# FINGERPRINT TEMPLATE PROTECTION SCHEMES: A LITERATURE REVIEW

*by* Apri Siswanto

**Submission date:** 11-Oct-2017 01:51PM (UTC+0700)
**Submission ID:** 860846201
**File name:** BIOMETRIC_FINGERPRINT_TEMPLATE_PROTECTION_ALGORITHM_A_SURVEY.doc (615K)
**Word count:** 6979
**Character count:** 40156

# 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**

This paper aims to provide an organized literature on fingerprint template protection (FTP). In this paper, surveys have been conducted on the types of FTP development schemes, the explanation of the fingerprint recognition systems (FRS), the threat model and prevention of FRS and the performance metrics often used by researchers in evaluating the performance of FTP schemes. The latest information and references are analysed and classified based on FTP methods and publication year to obtain information related in the development and application of FTP. This survey contains 86 references related to FTP that have been developed and used by researchers in an effort to protect fingerprint templates. The reference list includes related research work from 2000 to 2017. Ultimately, this can be a source of reference for other researchers in finding literature relevant to the FTP development research area.

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

## 1. INTRODUCTION

Biometric technology is used widely as an aunthentication 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 so that the risk of impersonation is very low. Further, authentication using biometric technology does not require users to remember the password or or carry such tokens (e.g., smart card, keys, etc.). 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 twins. 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 system is 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 through 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 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 researchers with state-of the-

art of 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 work on?
RQ2: What are the performance measures 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 where the FTP methods are listed and analysed. Finally, Section 4 discusses the limitation of the study and concludes the finding.

## 2. METHOD

In order to get the extraction results, research implications, and future research directions on the FTP field, a comprehensive article search is done on this complex topic, while the main keyword used for the search is fingerprint template protection. In addition, there are several keyword aides such as cancelable fingerprint, transformation template, feature transformation, biometric crypto system, fingerprint cryptosytem, Fingerprint cryptography, and homomorphic encryption. The search for articles in English, published between January 2000 and December 2017, was conducted using the IEEE Xplore Digital Library, ACM Digital Library, Science Direct, Springerlink, Google Scholar and Hindawi Publising Corporation.

In the initial stage, the search is done with the main keyword is fingerprint template protection. At this stage of the 3600 articles that index by search engine google, found as many as 20 relevant articles. From these 20 articles, comprises 2 e book, two PhD Thesis, 11 journals and five paper conference. At this stage, summarizes information about regarding techniques, methods or schemes used to develop fingerprint template protection in the enrollment and authentication process. It then summarized also the evaluation methods and data set used by researchers based on the method or scheme they proposed.

In the second, phase is a search with supporting keywords such as cancelable fingerprint, transformation template, feature transformation, biometric cryptosystem, fingerprint cryptosytem, fingerprint cryptography, and homomorphic encryption. At this stage of the tens of thousands of articles indexed from google search engines, selected 42 articles that describe the methods or techniques used by researchers to develop fingerprint template protection. The selection of 42 articles is based on a reading of the abstract and conclusion of the paper. Of the 42 articles, 26 are articles in journals and 16 paper conferences. In this, second stage is summarizing the findings obtained by researchers based on the scheme they proposed.

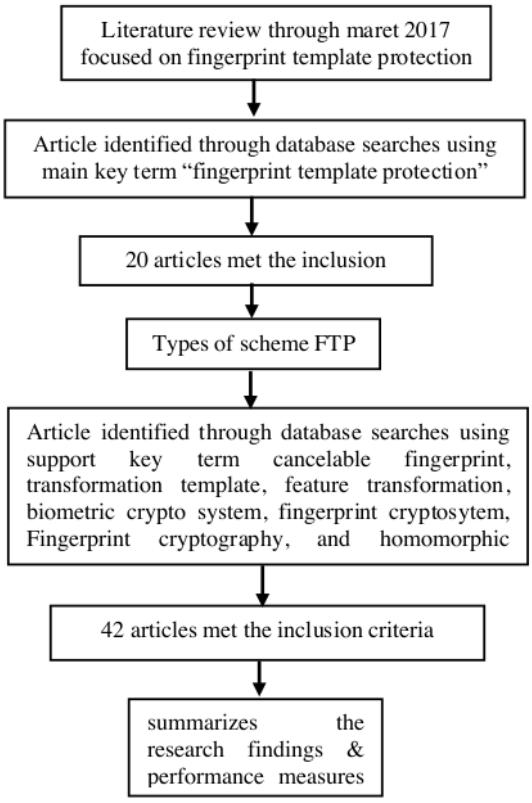


*Figure 1: The literature review process*

## 3. RESULTS

### 3.1 What are the types of FTP schemes that researchers work on?

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

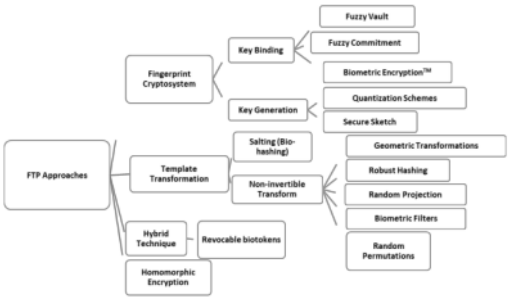


*Figure 2: Categorization of FTP schemes*

In the fingerprint cryptosystems (FC), helper data is used to describe additional information of FTstored in the database [4]. 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. Fingerprint cryptosystems provide high security. However, they do not provide diversity and revocability. Based on how the helper data derived, the fingerprint cryptosystem are cat[5]egorized into key binding and key generation system [6].

Some of the most popular schemes in the key binding category are the Biometric Encrytion proposed by soetar [7]. Then the fuzzy vaul scheme was first introduced by Juels and sudan [8]. Other researchers who developed the fuzzy vault scheme can be viewed more in detail at [9-25]. And the last fuzzy commitment made by juels and Waterberg [26]. The researcher developing on this scheme are [27-30]. 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 FC [31]. Some work in this field can be viewed in more detail in the article [32-35].

In 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-ivertible* transforms are the two most popular schemes in feature transformation approaches. Key secrecy or keywords are the basis of *salting* scheme security. Meanwhile, the security of non-invertible transformation techniques employs one way of computing functions which is difficult to reverse, even with a known key. However, the main disadvantage of this technique is the security of the system that is hard to verify. It is for this reason that no mathematical foundation is used to perform robust security analysis. Furthermore, it is assumed that the distribution of uniform fingerprint features [36] and enemies may be able to exploit the non-uniform features of fingerprint features to launch attacks that may require far less effort to compromise system security. Schematically, the authentication process in a FTP based on feature transformation is depicted in Figure 3.


*Figure 3: The authentication process in a fingerprint recognition system employing feature transformation [6]*

Salting is a FTP approach 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. [6].

The salting approach has a particular limitation in that the security depends on the secrecy of the password or key [37, 38]. 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. Research related to salting can be een in the article [39-45].

Meanwhile, in non-invertible transform approach, a one-way function non-invertible transform applying to secure the biometric template. The intruder cannot reconstruct the original fingerprint template 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 on 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 [6, 31]. 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 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. There is a trade-off between discriminability and non-invertibility, because it is a challenge to design transform functions which simultaneously satisfy both requirements.

The most influential researchers with regard to this scheme are Ratha, et al. [46]. They analyzed cancelable fingerprint biometric using non-invertible transforms for producing cancelable fingerprint templates. This can change the raw templates of fingerprint by using either feature or signal domain transformations. The three transformation functions include Cartesian transformation, polar transformation, and functional transformation. Figure 4 shows the proposed scheme of ratha. Research employing the same technique was conducted by [47-63].

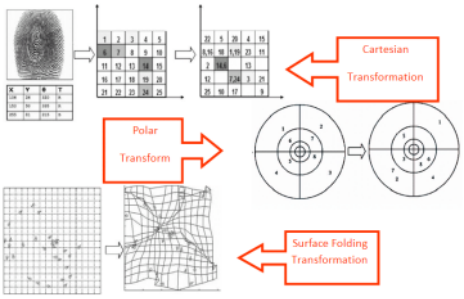


*Figure 4: Ratha Schemes using Cartesian, polar and functional transformation*

Then on hybrid methods, that technique can be designed with the combination of feature transformation and fingerprint cryptosystems. The examples of some hybrid systems are presented in the literature. Some of the systems incorporate the functions of traditional cryptographic hashing into the hybrid protection system, such as An application-specific key releases scheme that retrieves a cryptographic key bound to a biohashed fingerprint, combining salting with key binding methods [64]. Then, Nandakumar, et al. [65] proposed hardening a fingerprint-based fuzzy vault with a user-specific password, combined key binding with salting approach. In addition, several researches that have been done in FTP based on hybrid scheme are present in the article [66-69]

The latter is homomorphic encryption. This technique allows calculations on encrypted data. The techniques have the advantage of meeting the requirements of FTP without degrading its accuracy. The way is to combine homomorphic encryption with fingerprint recognition system [70]. The studies FTP under homomorphic encryption schemes was developed in Rane, et al. [71] study. For secure fingerprint applications, they presented Hamming distance calculation. Exploiting cryptosystems, Barni, et al. [72] revealed a distributed biometric system, homomorphic encryption on fingercode templates in a semi-honest model.

The summary of the FTP categories are summarized in Table 1.

*Table 1: Summary of key articles on FTP schemes.*

| Authors | FTP Approaches | Dataset | Key findings |
|---|---|---|---|
| Uludag and Jain [10] | Fuzzy Vault | DB2 database of FVC 2002 | This scheme has the advantage of tolerant to intra-user variations. on the other hand, this scheme is low matching accuracy. |
| Teoh and Ngo [39] | Salting | FVC 2002 (Set A), DB1 and DB2 | This scheme excels in the FAR measure context, but the template is no longer secure if the user key is compromised. |
| Ratha, et al. [73] | Non Invertible Transform | IBM-99 optical database | This scheme can be applied without much loss of performance in the feature domain. |
| Nandakumar, et al. [65] | Fuzzy Vault | FVC2002-DB2 and MSU-DBI fingerprint databases | Scheme for hardening a fingerprint minutiae-based fuzzy vault using password can increase the entropy thereby improving the vault security; also enhances user privacy. The disadvantage is not user-friendly; user needs to provide both the password and the biometric during authentication. |
| Nagar, et al. [13] | Fuzzy Vault | FVC2002 DB2 | The security and matching accuracy of the fuzzy vault more better than the other technique. No diversity and revocability properties. |
| Teoh and Kim [27] | Fuzzy Commitment | FVC2002 DB1 | Based on the EER evaluation, this scheme indicates 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 Yanikoglu [20] | Fuzzy Vault | Database of 400 fuzzy vaults | In this work the fuzzy vault scheme is implemented using a database with 400 fingerprint impressions. This scheme able to successfully unlock 59% of the vaults created using different impressions of the same fingerprint. In addition, the scheme shows that for 41% of all cases, it was possible to link an unknown vault to a small set containing the matching vault. There should be additional security measures for the system to withstand attacks. |
| Boult, et al. [66] | Hybrid Method | FVC2000,2002 and 2004 DB1 and DB2 | This scheme provides privacy and security, and improve the accuracy of the underling biometrics. |
| Chikkerur, et al. [47] | Non Invertible Transform | Database of 188 fingerprint images acquired from an optical sensor | This scheme provide a viable solution to address the privacy and security concerns around biometric authentication. |
| Yang, et al. [48] | Non Invertible Transform | FVC 2002 | Based on researchers work, this scheme achieved revocability and security properties. |
| Nandakumar [28] | Fuzzy Commitment | FVC2002-DB1 and DB2 | This scheme provide high fingerprint matching accuracy, low performance. |
| Lee and Kim [49] | Non Invertible Transform | FVC2004 database | A low-complexity method that does not require pre-alignment and the proposed method produces bit-strings by mapping minutiae into a predefined 3D array using the coordinates of each minutia. when PINs were duplicated the performance was highly secure. |
| Liu, et al. [34] | Key Generating | FVC2002 DB1 and DB2 | This scheme is able to improve the FTP performance of the system compared to a system based solely on minutiae. All features of fingerprint should be changed into the features that can be handled by some known secure sketch construction. |
| Nagar, et al. [67] | Hybrid Method | FVC2002 DB2 | The performance and security matching of the fingerprint fuzzy vault can be enhanced by combining minutiae descriptors. |
| Zhou, et al. [21] | Fuzzy Vault | NIST SD 14 database | FMR can be reduced strongly, significantly improve resistance against polynomial reconstruction attacks. Requires additional analysis and empirical evaluation. |
| Zhe and Jin [50] | Non Invertible Transform | FVC2002 DB2 | This scheme is able to provide satisfactory performance accuracy and revocation and template irreversibility. |

| | | | |
|---|---|---|---|
| Ahmad, et al. [51] | Non Invertible Transform | FVC2002DB1, FVC2002DB2 and FVC2002DB3 | This scheme meets the requirements of fingerprint protection templates. On the other hand, performance degradation caused by very low transformation. |
| Wang and Hu [53] | Non Invertible Transform | FVC2002 DB1, DB2 and DB3 | This scheme has strong security because the transformation and stored templates remain, and the raw fingerprint data cannot be recovered. But cancellable properties have been reached |
| Das, et al. [54] | Non Invertible Transform | FVC2002-DB1a and FVC2002-DB2a | This approach success in capturing the minutia positional variations across users. But fingerprint hash generation and matching processes is relatively low. |
| Ferrara, et al. [55] | Non Invertible Transform | FVC2002 datasets and on FVC2006 DB2 | This approach is excellent in terms of accuracy and is able to provide good protection minutiae information and is robust against masquerade attacks. No adding a user-specific secret key to P-MCC to achieve diversity and revocability. |
| Li, et al. [29] | Fuzzy Commitment | FX3000 database, FVC2002 DB1, FVC2002 DB2 | This approach has the leading performance in the field of cryptosystem biometrics. |
| Imamverdiyev, et al. [30] | Fuzzy Commitment | FVC2000 DB2a | FC built by feature exceed most of the existing FC in terms of Zero FAR. This approach experiences significant degradation in accuracy compared to conventional FAS. It is then computationally difficult to retrieve the original cryptographic key or template. |
| Ranjan and Singh [32] | Key Generating | Key genetation management | This scheme used divide and conquer method of biometric authentication and making the biometric data axes-independent with relative distances.This method can aid to high security and addresses the problem of biometric variation of a person. |
| Prasad and Kumar [56] | Non Invertible Transform | FVC 2002 DB1, DB2, and DB3 | This scheme achieves the four necessary properties in cancellable template design that are non-invertible, accuracy, diversity and revocability. |
| Yang, et al. [35] | Key Generating | FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 and FVC2004 DB2 | This scheme achieve better recognition performance compared to authentication systems that use absolute geometric measurements in local registration. |
| Nguyen, et al. [22] | Fuzzy Vault | FVC2002-DB2A, FVC2004-DB3A | This scheme provides good performance and strong security. |
| Bansal, et al. [24] | Fuzzy Vault | FVC2002-DB1_B | This technique provides revocability and diversity for increased security, but analysis security not complete |
| Li and Hu [25] | Fuzzy Vault | FVC 2000 (DB1), FVC 2002 (DB1, DB2, DB3, DB4), FVC 2004 (DB2) and FVC 2006 (DB2, DB3) | This technique provides strong security. However, security analysis is done only with brute force attack and Cross-Matching Attack. |
| Murillo-Escobar, et al. [57] | Non Invertible Transform | This scheme verify and justify in security aspects and its implementation in real applications embedded systems. | This scheme has advantages in complete statistical analysis. On the other hand no revocability properties achieve. |
| Sandhya and Prasad [58] | Non Invertible Transform | FVC2002 | This method has a good performance in terms of Equal Error Rate (EER) and also in terms of d-prime and K-S test values obtained. But the cryptographic process is too much to spend much time on the process |
| Wang and Hu [59] | Non Invertible Transform | FVC2002 DB1, DB2 and DB3 | This method satisfactory performance compared to the existing alignment-free cancellable template schemes. The performance of cancellable templates not achieved. |
| Sandhya and Prasad [69] | Hybrid Method | FVC 2002 DB1, DB2, and DB3 | This technique has good accuracy and strong security, then also has cancellable properties.- |
| Jin, et al. [74] | Hybrid Method | FVC2002 and FVC2004 | This scheme has good and strong accuracy against some major security and privacy attacks. |
| Barni, et al. [72] | Homomorphic | Public fingerprint | This method has advantages in terms of data |

| | Encryption | dataset | confidentiality but low accuracy. |
|---|---|---|---|
| Guo, et al. [60] | Non Invertible Transform | FVC2002 (OBI, DB2) and FVC2004 (OBI, DB2) | This scheme provided security, diversity and revocability. However, this scheme still experiences stolen-token scenario. |
| Wong, et al. [61] | Non Invertible Transform | FVC Datasets | This designated scheme achieves the non-invertible and revocable properties of the cancellable template. On the other hadn this scheme is still weak in the face of masquerade attack. |
| Gao [62] | Non Invertible Transform | FVC2000 DB1B, FVC2002 DB1B, FVC2004 DB1 | Recognition templates can perform more accurately than the original templates. |
| Gomez-Barrero, et al. [75] | Homomorphic Encryption | Chimeric databases | In this scheme, verification can be performed in encrypted domains without degradation. Then the system meets biometric information protection on irreversibility analysis and unlinkability. But schemas usually imply higher computational loads, and are not suitable for identification purposes. |
| Sadhya and Singh [76] | Salting | FVC2002 DB1, DB2, FVC2004 DB1, DB2 | This scheme has achieved unlinkability, cancelability and diversity requirements. |
| Wang, et al. [63] | Non Invertible Transform | FVC2002 DB1, FVC2002 DB2, FVC2002 DB3 FVC2004 DB2 | This method can reduce the risk of ARM, then this method performs better than the state-of-the-art alignment-free cancellable FTs. However, recognition efficiency and accuracy are still lacking. |
| Jin, et al. [77] | Salting | FVC2002 and FVC2004 | This scheme has a good accuracy performance and also meets the non-linkability and revocability template protection criteria. Further research is needed for the use of this scheme in the identification setting. |

### 3.2 What are the performance measures for evaluating the FTP schemes?

The FTP schemes can be measured from the security templates and matching performance. Security is measured in terms of information leakage levels or computational complexity which is involved in recovery of original templates from safe sketches or transformed templates [78, 79]. tching performance is normally calculated with False Accept Rate (FAR) and Genuine Accept Rate AR), of the FAS. Because of the intra-user riability in fingerprint images, in general, there is a trade-off between FAR/GAR and security in most template protection schemes. Lower security schemes tend to have higher FAR/GARs and vice versa. In addition th is also evaluation of ching performance using equal error rate (EER). value EER indicates that the proportion of false eptances is equal to that of false rejections [80]. The lower of EER means the higher accuracy of the biometric system. A variety of FTP schemes have been proposed. However, the matching performance and template security of many of the proposed algorithms have not been carefully evaluated.

To evaluate the security properties, there are three approaches that can be done based on some literature that has been reviewed. The first approach involves ntifying security evaluation by mating the number of guesses needed to recover the original minutiae template from the protected minutiae template via brute force [73, 81]. The second approach involves providing a proof that the proposed method is security evaluation by showing that the forward mapping is many-to-one and thus that the reverse mapping is one-to-many[82-84]. The third approach for evaluating the security properties of FTP schemes involves computing the percentage of the original minutiae template which remains unrecoverable when the protected template is compromised. This evaluation is more intuitive than a brute-force complexity analysis. It can be seen from Ferrara et al. [55]

In revocability measures, if the stored fingerprint template is compromised it should be sible to cancel that fingerprint template and sue a new one. Furthermore, the newly issued template should not match with the previously compromised template. 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 FTP scheme may be cancelled because of the possibility of altering irreversible transformation or a set of external parameters used on protected generation templates. This approach has been done in [48, 83, 85, 86]

In the evaluation of diversity,It should be sible to issue differents fingerprint templates for different applications related to the same user. these fingerprint templates 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 templates from the same fingerprint matches are 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 templates 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. Li and Hu [86] have shown that that this observation is correct by proving that it is possible to correlate some protected template from the same fingerprint to reconstruct the original template of the fingerprint. Some FTP schemes that address diversity evaluation are [48, 51, 53].

*Table 2: Performance measures for evaluating FTP*

| **Performance measure** | **Studies** |
|---|---|
| Security | [22, 25, 28, 34, 35, 50, 53, 54, 56, 58, 59, 67, 69, 74, 77] |
| Revocability | [25, 49-51, 53, 54, 56, 58, 59, 62, 69, 73-77] |
| Diversity | [20, 25, 50, 51, 58, 75, 76] |
| False Accept Rate (FAR)/ False Match Rate (FMR) | [10, 13, 22, 21, 25, 29, 30, 34, 35, 48, 49, 53-56, 58-60, 62, 65, 67, 72, 74] |
| Genuine Accept Rate (GAR) | [10, 13, 22, 24, 30, 34, 47, 54, 59, 65, 67, 74] |
| Equal Error Rate (EER) | [25, 30, 35, 39, 48, 50, 51, 53, 54, 56, 58-60, 66, 69, 72, 75-77] |
| False Rejection Rate (FRR)/ False Non Matching Rate (FNMR) | [21, 25, 27-29, 35, 48, 53, 55, 56, 58, 60, 74] |

Most FTP schemes are tested using a small database containing at least several hundred users. Thus, it is difficult to assess the difference in matching performance among the various FTP schemes proposed by the researchers. Similarly, accurate security estimates are provided for the fingerprint features distribution. If such models are not present, most schemes are unrealistic. Usually on security testing, researchers often assume that a uniform distribution of features is wrong to indicate that the system is secure. Whereas there are still things that need to be tested like leaked information from a safe sketch or a modified template. Usually, the performance implementation of the proposed algorithm is evaluated using public domain fingerprint databases such as FVC2004, FVC2002 and FVC2000. The goal is to highlight the issues that should be addressed during the implementation of the template protection scheme. Of course, different performance depends upon the choice of features, the adaptation of the selected feature schema, the database used, and the parameter values used in each schema.

*Table 3: List of fingerprint databases*

| **Fingerprint database** | **Studies** |
|---|---|
| FVC2000 | [25, 30, 62, 66] |
| FVC2002 | [10, 13, 22, 24, 25, 27, 28, 34, 35, 39, 48, 50, 51, 53-56, 58-60, 61, 62, 65-67, 69, 74, 76, 77] |
| FVC2004 | [22, 25, 49, 60-62, 66, 74, 76, 77] |
| FVC2006 | [25] |
| database of 400 fingerprint impressions | [20] |
| database of 188 fingerprint images acquired from an optical sensor. | [47] |
| NIST SD 14 database | [21] |
| IBM-99 optical database | [73] |
| CrossMatch Verifier 300 sensor | [72] |

Based on list table 3, it can be concluded that the fingerprint database most widely used by researchers to measure the performance evaluation is FVC2002, then FVC2004 and FVC2000. Only 1 paper is recorded in this work using FVC2006 database. And other databases such as NIST SD and IBM-99 are used by certain researchers. While some researchers collect their own data fingerprint through a fingerprint sensor. For more clearly can be seen in figure 5.

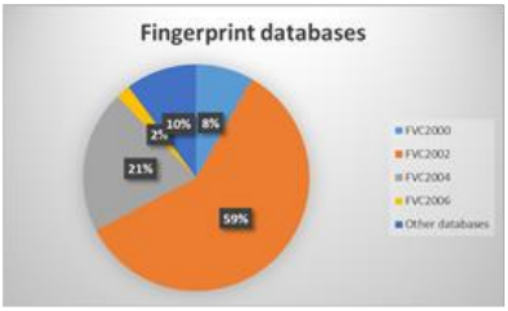


*Figure 5 : pie chart percentage of database fingerprint*

## 5. CONCLUSION

Based on surveys consisting of the last 17 years, it can be concluded that there are 4 techniques that can be done to overcome the problem of FT protection ie biometric cryptosystem, template transformation, hybrid method and homomorphic encryption. To design an ideal FTP scheme there are 4 traits that need attention are revocability, diversity, security and performance. The performance metrics that are often used to measure the performance of FTP are FAR, GAR, False Rejection Rate and EER. This library survey is expected to help fellow researchers in finding the latest critical and critical information from FTP. In addition, it can simplify the process of finding relevant literature that can be used for specific research scopes within the FTP.

## REFRENCES:


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

[5] J. Jeffers and A. Arakala, "Fingerprint alignment for a minutiae-based fuzzy vault," in *Biometrics Symposium, 2007*, 2007, pp. 1-6.

[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] 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.

[8] A. Juels and M. Sudan, "A fuzzy vault scheme," in *Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, 2002, p. 408.

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

[10] 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.

[11] 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.

[12] K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," *IEEE transactions on information forensics and security*, vol. 2, pp. 744-757, 2007.

[13] 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.

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

[15] S. Yang and I. M. Verbauwhede, "Secure fuzzy vault based fingerprint verification system," in *Signals, Systems and Computers, 2004. Conference Record of the Thirty-Eighth Asilomar Conference on*, 2004, pp. 577-581.

[16] S. Yang and I. Verbauwhede, "Automatic secure fingerprint verification system based on fuzzy vault scheme," in *Acoustics, Speech, and Signal Processing, 2005. Proceedings.(ICASSP'05). IEEE International Conference on*, 2005, pp. v/609-v/612 Vol. 5.

[17] 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.

[18] A. Nagar and S. Chaudhury, "Biometrics based asymmetric cryptosystem design using modified fuzzy vault scheme," in *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on*, 2006, pp. 537-540.

[19] J. Jeffers and A. Arakala, "Minutiae-based structures for a fuzzy vault," in *Biometric Consortium Conference, 2006 Biometrics Symposium: Special Session on Research at the*, 2006, pp. 1-6.

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

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

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

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

[28] 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.

[29] 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.

[30] 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.

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

[32] 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.

[33] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint bio-cryptosystem based on modified Voronoi neighbor structures," *Pattern Recognition,* vol. 47, pp. 1309-1320, 2014.

[34] 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.

[35] 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.

[36] 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.

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

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

[39] 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.

[40] 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.

[41] 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.

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

[43] 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.

[44] 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.

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

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

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

[52] 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.

[53] 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.

[54] 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.

[55] 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.

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

[57] 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.

[58] 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.

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

[60] 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.

[61] 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.

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

[63] 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.

[64] 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.

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

[66] 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.

[67] 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.

[68] 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.

[69] 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.

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

[71] 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.

[72] 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.

[73] 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.

[74] 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.

[75] 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.

[76] 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.

[77] 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.

[78] 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.

[79] 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.

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

[81] S. Wang and J. Hu, "Design of alignment-free cancelable fingerprint templates via curtailed circular convolution," *Pattern Recognition,* vol. 47, pp. 1321-1329, 2014.

[82] 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.

[83] 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.

[84] 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.

[85] J. Shi, Z. You, M. Gu, and K.-y. Lam, "Biomapping: privacy trustworthy biometrics using noninvertible and discriminable constructions," in *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on*, 2008, pp. 1-4.

[86] C. Li and J. Hu, "Attacks via record multiplicity on cancelable biometrics templates," *Concurrency and Computation: Practice and Experience,* vol. 26, pp. 1593-1605, 2014.

# FINGERPRINT TEMPLATE PROTECTION SCHEMES: A LITERATURE REVIEW

ORIGINALITY REPORT

| 22% | 12% | 19% | 3% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | www.cse.msu.edu<br>Internet Source | 2% |
| 2 | M.A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R.M. López-Gutiérrez. "A robust embedded biometric authentication system based on fingerprint and chaotic encryption", Expert Systems with Applications, 2015<br>Publication | 1% |
| 3 | Security and Privacy in Biometrics, 2013.<br>Publication | 1% |
| 4 | people.sabanciuniv.edu<br>Internet Source | 1% |
| 5 | Sharat Chikkerur, Nalini K. Ratha, Jonathan H. Connell, Ruud M. Bolle. "Generating Registration-free Cancelable Fingerprint Templates", 2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems, 2008<br>Publication | 1% |

| | | |
|---|---|---|
| 6 | R. Ranjan, S. K. Singh. "Improved and innovative key generation algorithms for biometric cryptosystems", 2013 3rd IEEE International Advance Computing Conference (IACC), 2013<br>Publication | 1 % |
| 7 | coek.info<br>Internet Source | 1 % |
| 8 | Song Wang, Wencheng Yang, Jiankun Hu. "Design of Alignment-Free Cancelable Fingerprint Templates with Zoned Minutia Pairs", Pattern Recognition, 2017<br>Publication | 1 % |
| 9 | "Biometric Security and Privacy", Springer Nature, 2017<br>Publication | 1 % |
| 10 | Chulhan Lee, Jaihie Kim. "Cancelable fingerprint templates using minutiae-based bit-strings", Journal of Network and Computer Applications, 2010<br>Publication | 1 % |
| 11 | Submitted to Multimedia University<br>Student Paper | 1 % |
| 12 | www.semanticscholar.org<br>Internet Source | 1 % |
| 13 | Husna Jamal Abdul Nasir, Ku Ruhana Ku-Mahamud. "Wireless Sensor Network: A | 1 % |

Bibliographical Survey", Indian Journal of Science and Technology, 2016
Publication

| | | |
|---|---|---|
| 14 | pdfs.semanticscholar.org<br>Internet Source | <1% |
| 15 | Sanjay G. Kanade, Dijana Petrovska-Delacrétaz, Bernadette Dorizzi. "Enhancing Information Security and Privacy by Combining Biometrics with Cryptography", Springer Science and Business Media LLC, 2012<br>Publication | <1% |
| 16 | Lecture Notes in Computer Science, 2007.<br>Publication | <1% |
| 17 | www.slideshare.net<br>Internet Source | <1% |
| 18 | Limei Guo, Yun Mao, Ying Guo. "Non-invertible fingerprint template protection with polar transformations", 2016 14th Annual Conference on Privacy, Security and Trust (PST), 2016<br>Publication | <1% |
| 19 | Andrew Beng Jin Teoh, Thian Song Ong. "Secure biometric template protection via randomized dynamic quantization transformation", 2008 International | <1% |

| | | |
|---|---|---|
| | Symposium on Biometrics and Security Technologies, 2008<br>Publication | |
| 20 | Azizi Ab Aziz. "Incorporating an Ambient Agent to Support People with a Cognitive Vulnerability", Studies in Computational Intelligence, 2012<br>Publication | <1 % |
| 21 | unsworks.unsw.edu.au<br>Internet Source | <1 % |
| 22 | doi.org<br>Internet Source | <1 % |
| 23 | www.warse.org<br>Internet Source | <1 % |
| 24 | www.ijert.org<br>Internet Source | <1 % |
| 25 | Pradheeba, , and Ravi Subban. "Fingerprint template protection techniques — A survey and analysis", 2014 IEEE International Conference on Computational Intelligence and Computing Research, 2014.<br>Publication | <1 % |
| 26 | Feng, Yicheng, and Pong C. Yuen. "BIOMETRIC TEMPLATE PROTECTION: TOWARDS A SECURE BIOMETRIC SYSTEM", Handbook of Pattern Recognition and Computer Vision, 2009.<br>Publication | <1 % |

| | | |
|---|---|---|
| 27 | Mulagala Sandhya, Munaga V.N.K Prasad. "k-Nearest Neighborhood Structure (k-NNS) based alignment-free method for fingerprint template protection", 2015 International Conference on Biometrics (ICB), 2015<br>Publication | <1 % |
| 28 | arxiv.org<br>Internet Source | <1 % |
| 29 | oaji.net<br>Internet Source | <1 % |
| 30 | researchbank.swinburne.edu.au<br>Internet Source | <1 % |
| 31 | Communications in Computer and Information Science, 2012.<br>Publication | <1 % |
| 32 | Priyanka Das, Kannan Karthik, Boul Chandra Garai. "A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs", Pattern Recognition, 2012<br>Publication | <1 % |
| 33 | Zhou, Xuebing, Alexander Opel, Johannes Merkle, Ulrike Korte, and Christoph Busch. "Enhanced template protection with passwords for fingerprint recognition", 2011 Third International Workshop on Security and Communication Networks (IWSCN), 2011.<br>Publication | <1 % |

| | | |
|---|---|---|
| 34 | academicscience.co.in<br>Internet Source | <1 % |
| 35 | Vedrana Krivokuća, Waleed Abdulla. "Cancellability and diversity analysis of fingerprint template protection scheme based on compact minutiae pattern", Information Security Journal: A Global Perspective, 2016<br>Publication | <1 % |
| 36 | hrcak.srce.hr<br>Internet Source | <1 % |
| 37 | mafiadoc.com<br>Internet Source | <1 % |
| 38 | subs.emis.de<br>Internet Source | <1 % |
| 39 | wavelab.at<br>Internet Source | <1 % |
| 40 | www.irjet.net<br>Internet Source | <1 % |
| 41 | www.mecs-press.org<br>Internet Source | <1 % |
| 42 | Advances in Intelligent Systems and Computing, 2016.<br>Publication | <1 % |
| 43 | Jinyang Shi. "Reusable Set Constructions Using Randomized Dissolvent Templates for | <1 % |

Biometric Security", GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference, 11/2009
Publication

| | | |
|---|---|---|
| 44 | Krivokuća, Vedrana, and Waleed Abdulla. "Fingerprint template protection scheme based on partial minutiae patterns: a comprehensive non-invertibility analysis", International Journal of Biometrics, 2015.<br>Publication | <1 % |
| 45 | Musa, Wahab, Ku Ruhana, and Azman Yasin. "Long Term Energy Demand Forecasting based on Hybrid, Optimization: Comparative Study", International Journal of Soft Computing and Software Engineering, 2012.<br>Publication | <1 % |
| 46 | Zhe Jin, Yen-Lung Lai, Jung Yeon Hwang, Soohyung Kim, Andrew Beng Jin Teoh. "Ranking Based Locality Sensitive Hashing Enabled Cancelable Biometrics: Index-of-Max Hashing", IEEE Transactions on Information Forensics and Security, 2017<br>Publication | <1 % |
| 47 | thesai.org<br>Internet Source | <1 % |
| 48 | www.cerias.purdue.edu<br>Internet Source | <1 % |

| | | |
|---|---|---|
| 49 | A. Idri, H. Benhar, J.L. Fernández-Alemán, I. Kadi. "A Systematic Map of Medical data preprocessing in knowledge discovery", Computer Methods and Programs in Biomedicine, 2018<br>Publication | <1 % |
| 50 | Joanna Putz-Leszczyńska. "Signature verification: A comprehensive study of the hidden signature method", International Journal of Applied Mathematics and Computer Science, 2015<br>Publication | <1 % |
| 51 | Juan Carlos Bernal-Romero, Juan Manuel Ramirez-Cortes, Jose De Jesus Rangel-Magdaleno, Pilar Gomez-Gil et al. "A Review on Protection and Cancelable Techniques in Biometric Systems", IEEE Access, 2023<br>Publication | <1 % |
| 52 | Marina Blanton, William M. P. Hudelson. "Chapter 14 Biometric-Based Non-transferable Anonymous Credentials", Springer Science and Business Media LLC, 2009<br>Publication | <1 % |
| 53 | atvs.ii.uam.es<br>Internet Source | <1 % |
| 54 | cps-vo.org<br>Internet Source | |

| | | |
|---|---|---|
| | | <1% |
| 55 | ijcnis.org<br>Internet Source | <1% |
| 56 | mountainscholar.org<br>Internet Source | <1% |
| 57 | ntnuopen.ntnu.no<br>Internet Source | <1% |
| 58 | pure.tue.nl<br>Internet Source | <1% |
| 59 | repository.iiitd.edu.in<br>Internet Source | <1% |
| 60 | research.sabanciuniv.edu<br>Internet Source | <1% |
| 61 | www.dtic.mil<br>Internet Source | <1% |
| 62 | www.scribd.com<br>Internet Source | <1% |
| 63 | Anil K. Jain. "Biometric Template Security", EURASIP Journal on Advances in Signal Processing, 2008<br>Publication | <1% |
| 64 | Anil K. Jain. "Security Of Biometric Systems", Introduction to Biometrics, 2011<br>Publication | <1% |

| | | |
|---|---|---|
| 65 | Arpita Sarkar, Binod K. Singh. "A review on performance,security and various biometric template protection schemes for biometric authentication systems", Multimedia Tools and Applications, 2020<br>Publication | <1% |
| 66 | Ferrara, M., D. Maltoni, and R. Cappelli. "Non-invertible Minutia Cylinder-Code Representation", IEEE Transactions on Information Forensics and Security, 2012.<br>Publication | <1% |
| 67 | Karthik Nandakumar, Anil K. Jain. "Biometric Template Protection: Bridging the performance gap between theory and practice", IEEE Signal Processing Magazine, 2015<br>Publication | <1% |

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | On | | |