FinCaT: Fingerprint Cancellable Template Protection Remediation Schemes, Challenges, and Future Directions

Eain Ul Sehar
Dept. of Computer Science and Information Technology
Central University of Jammu
Jammu and Kashmir, India
eaini97@gmail.com

Arvind Selwal
Dept. of Computer Science and Information Technology
Central University of Jammu
Jammu and Kashmir, India
arvind.csit@cujammu.ac.in

Deepika Sharma
Dept. of Computer Science and Information Technology
Central University of Jammu
Jammu and Kashmir, India
sharmadeepika749@gmail.com

***Abstract*— Recent years have revealed a rapid expansion in the use of various biometric technologies for authentication management systems. Although biometric systems have innumerable merits over conventional token-based and knowledge-based identification systems like ID cards or passwords, but they are still susceptible to diverse security threats. Among all, the attack on the biometric template database is the most crucial and adverse attack. If the user templates are jeopardized at any level of biometric system, then they cannot be further used for security mechanism. Henceforth, it is requisite to provide privacy and security to biometric template data by modifying these through revocable and non-invertible transformations to acquire cancellable biometric templates. The cancellable biometrics offers promising remedies for biometric template protection. Our work aims to expound a detailed review of state-of-the-art transformation-based fingerprint template protection schemes. Additionally, the paper discusses various publicly available benchmark datasets. We also deliberate the research challenges emerging from this study, which requires to be addressed in this rapidly evolving field of research. The selection of a suitable function for transformation process is still a major open challenging task, so that the results obtained after applying the function does not result in cross-matching of the templates in the database.**

Keywords*— *cancellable biometrics, cryptosystem, fingerprint, template attacks, template protection.

I. INTRODUCTION

The advancement and progression in the field of information technology and other fields of science has played a great role in improving the living standard of humans. The need of identity management and protections has surged as a result of these advancements. To build up the identity of a person is the most crucial job in any identity management system. Other substitute identity representations like traditional token-based (ID cards) and knowledge-based (passwords) are not enough to ascertain the reliable identity of a person because they can be displaced, forgotten or heisted easily. Biometric recognition provides a genuine solution to this problem. The significance of biometric science in today's society has been augmented by the necessity for extensive identity management systems whose operability depends on the precise ascertainment of a person's identity in relation to certain distinct applications. The physical and behavioral traits (biometric traits) of an individual like fingerprint, face, iris, hand geometry, voice, gait, etc. have exhibited tremendous potential to distinguish between an adversary and a genuine person [1]. A biometric system, basically, refers to a pattern recognition system that captures the data from a person, elicits a principal feature set from the biometric data, matches the query feature set with the existing feature sets kept in the database, and provides a match score based on this comparison. The identification/verification of a person in a biometric system is carried out in two steps: (i) Enrolment of the individual, and (ii) Verification/Identification of the individual.

The biometric system provides numerous benefits over the conventional identification system, but it is still in peril to various adversarial attacks. The most crucial among all the attacks is the attack on the template database. With the aim to surmount the vulnerabilities of the fingerprint biometric template database, several template protection schemes like cancellable biometrics and cryptosystem-based techniques have been presented in the literature. The irreversible conversion of the biometric template that guarantees the security and privacy of the user template is termed as cancellable biometrics. The main concept behind cancellable biometrics is that a user template can be revoked, if jeopardized and by substituting the user key with a new key, a fresh template can be reissued [2]. Particularly, a lot of research work is being carried out in the field of cancellable biometrics since the last decade. As the fingerprint biometric systems hold the largest market share in biometrics and have been used in numerous applications, the security challenges and deployment of new security techniques in the fingerprint template is a crucial research challenge.

We have inferred from the literature that though the existing survey papers provide quality information regarding the cancellable biometrics, however, most of the study has been carried out until 2019. The recent considerable work by eminent researchers in the field of FinCaT protection has motivated us to undertake this survey. The main motivation is to study and analyze various state-of-the-art FinCaT protection techniques as well as their strengths and limitations.

The key contributions of this paper are underlined as:

i. Our study expounds the taxonomy of template protection schemes.
ii. A comprehensive review of the state-of-the-art FinCaT techniques is presented in this paper.
iii. We provide the details regarding the publicly available benchmarking databases.
iv. The paper also presents some open research challenges which arose from our study.

The rest of the paper is assembled as follows: Section 2 provides the literature survey of various state-of-the-art transformation-based template protection schemes. Section 3 provides the survey of the databases. Section 4 presents the various open research challenges followed by the conclusion in Section 5.

978-1-6654-2392-2/21/$31.00 ©2021 IEEE
DOI 10.1109/CICT53244.2021.00056

II. State-of-the-art FinCaT

A. Biometric System Attacks

Ratha et al. [3] studied and identified that in a general biometric system, there are eight different types of attack points (Fig. 1). *In attack 1*, the adversary bypasses the recognition systems by presenting a fabricated biometric trait to the sensor [4] [5]. *In attack 2*, the sensor is bypassed by replaying a biometric trait, which is stolen by the adversary by obstructing the medium between the feature extractor module and the sensor, to the feature extractor. *In attack 3*, the feature extractor module is constrained by the adversary to produce the feature values selected by the interloper in lieu to generate values from the genuine data obtained from the sensor. *In attack 4*, the imposter purloins the feature values of genuine user, which are replayed to the matcher, by intercepting the communication channel between the feature extractor and matcher modules. *In attack 5*, in spite of the values acquired from input feature set, the adversary bypasses the biometric system by selecting a high matching score and constraining the matcher to produce the same score. *In attack 6*, the security of the database is compromised by modifying or removing existing templates and adding new ones by the adversary. *In attack 7*, the biometric template is taken away, replaced or altered by the adversary by obstructing the medium between the system database and the matcher. *In attack 8*, the original decision of acceptance or rejection by the matcher is altered by the adversary by meddling in the match score.

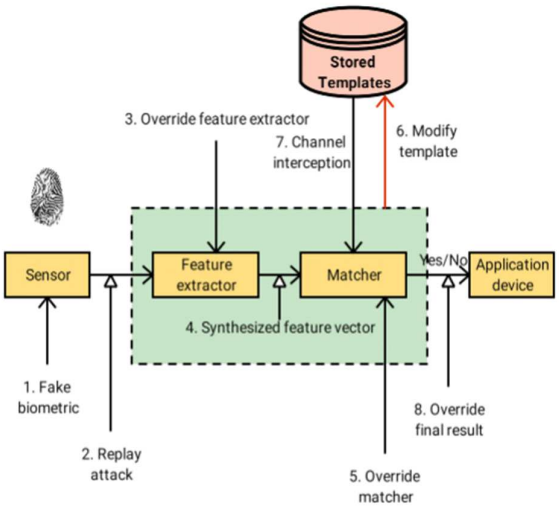

Fig. 1. Points of attack in a biometric system [3]

The biometric data of the user can be severely influenced by the detrimental and critical attacks on the biometric template database. The biometric data is set down in a template database during the enrolment stage and this data is correlated with the query data during the verification stage. Not typical of conventional identity representations like passwords or ID cards, physiological and behavioral traits are unable to rescind or revalue. The storage of raw or unprotected template in a database could lead to consequential security concerns [6] [7]. If the template database is either heisted or disclosed, it can be used to reconstruct the original biometric features. Like in case of fingerprint biometric system, some information such as minutiae location and orientation can be acquired from the stolen template and utilized to recreate an analogous fingerprint of the original fingerprint with admissible precision. Three consequential susceptibilities of template database attack are as follows: The adversary's template replaces the original template; the imposter can create a physical spoof from the template; and the matcher can be iterated using the stolen template to gain illicit access. This issue of the attack on template database facilitates that the protection of the biometric templates is a primary apprehension in the current times.

B. Broad Template Protection Schemes

The essence of designing a secured biometric system lies in the generation of a protected template through transformation of the features of a person and later the use of this secure template for verification in preference to the direct deposition of raw template in the database [8]. The protected transformed template is generated by performing the transformation in such a manner that the information, which could be used by the adversary to reconstruct the original template, is kept concealed so as not to be withdrawn by the adversary [9]. In literature, there are plentiful techniques for securing the biometric template database. Each and every template security scheme ought to fulfill the following properties:

TABLE I. DESIGN CRITERIA FOR AN IDEAL BIOMETRIC TEMPLATE PROTECTION SCHEME

S. No.	Characteristic	Description
1.	Diversity	All the protected templates derived from the same biometric sample must be non-identical, thereupon guaranteeing the privacy of the user.
2.	Security	It ought to be extremely hard or impossible to rebuild the authentic biometric template from the protected one.
3.	Revocability	It should be facile to revoke a jeopardized template and issue a new template in lieu of the jeopardized template.
4.	Performance	After applying the transformation on the user template, the recognition performance should not degrade.

The template protection techniques presented in the literature can be mainly categorized into *feature transformation/ cancellable biometrics* and *biometric cryptosystem*.

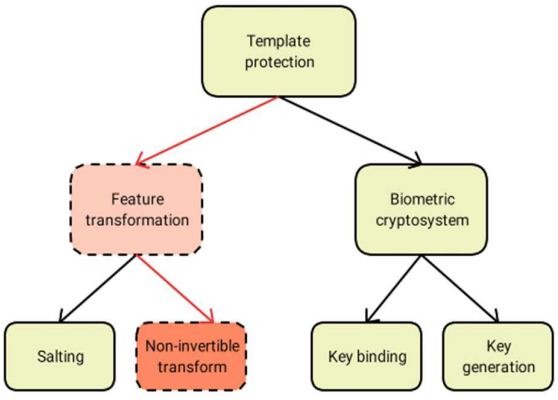

Fig. 2. Classification of template protection schemes

The biometric cryptosystems can be utilized for the purpose of biometric template protection. In a *biometric cryptosystem*, some universal details about the template, known as helper data, are stored. This helper data is required to draw out a key from the query feature-set during the process of matching. Matching is carried out indirectly by conforming the viability of the drawn-out key. Biometric cryptosystems are categorized into key-binding and key-generation systems. The key-binding biometric cryptosystem approach is widely used the popular techniques of fuzzy vault [10] and fuzzy commitment. Fuzzy extractors and secure sketches are the examples of key-generation schemes.

The main focus of this research is on the approach of feature transformation. In this technique, a transformation function (F) is used to transmute a raw template (T) into protected-template (F (T, K)) and the transmuted template is deposited in a database. Mostly, the transformation function uses an arbitrary key K as an input parameter. Before the matching, the input query feature (Q) is transmuted into protected query (F (Q, K)) using the same transformation function (F) and the transmuted query (F (Q, K)) is compared with the transmuted template (F (T, K)) [11]. Based on the properties of the transformation function (F), there are two further classifications of the feature transform schemes as *salting* and *non-invertible transform*.

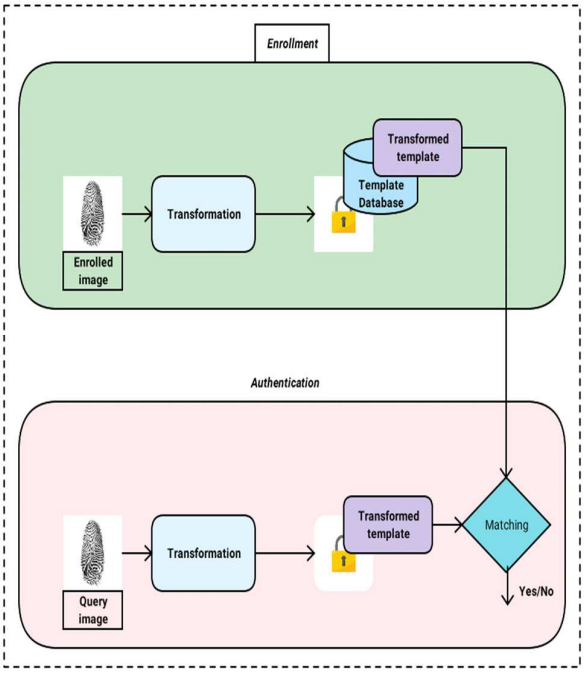

Fig. 3. Authentication mechanism in a general feature transformation approach [1]

i. Salting: Salting or bio-hashing is an invertible transformation, which means the secured template can be easily changed back into the original template with use of key and transformation function. The reliability of salting is subject to confidentiality of the key or password.
ii. Non-invertible transform: In this approach, the biometric template is converted into a protected template by the application of a non-invertible transformation function. It is a uni-directional function, F, which is arduous to invert even with the key. The principal property of this procedure is that although the key and/or the transmuted template are familiar to the adversary, it is computationally arduous for him/her to revert it back into the original biometric. Some of the different non-invertible transforms used in the literature are Cartesian transform, Polar transform, Hadamard transform, Wavelet transform, rotation-based transform, projection-based transform, etc.

For generating a cancellable and rescindable fingerprint template, polar-grid based 3-tuple quantization (PGTQ) was proposed by Jin et al. [2] in 2012, wherein a set of minutiae points is transformed into bit-string. Liu et al. (2012) [12] proposed a random local region descriptor (RLRD) based determined-length feature extraction mechanism for fingerprint biometric. Wong et al. (2016) [13] designed a determined-length cancellable fingerprint technique formulated on a minutia descriptor called "multi-line code" (MLC). The proposed algorithm consists of four stages, namely MLC generation, a random projection (RP) technique, kernel principal component analysis (KCPA) and binarization. Wang et al. (2017) [14] used partial discrete Fourier transform (DFT) and handmade transform in order to generate a secured fingerprint template from the minutiae points. In Wang et al. (2017) [15], they designed a new alignment-free method for the generation of cancellable fingerprint templates in which local minutiae structures are constructed through zoned minutia pairs.

Trivedi et al. (2018) [16] proposed a non-invertible fingerprint template, which contains only the correlative geometric information regarding the minutiae points. Similar to this technique, Ali et al. (2018) [8] proposed a distinctly secure scheme, which utilizes the location information regarding the minutia points to create a protected user template. Security analysis proves that this technique is very sturdy and reliable. In 2019, Atighehchi et al. [17] proposed an improved Bio-hashing algorithm in which the projection matrix is produced by integrating the secret and biometric data. The proposed technique has been evaluated on FVC2002 DB1 fingerprint database, PolyFKP (knuckle print database) and VEINEGY database (dorsal hand vein database). The experimental analysis shows that by combining the secret with biometric data, the proposed scheme has reduced the impact of the stolen-token attack. Kho et al. (2019) [18] proposed a binary cancellable fingerprint template based on an alignment-free minutiae descriptor, PLS and PR-NNLS optimization problem.

In order to overcome the shortcomings of traditional fingerprint systems formed on minutiae representation, determined-length and ordered bit-string transformation technique was proposed by Kho et al. (2020) [19]. In 2020, Trivedi et al. [1] improvised the method proposed in [16] by using Delaunay triangulation of minutiae points and user key. Some feature which does not contain any information regarding the location of minutia points is elicited from the triangle so as to obtain a non-invertible template. A modified symmetric hash method was proposed by Ajish S. et al. (2020) [11] in which a key value is used as a multiplication parameter. The modified symmetric hash function is a combination of salting and non-invertible transformation.

An advanced feature transformation technique was recently proposed by Jacob et al. (2020) [20], which uses

DNA based encoding methodology. The Z pattern generation has been used for implementing the transformation followed by the DNA codec. A fingerprint authentication technique built upon the modification of minutiae point characteristics using a unique user key was proposed by Ali et al. (2020) [21]. Abdullahi et al. (2020) [22] proposed a novel technique for the generation of a reliable and sturdy hash from a fingerprint image using Fourier-Mellin transform and fractal coding. Much recently, alignment-free cancellable fingerprint templates with dual protection, composed of the window-shift-XOR model and the partial discrete wavelet transform were designed by Shahzad et al. (2021) [23]. The window-shift-XOR model effectively defends the ARM with simple operations and is combined with the partial DWT to provide dual protection and enhance matching performance.

TABLE II. A COMPARATIVE SUMMARY OF THE EXISTING TRANSFORMATION-BASED TEMPLATE PROTECTION SCHEMES

Authors (Year)	Key Concept	Type		Dataset Used	Performance (EER)	Observations	
		Salting	*Cancellable*			*Strength*	*Weakness*
Jin et al. (2012) [2]	Fingerprint binary vector using Polar-grid based 3-tuple quantization (PGTQ)	×	✓	FVC2002(DB1 &DB2) and FVC2004(DB1 & DB2)	EER = 1.19%, 6.94%, 8.66% & 16.35% for respective databases	The proposed template has attained a good level of reliability	The performance deterioration as a consequence of many-to-one mapping could not be rectified
Liu et al. (2012) [12]	Random local region descriptor (RLRD)-based determined-length feature extraction using Tico's sampling structure	×	✓	FVC2002(DB1, DB2 & DB3)	EER = 4.07% for real RLRD & 3.67% for bit RLRD	The proposed RLRD features outperform other fixed-length features	Low performance due to the lack of core point for alignment
Wong et al.(2016) [13]	A determined-length binary cancellable fingerprint scheme based on Multi-line code (MLC) descriptor	×	✓	FVC2002 (DB1 & DB2) and FVC2004 (DB1 & DB2)	EER = 1.61%, 1.69%, 3.73% & 3.26% for respective databases	Immune to inverse attack and linkage attack	The system may be exposed to masquerade attack because of the subjection of certain information needed for KCPA
Wang et al.(2017) [14]	Generation of protected template using Partial DFT and handmade transform	×	✓	FVC2002(DB1, DB2 & DB3)	EER = 1%, 2% & 5.2% for respective databases	Satisfied all the design criteria for cancellable biometrics	The recognition performance is affected by the consequential degradation of the distinguished fingerprint features in the course of transformation
Wang et al.(2017) [15]	Local minutiae structures are constructed through zoned minutia pairs and Partial DFT-based transformation is applied	×	✓	FVC2002(DB1, DB2 & DB3) and FVC2004 DB2	EER = 0.19%, 1%, 4.29% & 9.01% for respective databases	Reduces the risk of ARM	Accuracy degradation problem
Trivedi et al. (2018) [16]	A cancellable template storing only the correlative geometric information about the minutiae points	×	✓	FVC2000(DB1, DB2, DB3 & DB4)	EER = 6.806%, 8.044%, 2.509% & 4.506% for respective databases	The proposed template does not vary with rotation, translation, distortion and is immune to reconstruction algorithm	The EER (6.806 in FVC2000 DB1 & 8.044 in FVC2000 DB2) is not adequate to depict the viability of the proposed technique in real-life applications
Ali et al. (2018) [8]	A distinctly secure scheme that utilizes location information of the minutiae points	×	✓	FVC2002(DB1, DB2 & DB3)	EER = 2%, 1% & 3.1% for respective databases	The proposed template shows good recognition accuracy	Reduces efficiency
Atighehchi et al. (2019) [17]	An improved Bio-hashing algorithm in which the projection matrix is produced by integrating the secret and biometric data	✓	✓	FVC2002 DB1, PolyFKP and VEINEGY	EER = 3.72% for FVC2002 database	Reduces the impact of stolen-token attack	Performance deterioration due to the assumption of random secret

Kho et al. (2019) [18]	An innovative transformation mechanism based on minutiae descriptor called Partial Local Structure (PLS) and Permuted Randomised Non-Negative Least Square (PR-NNLS) optimization	×	✓	FVC2002(DB1, DB2, DB3 & DB4) and FVC2004(DB2)	EER = 0.01%, 0.06% 3.61%, 5% & 4.51% for respective databases	Satisfied all four design criteria for cancellable biometrics and avoided performance deterioration	Suffers from slight security-performance trade-off
Kho et al. (2020) [19]	2-D elliptical Gaussian functions based fixed-length and ordered bit transformation	×	✓	FVC2002 (DB1, DB2 & DB3), FVC2004 (DB1 & DB2) and FVC2006 (DB1 & DB2)	EER = 1.10%, 0.70%, 4.23%, 7.71%, 5.79%, 0.82% & 5.24% for respective databases	Superior recognition accuracy than existing techniques	The simple pixel intensity representation is prone to image mis-alignment
Trivedi et al. (2020) [1]	Delaunay triangulation of minutiae points and user key to generate a cancellable fingerprint	×	✓	FVC2002 (DB1 & DB2)	EER = 1.2% & 2.1% for respective databases	The template is rescindable, distinctive, secure and also provides good recognition performance	_
Ajish S. et al. (2020) [11]	Modified symmetric hash method	✓	✓	FVC2004 DB3	Accuracy reaches to 96.09%	The modified hashed fingerprint templates are more secure than the existing hashed fingerprint templates	Vulnerable to reversibility attacks
Jacob et al. (2020) [20]	Feature transformation using DNA based encoding methodology	×	✓	_	_	The proposed system is sturdy and effectual in terms of computation to control the attacks	_
Ali et al. (2020) [21]	Fingerprint authentication technique based on modification of minutiae point characteristics using a distinctive user key	✓	✓	FVC2002 (DB1, DB2 & DB3)	EER = 1.73%, 1% & 2.43% for respective databases	Provides good recognition accuracy and intra-subject variations caused by rotation and translation can be handled	_
Abdullahi et al. (2020) [22]	A secure robust hash using Fourier-Mellin transform and fractal coding	✓	✓	FVC2002 (DB1, DB2 &DB3) and FVC2004 (DB1, DB2 & DB3)	EER = 0.364%, 0.538%, 2.395%, 2.348%, 5.925% & 2.365% for respective databases	The proposed method shows sturdiness and resilience to confidentiality and security attacks	Incapable of detecting malicious tampering in biometric samples
Shahzad et al. (2021) [23]	Window-shift-XOR model and the partial DWT for designing alignment-free cancellable fingerprint templates with dual protection	×	✓	FVC2002 (DB1, DB2 & DB3), FVC2004 (DB1 & DB2)	EER = 0%, 0%, 1.63%, 7.35% & 4.69% for respective databases	The proposed method tackles the ARM attack and satisfies all the requirements for cancellable biometrics	The designed transformation doesn't directly protect the minutiae set.

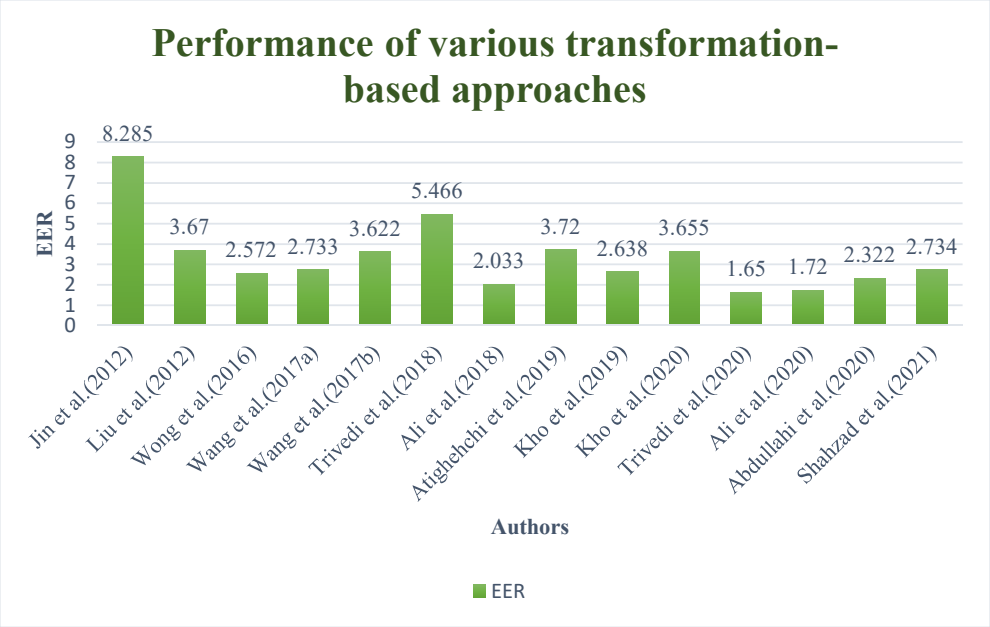

Fig. 4. Performance of some transformation-based template protection technique

III. Databases

This section provides an overview of the various fingerprint benchmarking databases.

A. FVC databases

The four international Fingerprint Verification Competition (FVC) were arranged in the years 2000, 2002, 2004, and 2006. By employing three sensors and a synthetic generator, four databases were compiled. Each database in FVC2000 and FVC2002 used 110 fingers with 8 impressions per finger leading to 880 impressions per database. In FVC2004, 120 fingers were used with 12 impressions per finger, resulting in 1440 fingerprint images in each database. FVC2006 used 150 fingers with 12 samples per finger, which means each database consists of 1800 fingerprint images. The performance of fingerprint template protection methods using FVC databases, is evaluated using two different protocols, namely FVC protocol and 1vs1 protocol.

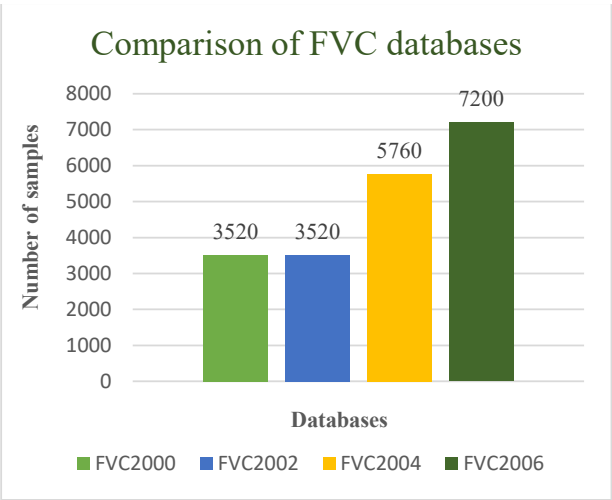

Fig. 5. A comparison of FVC databases

B. CASIA-Fingerprint Version 5.0

The Institute of Automation, Chinese Academy of Sciences (CASIA) acquired the CASIA fingerprint database (version 5). This database consists of 20,000 fingerprint images from 500 persons. URU4000 fingerprint sensor has been used to capture the images. In this database, 8 fingers were used with 5 samples per finger, resulting in 40 samples per person. All the fingerprint images have the image resolution as 328*356 and are 8-bit gray-level BMP files [24].

C. NIST special database-302

A data collection was organized by the Intelligence Advanced Research Projects Activity (IARPA) as a segment of its Nail to Nail (N2N) Fingerprint Challenge in September 2017 [25]. Two different FBI experts captured the N2N fingerprint images twice per person, resulting in two N2N baseline datasets. SD-302 is a series of distributions, each comprising of a logical subset of N2N fingerprint challenge data collection images. The dataset has been divided into several parts. SD302d contains plain fingerprint images from auxiliary devices.

IV. Open Research Challenges and Future Perspectives

In our study, we have reviewed various transformation-based template protection schemes with their proposed methodologies and performances. This study has unveiled several research challenges that may be utilized as future research opportunities. The open research issues with their future perspectives which have been identified from our study are listed below.

a. The template transformation techniques are vulnerable to different security attacks. This requires the security strength of template transformation techniques to be considered and the complexity of recovering the original template to be analyzed. The complexity of obtaining the complete pre-image of a

transformed template also needs to be taken into consideration.

b. Biometric image hashing techniques are extensively explored and have attained impactful developments. But just a few of available remedies impart two-factor cancellability as well as synchronously satisfy the trade-off among all design criteria of an ideal template security technique. Hence, image hashing techniques with improved potential to detect malicious interfering in biometric samples and increased biometric quality need to be developed.
c. While artificial intelligence (AI) has attained prominent success in biometric applications, how to protect template data of AI-based biometric systems is an open area and a lot of work requires to be done. In addition, homomorphic encryption is worthy of further study to apply it to fingerprint matching with transformed templates.
d. Due to the well-known trade-off between security and performance, a sole template security scheme may not be adequate to fulfill all the requirements of an application. AS such, hybrid schemes which utilize the strengths of various template security approaches must be designed.
e. Selection of an appropriate function for transformation purposes is a challenging task so that the results obtained after applying the function must not result in cross-matching of templates in the database.
f. Performance deterioration is caused if the transformation function is implemented directly over the minutiae descriptor. Hence, the techniques need to designed, wherein the conversion function is not implemented over the biometric features directly. The techniques which have already been proposed in the literature need to be amplified or augmented by integrating with available biometric approaches.
g. The performance of some transformation methods is impacted by the quality of binary biometric representations, hence efficient means of capturing the distinguished biometric feature information need to be examined, which can result in better binary representations.

V. Conclusions

The current approach of biometrics-based authentication suffers from most susceptible template attacks which need to be addressed by the research community**.** Besides, biometric template protection has gained noticeable attentiveness from the prominent researchers because of the security and confidentiality issues for the biometric template. This survey focused on the detailed study of several template protection techniques presented in the literature and their underlined merits and demerits are also highlighted. Additionally, we reviewed the existing publically available benchmarking fingerprint datasets used for evaluating the performance of cancellable biometrics-based template protection schemes. The study clearly reveals that, the well-known security-performance trade-off issue needs to be addressed. Also, the robustness of the templates against the security attacks requires to be increased. In the future, the research work may be slanted towards designing more robust template protection techniques with lower FAR and FRR.

References

[1] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Comput. Secur.*, vol. 90, p. 101690, 2020, doi: 10.1016/j.cose.2019.101690.

[2] Z. Jin, A. B. Jin Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacy preserving," *Expert Syst. Appl.*, vol. 39, no. 6, pp. 6157–6167, 2012, doi: 10.1016/j.eswa.2011.11.091.

[3] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001, doi: 10.1147/sj.403.0614.

[4] D. Sharma and A. Selwal, "On data-driven approaches for presentation attack detection in iris recognition systems," In: P. K. Singh, Y. Singh, M. H. Kolekar, A. K. Kar, J. K. Chhabra, A. Sen (eds) Recent Innovations in Computing. ICRIC 2020, *Lecture Notes in Electrical Engineering*, vol 701. Springer, Singapore. doi: 10.1007/978-981-15-8297-4_38.

[5] A. Habib and A. Selwal, "Robust anti-spoofing techniques for fingerprint liveness detection : A Survey," *IOP Conf. Ser.: Mater. Sci. Eng.*, 2021, doi: 10.1088/1757-899X/1033/1/012026.

[6] S. I. Manzoor and A. Selwal, "An analysis of biometric based security systems," *2018 Fifth Int. Conf. Parallel, Distrib. Grid Comput.*, no. 4, pp. 306–311, 2018, doi: 10.1109/PDGC.2018.8745722.

[7] A. Selwal, S. K. Gupta, Surender, and Anubhuti, "Performance analysis of template data security and protection in biometric systems," *2015 2nd International Conference on Recent Advances in Engineering & Computational Sciences (RAECS)*, 2015, pp. 1-6, doi: 10.1109/RAECS.2015.7453302.

[8] S. S. Ali, I. I. Ganapathi, and S. Prakash, "Robust technique for fingerprint template protection," *IET Biometrics*, vol. 7, no. 6, pp. 536–549, 2018, doi: 10.1049/iet-bmt.2018.5070.

[9] A. Selwal and S. K. Gupta, "Low overhead octet indexed template security scheme for multi-modal biometric system," *Journal of Intelligent & Fuzzy Systems*, vol. 32, no. 5, pp. 3325-3337, 2017, doi: 10.3233/JIFS-169274.

[10] R. Mehmood and A. Selwal, "Polynomial based fuzzy vault technique for template security in fingerprint biometrics," *International Arab Journal Of Information Technology*, vol. 17, no. 6, pp. 926–934, 2020.

[11] A. S and K. S. Anil Kumar, "Security and performance enhancement of fingerprint biometric template using symmetric hashing," *Comput. Secur.*, vol. 90, 2020, doi: 10.1016/j.cose.2020.101714.

[12] E. Liu, H. Zhao, J. Liang, L. Pang, H. Chen, and J. Tian, "Random local region descriptor (RLRD): a new method for fixed-length feature representation of fingerprint image and its application to template protection," *Futur. Gener. Comput. Syst.*, vol. 28, no. 1, pp. 236–243, 2012, doi: 10.1016/j.future.2011.01.001.

[13] W. J. Wong, A. B. J. Teoh, Y. H. Kho, and M. L. Dennis Wong, "Kernel PCA enabled bit-string representation for minutiae-based cancellable fingerprint template," *Pattern Recognit.*, vol. 51, pp. 197–208, 2016, doi: 10.1016/j.patcog.2015.09.032.

[14] S. Wang, G. Deng, and J. Hu, "A partial Hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations," *Pattern Recognit.*, vol. 61, pp. 447–458, 2017, doi: 10.1016/j.patcog.2016.08.017.

[15] S. Wang, W. Yang, and J. Hu, "Design of alignment-free cancelable fingerprint templates with zoned minutia pairs," *Pattern Recognit.*, vol. 66, pp. 295–301, 2017, doi: 10.1016/j.patcog.2017.01.019.

[16] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "A robust and non-invertible fingerprint template for fingerprint matching system," *Forensic Sci. Int.*, vol. 288, pp. 256–265, 2018, doi: 10.1016/j.forsciint.2018.04.045.

[17] K. Atighehchi, L. Ghammam, M. Barbier, and C. Rosenberger, "GREYC-Hashing: Combining biometrics and secret for enhancing the security of protected templates," *Futur. Gener. Comput. Syst.*, vol. 101, pp. 819–830, 2019, doi: 10.1016/j.future.2019.07.022.

[18] J. B. Kho, J. Kim, I. J. Kim, and A. B. J. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognit.*, vol. 91, pp. 245–260, 2019, doi: 10.1016/j.patcog.2019.01.039.

[19] J. B. Kho, A. B. J. Teoh, W. Lee, and J. Kim, "Bit-string representation of a fingerprint image by normalized local structures," *Pattern Recognit.*, vol. 103, p. 107323, 2020, doi: 10.1016/j.patcog.2020.107323.

[20] I. J. Jacob, P. Betty, P. E. Darney, S. Raja, Y. H. Robinson, and E. G. Julie, "Biometric template security using DNA codec based transformation," *Multimed. Tools Appl.*, vol. 80, no. 5, pp. 7547–7566, 2021, doi: 10.1007/s11042-020-10127-w.

[21] S. S. Ali, I. I. Ganapathi, S. Prakash, P. Consul, and S. Mahyo, "Securing biometric user template using modified minutiae attributes," *Pattern Recognit. Lett.*, vol. 129, pp. 263–270, 2020, doi: 10.1016/j.patrec.2019.11.037.

[22] S. M. Abdullahi, H. Wang, and T. Li, "Fractal coding-based robust and alignment-free fingerprint image hashing," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2587–2601, 2020, doi: 10.1109/TIFS.2020.2971142.

[23] M. Shahzad, S. Wang, G. Deng, and W. Yang, "Alignment-free cancelable fingerprint templates with dual protection," *Pattern Recognit.*, vol. 111, p. 107735, 2021, doi: 10.1016/j.patcog.2020.107735.

[24] T. Tan, "CASIA-FingerprintV5," National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Nov., 2016, http://biometrics.idealtest.org/index.jsp.

[25] G. Fiumara, P. Flanagan, J. Grantham, K. Ko, K. Marshall, M. Schwarz, E. Tabassi, B. Woodgate, and C. Boehnen (2018), "National Institute of Standards and Technology Special Database 302: Nail to Nail Fingerprint Challenge," *NIST Technical Note 2007*, https://doi.org/10.6028/NIST.TN.2007.