme in terms of ZeroFAR and security strength.
Imamverdiyev, et al. [44]	Fuzzy Commitment	FVC2000 DB2a	This approach experienced a significant degradation in accuracy and computationally difficult to retrieve the original cryptographic key or template.
Ranjan and Singh [45]	Key Generating	Key generation management	This scheme applied the divide-and-conquer method of biometric authentication. It had high security and addressed the problem of biometric variation of a person.
Prasad and Kumar [46]	Non-Invertible Transform	FVC 2002 DB1, DB2, and DB3	This scheme proposed alignment-free cancellable template generation. It achieved the FTP properties that are non-invertible, accuracy, diversity and revocability.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Yang, et al. [47]	Key Generating	FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 and FVC2004 DB2	This scheme employed Delaunay quadrangle-based fingerprint authentication. It achieved better recognition performance compared to authentication systems that use absolute geometric measurements in local registration.
Nguyen, et al. [48]	Fuzzy Vault	FVC2002-DB2A, FVC2004-DB3A	This scheme proposed fingerprint fuzzy vault scheme based on ridge features. It had good performance and provided FT security.
Bansal, et al. [49]	Fuzzy Vault	FVC2002-DB1_B	This scheme used Hadamard transformation to achieve revocability, diversity, and security.
Li and Hu [50]	Fuzzy Vault	FVC 2000 (DB1), FVC 2002 (DB1, DB2, DB3, DB4), FVC 2004 (DB2) and FVC 2006 (DB2, DB3)	This scheme proposed an alignment-free fuzzy vault using highly discriminative pair-polar (P-P) minutiae structures. It provided strong security against brute force and cross-matching attacks.
Murillo-Escobar, et al. [51]	Non-Invertible Transform	This scheme verifies and justify in security aspects and its implementation in real applications embedded systems.	The scheme used chaotic encryption by combining the logistic map and Murillo-Escobar's algorithm. The scheme is secure, effective and low cost.
Sandhya and Prasad [52]	Non-Invertible Transform	FVC2002	The scheme constructed k-Nearest Neighbourhood Structure (k - NNS) for minutiae points for FT. It has a satisfactory performance in terms of EER and also in terms of d-prime and K-S test values obtained.
Wang and Hu [53]	Non-Invertible Transform	FVC2002 DB1, DB2 and DB3	This method has satisfactory performance compared to the existing alignment-free cancellable template schemes. However, the performance of cancellable templates not achieved.
Sandhya and Prasad [54]	Hybrid Method	FVC 2002 DB1, DB2, and DB3	This technique has good accuracy and strong security, then also has cancellable properties.
Jin, et al. [55]	Hybrid Method	FVC2002 and FVC2004	This scheme has good and strong accuracy against some major security and privacy attacks.
Barni, et al. [56]	Homomorphic Encryption	Public fingerprint dataset	This method has advantages in terms of data confidentiality but low accuracy.
Guo, et al. [57]	Non-Invertible Transform	FVC2002 (OBI, DB2) and FVC2004 (OBI, DB2)	This scheme achieved security, diversity, and revocability. However, this scheme still experiences stolen-token scenario.
Wong, et al. [58]	Non-Invertible Transform	FVC Datasets	This scheme achieved the non-invertible and revocable properties of the cancellable template.
Gao [59]	Non-Invertible Transform	FVC2000 DB1B, FVC2002 DB1B, FVC2004 DB1	This scheme allowed FT recognition to be performed more accurately than the original templates.
Gomez-Barrero, et al. [60]	Homomorphic Encryption	Chimeric databases	The scheme met FTP on irreversibility analysis and unlinkability.
Sadhya and Singh [61]	Salting	FVC2002 DB1, DB2, FVC2004 DB1, DB2	This scheme achieved unlinkability, cancelability and diversity requirements.
Wang, et al. [62]	Non-Invertible Transform	FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 FVC2004 DB2	This scheme reduced the risk of attack via record multiplicity (ARM). However, recognition efficiency and accuracy are still lacking.
Jin, et al. [63]	Salting	FVC2002 and FVC2004	This scheme has good accuracy and also meets the non-linkability and revocability FTP. Further research is needed for the use of this scheme in the identification setting.
Nandakumar, et al. [64]	Fuzzy Vault	FVC2002-DB2 and MSU-DBI fingerprint databases	The scheme increased the entropy, improved the vault security; and enhanced user privacy.
Rane, et al. [65]	Homomorphic	a proprietary database of	The scheme used Hamming distance,

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	Encryption	1035 fingers	Euclidean distance, and homomorphic encryption to enable the two parties to compute the distortion in encrypted form without revealing their inputs to each other.

Based on Table 2, template transformation was the most frequent type of FTP schemes studied by the researchers. It is followed by fingerprint cryptosystem, a hybrid method, and homomorphic encryption. The bar chart in Figure 6 shows the number of documents based on the types of FTP scheme.

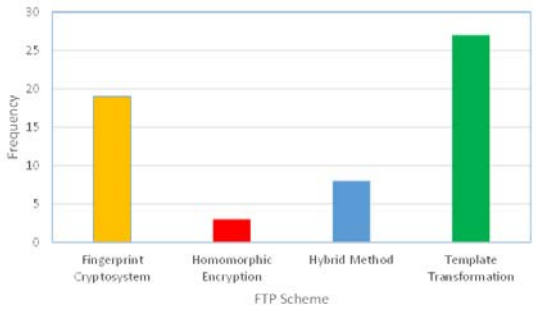

Figure 6: FTP schemes frequency using by researchers

3.2 What are the metrics used for evaluating the FTP schemes?

The FTP schemes can be measured using the following evaluation metric [68]:

1. Security: Computationally, it must be difficult to obtain the original FT from the secure FT.
2. Revocability: The scheme must be able to revoke the compromised FT from the same fingerprint data.
3. Diversity: To ensure user privacy, the secured FT must not be cross-matched.
4. Performance: The scheme should not degrade the accuracy of the recognition system.

Security is measured in terms of information leakage levels or computational complexity which is involved in the recovery of original templates from safe sketches or transformed templates [73, 74]. There are three approaches to evaluate the security property. The first approach involves quantifying security evaluation by estimating the number of guesses needed to recover the original FT from the protected FT via brute force [26, 75]. The second approach involves providing proof by showing that the forward mapping is many-to-one and thus that the reverse mapping is one-to-many [4, 76, 77]. The third approach for evaluating the security property of FTP schemes involves computing the percentage of the original FT which remains unrecoverable when the protected FT is compromised.

In revocability measures, if the stored FT is compromised, it should be possible to cancel that FT and reissue a new one. Furthermore, the newly issued FT should not match with the previously compromised FT. There are two general approaches to the revocability analysis of FTP schemes. The first approach, which has become less common with the progress of this field of research, involves simply stating that the FT may be canceled because of the possibility of altering irreversible transformation or a set of external parameters used on protected generation templates. The second approach involves evaluating a revocable method by generating multiple protected templates from unprotected templates and then trying to match them. If the probability of matching is low (e.g., approximately equal to the probability of matching two protected templates derived from unprotected templates), it serves as evidence that the FTP scheme is effectively able to establish a different identity from the same fingerprint; Therefore, it is concluded that the FTP scheme can be canceled.

In the evaluation of diversity, it should be possible to issue different FT for different applications related to the same user. The FT should not match with each other and should make cross-matching impossible. It prevents tracking of the templates. Because of their similarity with the nature of the cancellation, it is generally considered to be synonymous with decline. As a result, a similar analysis is performed to prove that the FTP scheme meets the cancellation and diversity requirements. If the probability of two protected FT from the same fingerprint matches is very low, the appropriate FTP scheme is considered to meet the requirements of diversity and cancellation. Evaluating the diversity of FTP schemes should adopt a more stringent definition of diversity, stating that two protected FT from the same fingerprint can only be considered truly diverse if they cannot be fully resolved. This is where disconnection is considered at the level deeper than implied by direct matching.

Performance is usually measured through the matching process with specific metrics called False Accept Rate (FAR) and Genuine Accept Rate (GAR). Because of the intra-user variability in fingerprint images; in general, there is a trade-off between FAR/GAR and security in most template

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

protection schemes. Lower security schemes tend to have higher FAR/GARs and vice versa. In addition, there is also evaluation of matching performance using equal error rate (EER). The EER indicates that the proportion of false acceptances is equal to that of false rejections [78]. The lower EER means, the higher accuracy of the scheme.

Analysis of the FTP scheme in Table 2 revealed that FAR/FMR is the most widely used evaluation metric followed by FRR, GAR, and EER. Table 3 lists the studies and the evaluation metric applied to the FTP schemes.

Table 3: Metrics for evaluating FTP schemes

Metrics	**Sources/Studies**
Security	[5, 8, 16, 17, 21, 33, 35, 36, 38, 40, 41, 46-48, 50, 52-55, 63]
Revocability	[4, 8, 10, 21, 26, 34, 38-41, 46, 50, 52-55, 59-61, 63]
Diversity	[4, 8, 10, 21, 29, 38, 39, 50, 52, 60, 61]
False Accept Rate (FAR)/ False Match Rate (FMR)	[4, 6, 8, 9, 12, 13, 16, 17, 21, 23, 27, 32, 34-37, 40-44, 46-48, 50, 52, 53, 55-57, 59, 64]
Genuine Accept Rate (GAR)	[9, 12, 13, 16, 23, 27, 31, 35, 36, 41, 44, 48, 49, 53, 55, 64]
Equal Error Rate (EER)	[4, 5, 8, 16, 17, 25, 30, 32, 38-41, 44, 46, 47, 50, 52-54, 56, 57, 60, 61, 63]
False Rejection Rate (FRR)/ False Non Matching Rate (FNMR)	[6, 8, 12, 16, 17, 21, 28, 32, 37, 40, 42, 43, 46, 47, 50, 52, 55, 57]

3.3 What are the common datasets used for evaluating the FTP schemes?

The FTP schemes were evaluated using standard datasets that are made available by researchers. The majority of the dataset was taken from the Fingerprint Verification Competition (FVC); a series of competition that aims to establish a benchmark for improving fingerprint recognition systems [79-82]. Apart from the FVC datasets, researchers also created their own fingerprint database for evaluating the FTP schemes. There are also other fingerprint databases that include NIST SD 14, and IBM-99. Table 4 shows the description of the dataset and the studies that utilized them respectively.

Table 4: List of fingerprint dataset used in FTP schemes

Fingerprint database	Description of the dataset	Sources/ Studies
FVC2000	This fingerprint database was developed for Fingerprint Verification Competition 2000 (website: http://bias.csr.unibo.it/fvc2000/ #). It consists of four different databases; DB1, DB2, DB3, and DB4 which the fingerprints were captured using the low-cost optical sensor, low-cost capacitive sensor, an optical sensor, and synthetic generator respectively.	[17, 30, 44, 50, 59]
FVC2002	This fingerprint database was developed for Fingerprint Verification Competition 2002 (website: http://bias.csr.unibo.it/fvc2002/ #). It consists of four different databases; DB1, DB2, DB3 and DB4 which the fingerprints were captured using optical sensor, capacitive sensor, and SFinGe v2.51 sensor respectively.	[4, 5, 8, 9, 12, 13, 16, 21, 23, 25, 27, 28, 30, 32, 33, 35, 36, 38-42, 46-50, 52-55, 57-59, 61, 63, 64]
FVC2004	This fingerprint database was developed for Fingerprint Verification Competition 2004 (website: http://bias.csr.unibo.it/fvc2004/ #). It consists of four different databases; DB1, DB2, DB3, and DB4 which the fingerprints were captured using an optical sensor, thermal sweeping sensor, and SFinGe v3.0 sensor respectively.	[4, 30, 34, 48, 50, 55, 57-59, 61, 63]
FVC2006	This fingerprint database was developed for Fingerprint Verification Competition 2006 (website: http://http://bias.csr.unibo.it/fvc 2006/#). It consists of four different databases; DB1, DB2, DB3, and DB4 which the fingerprints were captured using electric field sensor, an optical sensor, thermal sweeping sensor, and SFinGe v3.0 sensor respectively.	[50]
Database of 400 fingerprint impressions	This fingerprint database consists of 400 fingerprint images (2 different impressions for each of 200 different fingers) acquired with an optical sensor and with manually labelled minutiae points	[29]
Database of 188 fingerprint images acquired from an optical sensor.	The fingerprints were captured using an optical sensor.	[48]
NIST SD 14 database	This fingerprint database was developed by FBI. The complete database consists of	[37]

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

	27,000 pairs of fingerprints (https://www.fbibiospecs.cjis.gov/).	
IBM-99 optical database	This database consists of 188 fingerprint pairs, after rejecting poor quality fingerprints.	[83]
dataset Cross Match Verifier 300	This fingerprint database is obtained from crossMatch Verifier 300 sensor. The dataset contains 8 images for each individual. The owner is neurotechnology.	[84]
GUC100 Database	The GUC100 fingerprint database contains fingerprint samples collected in Norway in the winter-spring season of 2008 for TURBINE project.	[6]
Veringer database and the MCYT database	The Verifnger database contains fingerprints from six individual persons, ten fingers per individual, eight images per finger. The MCYT database contains fingerprints from 100 individuals, 10 fingers per individual, 12 images per finger.	[11, 13]
Veridicom 5th Sense	This dataset consists of 181 pairs of fingerprint images captured through a capacitive sensor	[21]

Based on the list in Table 4, it can be concluded that FVC2002, FVC2004 and FVC2000 are the top three frequently used datasets. The major reason leads to the selection of the database could be due to their availability. These databases were developed for FVC competition where experts from industry and academics participated in the competition. Only a study used FVC2006 dataset. Other databases such as NIST SD, IBM-99, verifier300, GUC100, verifinger, MYCT and veridicom 5t sense database were infrequently used. On the other hand, researchers constructed their own fingerprint dataset. Figure 7 summarizes the usage of fingerprint datasets.

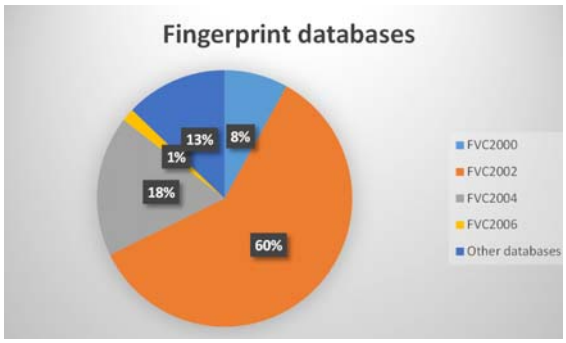

Figure 7: The fingerprint dataset usage

5. CONCLUSION

This paper reviewed studies pertaining FTP schemes published between the year of 2000 and 2017. 62 studies were collected and analysed in terms of the types of the FTP scheme, the metric used for evaluation of the schemes and the dataset used for the evaluation. The literature review presented in this paper can be a source of reference for researchers in the area and could lead the researchers to focus their work on a particular area of the FTP schemes for a specialized study.

The rapid growth of the Internet technology has expanded the use of fingerprint into a larger application boundary. For example, the fingerprint is a common authentication method for mobile applications nowadays. With the features of smartphones and wireless connection, FTP schemes definitely need to be designed to suit the mobility features and the smartphones limited resources. Further, the evolve of the Internet of Things (IoT) has also been a reason that requires FTP schemes to be designed in such a way that they achieve the four desired properties; security, revocability, diversity, and performance. Hence, there is a great opportunity to work and study FTP schemes for the emerging ICT particularly the mobile application and IoT.

REFERENCES:

[1] V. Jain, "Information Technology Issues & Challenges," *Pioneer Institute of Professional Studies, Indore,* 2009.

[2] D. Dasgupta, A. Roy, and A. Nag, "Advances in User Authentication," Springer2017.

[3] M. Sandhya and M. V. Prasad, "Biometric Template Protection: A Systematic Literature Review of Approaches and Modalities," in *Biometric Security and Privacy*, ed: Springer, 2017, pp. 323-370.

[4] Z. Jin, A. B. J. Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving," *Expert systems with applications,* vol. 39, pp. 6157-6167, 2012.

[5] B. Yang, C. Busch, P. Bours, and D. Gafurov, "Robust minutiae hash for fingerprint template protection," in *Media Forensics and Security II*, 2010, p. 75410R.

[6] B. Yang, C. Busch, K. De Groot, H. Xu, and R. N. Veldhuis, "Performance evaluation of fusing protected fingerprint minutiae templates on the decision level," *Sensors,* vol. 12, pp. 5246-5272, 2012.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] R. Subban, "Fingerprint template protection techniques—A survey and analysis," in *Computational Intelligence and Computing Research (ICCIC), 2014 IEEE International Conference on*, 2014, pp. 1-6.

[8] V. Krivokuca, "Fingerprint Template Protection using Compact Minutiae Patterns," ResearchSpace@ Auckland, 2015.

[9] W. Y. Choi, Y. Chung, J.-W. Park, and D. Hong, "Fingerprint Template Protection Using One-Time Fuzzy Vault," *KSII Transactions on Internet & Information Systems,* vol. 5, 2011.

[10] V. Krivokuća and W. Abdulla, "Cancellability and diversity analysis of fingerprint template protection scheme based on compact minutiae pattern," *Information Security Journal: A Global Perspective,* vol. 25, pp. 109-123, 2016.

[11] T. Stanko and B. Skoric, "Minutia-pair spectral representations for fingerprint template protection," *arXiv preprint arXiv:1703.06811,* 2017.

[12] N. Poonguzhali and M. Ezhilarasan, "A Hybrid Template Protection Technique for Fingerprint Biometric Authentication System," in *Proceedings of the International Conference on Informatics and Analytics*, 2016, p. 43.

[13] B. Tams, J. Merkle, C. Rathgeb, J. Wagner, U. Korte, and C. Busch, "Improved fuzzy vault scheme for alignment-free fingerprint features," in *Biometrics Special Interest Group (BIOSIG), 2015 International Conference of the*, 2015, pp. 1-12.

[14] Z. Jin, "Privacy Preserving Minutia-Based Fingerprint Template Protection Techiniques," UTAR, 2015.

[15] S. Kumar and A. Garg, "A Fingerprint Template Protection using Watermarking," *International Journal of Computer Applications,* vol. 149, 2016.

[16] R. Nazmul, M. R. Islam, and A. R. Chowdhury, "Alignment-Free Fingerprint Template Protection Technique Based on Minutiae Neighbourhood Information," in *International Conference on Applications and Techniques in Cyber Security and Intelligence*, 2017, pp. 256-265.

[17] P. Tuyls, A. H. Akkermans, T. A. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. Veldhuis, "Practical biometric authentication with template protection," in *International Conference on Audio-and Video-Based Biometric Person Authentication*, 2005, pp. 436-446.

[18] 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.

[19] R. S. Fernandez, "Fingerprint template protection scheme, security and vulnerabilities: A survey," presented at the 3rd International Conference & Exhibition on Biometrics & Biostatistics
Hilton Baltimore - BWI Airport, USA, 2011.

[20] M. Ashish and G. Sinha, "Biometric Template Protection," *J Biostat Biometric App,* vol. 1, p. 202, 2016.

[21] 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.

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

[23] U. Uludag and A. Jain, "Securing fingerprint template: Fuzzy vault with helper data," in *Computer Vision and Pattern Recognition Workshop, 2006. CVPRW'06. Conference on*, 2006, pp. 163-163.

[24] D. Moon, S. Lee, S. Jung, Y. Chung, M. Park, and O. Yi, "Fingerprint template protection using fuzzy vault," in *International Conference on Computational Science and Its Applications*, 2007, pp. 1141-1151.

[25] 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.

[26] 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.

[27] A. Nagar, K. Nandakumar, and A. K. Jain, "Securing fingerprint template: Fuzzy vault with minutiae descriptors," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, 2008, pp. 1-4.

[28] A. B. J. Teoh and J. Kim, "Secure biometric template protection in fuzzy commitment scheme," *IEICE Electronics Express,* vol. 4, pp. 724-730, 2007.

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

[30] T. E. Boult, W. J. Scheirer, and R. Woodworth, "Revocable fingerprint biotokens: Accuracy

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

and security analysis," in *Computer Vision and Pattern Recognition, 2007. CVPR'07. IEEE Conference on*, 2007, pp. 1-8.

[31] S. Chikkerur, N. K. Ratha, J. H. Connell, and R. M. Bolle, "Generating registration-free cancelable fingerprint templates," in *Biometrics: Theory, Applications and Systems, 2008. BTAS 2008. 2nd IEEE International Conference on*, 2008, pp. 1-6.

[32] 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.

[33] K. Nandakumar, "A fingerprint cryptosystem based on minutiae phase spectrum," in *Information Forensics and Security (WIFS), 2010 IEEE International Workshop on*, 2010, pp. 1-6.

[34] 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.

[35] E. Liu, J. Liang, L. Pang, M. Xie, and J. Tian, "Minutiae and modified biocode fusion for fingerprint-based key generation," *Journal of Network and Computer Applications,* vol. 33, pp. 221-235, 2010.

[36] 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.

[37] X. Zhou, A. Opel, J. Merkle, U. Korte, and C. Busch, "Enhanced template protection with passwords for fingerprint recognition," in *Security and Communication Networks (IWSCN), 2011 Third International Workshop on*, 2011, pp. 67-74.

[38] 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.

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

[40] 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.

[41] 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.

[42] 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.

[43] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Systems with Applications,* vol. 39, pp. 6562-6574, 2012.

[44] Y. Imamverdiyev, A. B. J. Teoh, and J. Kim, "Biometric cryptosystem based on discretized fingerprint texture descriptors," *Expert Systems with Applications,* vol. 40, pp. 1888-1901, 2013.

[45] 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.

[46] M. V. Prasad and C. S. Kumar, "Fingerprint template protection using multiline neighboring relation," *Expert Systems with Applications,* vol. 41, pp. 6114-6122, 2014.

[47] 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.

[48] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints," *IET Biometrics,* vol. 4, pp. 29-39, 2015.

[49] D. Bansal, S. Sofat, and M. Kaur, "Fingerprint fuzzy vault using hadamard transformation," in *Advances in Computing, Communications and Informatics (ICACCI), 2015 International Conference on*, 2015, pp. 1830-1834.

[50] C. Li and J. Hu, "A security-enhanced alignment-free fuzzy vault-based fingerprint cryptosystem using pair-polar minutiae structures," *IEEE Transactions on Information Forensics and Security,* vol. 11, pp. 543-555, 2016.

[51] M. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, and R. López-Gutiérrez, "A robust embedded biometric authentication system based on fingerprint and chaotic encryption," *Expert Systems with Applications,* vol. 42, pp. 8198-8211, 2015.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[52] M. Sandhya and M. V. Prasad, "k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection," in *Biometrics (ICB), 2015 International Conference on*, 2015, pp. 386-393.

[53] S. Wang and J. Hu, "A blind system identification approach to cancelable fingerprint templates," *Pattern Recognition,* vol. 54, pp. 14-22, 2016.

[54] 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.

[55] 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.

[56] 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.

[57] L. Guo, Y. Mao, and Y. Guo, "Non-invertible fingerprint template protection with polar transformations," in *2016 14th Annual Conference on Privacy, Security and Trust (PST)*, 2016, pp. 730-735.

[58] W. J. Wong, A. B. Teoh, Y. H. Kho, and M. D. Wong, "Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template," *Pattern Recognition,* vol. 51, pp. 197-208, 2016.

[59] Q. Gao, "Toward Constructing Cancellable Templates using K-Nearest Neighbour Method," 2017.

[60] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognition,* vol. 67, pp. 149-163, 2017.

[61] D. Sadhya and S. K. Singh, "Design of a cancelable biometric template protection scheme for fingerprints based on cryptographic hash functions," *Multimedia Tools and Applications,* pp. 1-25, 2017.

[62] S. Wang, W. Yang, and J. Hu, "Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs," *Pattern Recognition,* vol. 66, pp. 295-301, 2017.

[63] Z. Jin, Y.-L. Lai, J.-Y. Hwang, S. Kim, and A. B. J. Teoh, "A New and Practical Design of Cancellable Biometrics: Index-of-Max Hashing," *arXiv preprint arXiv:1703.05455,* 2017.

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

[65] 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.

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

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

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

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

[70] 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.

[71] T. S. Ong, A. T. B. Jin, and D. C. L. Ngo, "Application-Specific Key Release Scheme from Biometrics," *IJ Network Security,* vol. 6, pp. 127-133, 2008.

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

[73] T. Ignatenko and F. M. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Transactions on Information Forensics and Security,* vol. 4, pp. 956-973, 2009.

[74] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security tradeoffs in reusable biometric security systems," in *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on*, 2010, pp. 1722-1725.

[75] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

circular convolution," *Pattern Recognition,* vol. 47, pp. 1321-1329, 2014.

[76] D. Moon, J. H. Yoo, and M. K. Lee, "Improved cancelable fingerprint templates using minutiae-based functional transform," *Security and Communication Networks,* vol. 7, pp. 1543-1551, 2014.

[77] W.-j. Wong, M.-l. D. Wong, and Y.-h. Kho, "Multi-line code: A low complexity revocable fingerprint template for cancelable biometrics," *Journal of Central South University,* vol. 20, pp. 1292-1297, 2013.

[78] C. Rathgeb, A. Uhl, and P. Wild, *Iris biometrics: from segmentation to template security* vol. 59: Springer Science & Business Media, 2012.

[79] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2000: Fingerprint verification competition," *IEEE Transactions on Pattern Analysis and Machine Intelligence,* vol. 24, pp. 402-412, 2002.

[80] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2002: Second fingerprint verification competition," in *Pattern recognition, 2002. Proceedings. 16th international conference on*, 2002, pp. 811-814.

[81] D. Maio, D. Maltoni, R. Cappelli, J. L. Wayman, and A. K. Jain, "FVC2004: Third fingerprint verification competition," in *Biometric Authentication*, ed: Springer, 2004, pp. 1-7.

[82] R. Cappelli, M. Ferrara, A. Franco, and D. Maltoni, "Fingerprint verification competition 2006," *Biometric Technology Today,* vol. 15, pp. 7-9, 2007.

[83] Y. Chung, D. Moon, S. Lee, S. Jung, T. Kim, and D. Ahn, "Automatic alignment of fingerprint features for fuzzy fingerprint vault," in *CISC*, 2005, pp. 358-369.

[84] U. Uludag and A. K. Jain, "Fuzzy fingerprint vault," in *Proc. Workshop: Biometrics: Challenges arising from theory to practice*, 2004, pp. 13-16.