A Brief Overview of Hybrid Schemes for Biometric Fingerprint Template Security

Edwin T. L. Rampine and Cynthia H. Ngejane
Modelling and Digital Sciences, Council for Scientific and Industrial Research, Pretoria, South Africa

Keywords: Fingerprint, Biometric Systems, Template Protection, Cancelable Biometrics, Biometric Cryptosystem, Hybrid.

Abstract: Biometric systems are vastly adopted and consolidated into various information and security systems. Hence, it is vital that these biometrics-based systems be immune to attacks. Fingerprint template protection is a critical part of fingerprint based biometric systems. A significant number of fingerprint template protection schemes have been published. However, none of the existing protection schemes can satisfy all security requirements for template protection. Hence more researchers are combining these single schemes to create more robust hybrid schemes. In this paper we present an overview of some of the various proposed hybrid schemes for fingerprint template security. We also present their general performance results. Our goal is to briefly report on this growing interest in creating a fully secure biometric hybrid scheme, and show some of the proposed solutions in the literature so far.

1 INTRODUCTION

The term biometrics is defined by (Jain et al., 2004) as automatic recognition and analysis of individuals based on their unique physical and other traits, such as fingerprints, DNA, irises, voice patterns, facial patterns and hand gestures. Biological as well as behavioral biometric characteristics are obtained during a process called enrollment, by employing specialized sensors and unique feature extraction algorithms to create and store biometric templates. During the process of recognition, the system processes a query biometric input and compares it to the stored template, employing matching algorithms to yield an acceptance or rejection result.

The subject of biometric template security has gained value due to concerns about the likely misuse of stolen templates. (Cappelli et al., 2007) reported that the most persistent attack resulting from stolen biometric templates is spoofing. If an attacker manages to steal an unsecured stored templates, he can create a biometric spoof from the template and gain unauthorised access or deny access to legitimate users to a system. This is also made possible because of the limited liveness detection capability of most biometric systems (Nagar et al., 2008). Moreover, in instances where generic encryption methods (like AES, RSA, etc) are used, the comparison of biometric templates is not performed in the encrypted domain , thus, the templates can be vulnerable during every recognition transaction while they are decrypted (Nagar et al., 2008). Hence the vast research efforts in creating alternative protection methods or schemes to ensure biometric template security.

Biometric template protection schemes, which are generally categorized as biometric cryptosystems and feature transformation, are designed to have specific security properties (Ratha et al., 2007). These schemes provide various algorithms attempting to secure the user's biometric data. Deployment of a single scheme may not be sufficiently secure to meet all security requirements. Hence a combination of these may be required to enhance security (Feng et al., 2008), (Liu et al., 2014). A notable number of researchers have stated that a single scheme which is completely secure does not exist yet, and thus a growing interest in creating hybrid schemes to attempt to improve the security of biometric templates. In this paper, we present a brief overview of some of these proposed hybrid schemes. We report on various hybrid schemes presented in the literature so far and summarize some of their security performance contributions.

The remainder of the paper is structured as

Rampine, E. and Ngejane, C.
A Brief Overview of Hybrid Schemes for Biometric Fingerprint Template Security.
DOI: 10.5220/0005730503400346
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 340-346
ISBN: 978-989-758-167-0

follows: Sect. 2 gives a brief overview of commonly known schemes. In Sect. 3 we list the security properties that each scheme must fulfil. In Sect. 4, the surveyed hybrid schemes are presented. And before concluding in Sect. 6, Sect. 5 presents summary of hybrid schemes performances.

2 FINGERPRINT TEMPLATE SECURITY SCHEMES

Fingerprint template security schemes documented in the literature can be divided into two main categories, namely, feature transformation and biometric cryptosystems as depicted in Figure 1 below.

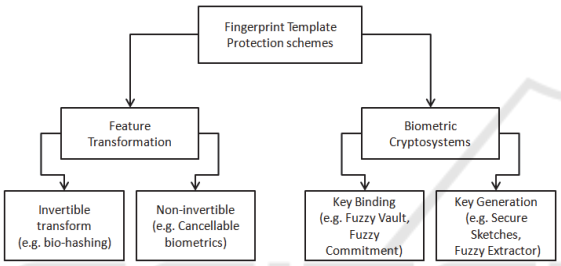

Figure 1: Classification of biometric template protection schemes.

(Ratha et al., 2001) and (Vacca, 2007) define feature transformation as an irreversible but repeatable distortion of a biometric template based on a chosen transform. The biometric template signal is distorted with the same transform at each presentation, for enrollment and for every verification. The transformed templates never need to be decrypted because the matching of the stored/enrolled templates and query templates is performed in the transformed domain.

On the other hand, biometric cryptosystems either create secure templates, also referred to as secure sketches, by using cryptographic keys or directly generating the cryptographic keys from the enrolled biometric templates (Ulaganathan and Baskaran, 2015). If a non-genuine authentication query is presented, it becomes computationally hard to reconstruct the template from the secure sketch. Whereas, given an authentication query template that sufficiently matches the enrolled template, it should be easy to decode the sketch and recover the template. A biometric cryptosystem secures the biometric template and also handles the secure key management (Jain et al., 2013).

2.1 Feature Transformation

(Jain et al., 2013) explained that in Feature Transformation techniques, the biometric template (x^{-E}) is modified with a user specific key (yt) such that the original template is irrecoverable from the transformed template (yt). During verification, the same transformation is applied to the biometric query (x^{A}) and the matching is performed in the transformed space to avoid recovery of the original biometric template. Since the key (kt) needs to be in the same storage system with (yt), the template security is assured only if the transformation method is non-invertible even when (kt) is compromised (Jain et al., 2013). However, in other techniques of feature transformation known to be invertible transforms, the key (kt) can be used to recover the original biometric template (Beng and Hui, 2010). Some established examples of template transformation include Bio-Hashing (invertible) and cancellable biometrics (non-invertible) (Teoh et al., 2007), (Ratha et al., 2007).

2.1.1 Bio-hashing

Bio-hashing is defined (Mwema et al., 2015) as a biometric template security technique in which features from a biometric template are transformed using a transformation function defined by a cryptographic key known only to the user. This key or token is securely stored and remembered by the user for subsequent authentication. However, the performance of bio-hash can degrade and the secure template be reverted to the original state if the genuine token is stolen and used by the impostor to pose as the genuine user (Teoh et al., 2008).

For any invertible transform function $y = f(x)$, we can derive $x = f^{-1}(y)$ where f^{-1} is the inverse of f. From the security point of view, invertible transforms can be easily circumvented when the transformation used is known by the attacker (Cheung et al., 2005). There are some existing proposals in the literature on how to improve the non-invertibility of bio-hashing transforms. (Teoh et al., 2008) demonstrated for instance that, the use of multi-state bio-hash transforms can resolve the stolen-token problem. Bio-hashing is an instance of Biometric Salting (Rathgeb and Uhl, 2011). (Savvides et al., 2004) denotes Biometric salting as transforms which can be invertible.

2.1.2 Cancellable Biometrics

Cancellable biometrics, according to (Jin and Lim, 2010), refers to the methodically reproducible

distortion of biometric features used to secure a transformed biometric template. If a cancellable transformed biometric template is compromised, the distortion/transformation characteristics can be replaced, and the same biometrics is mapped to a new transformation template, which can used subsequently (Radha and Karthikeyan, 2011).

For non-invertible transforms, non-invertibility improves the security of the biometric template by resetting the order or position of the feature set with a transformation process. However, this degrades the performance of the transformed features due to the enlargement of intra-user variation in the biometrics. Hence, it is challenging to create a non-invertible transformation process that satisfies both performance and non-invertibility (Jin and Lim, 2010).

2.2 Biometric Cryptosystem

Biometric cryptosystems techniques employ the use of extra biometric reliant information that can be made public referred to as helper data. This helper data is used to either retrieve or generate cryptographic keys. The biometric matching process is performed by validating the generated key, where the result of the process is either a key or a match or no match result (Ramu and Arivoli, 2012).

(Uludag et al., 2004) stated that cryptographic keys are long and random, they are difficult to predict or hack. Moreover, the cryptographic keys can be stored locally or centrally and are accessed by authorized users only. Depending on the kind of helper data derived, Biometric cryptosystems can be categorized as key-binding or key-generation systems, see Figure 2 (Ramu and Arivoli, 2012).

2.2.1 Key-binding

In key-binding, helper data is created by combining a secret key with the biometric template. During authentication, the cryptographic key can be retrieved from the helper data. (Ramu and Arivoli, 2012) stated that the cryptographic keys are revocable because they are not dependent of the biometric information, but to update the key would require a complete reenrollment to create new helper data.

(Juels and Wattenburg, 1999) proposed Fuzzy commitment scheme, which is now a well-known example of the key binding cryptosystem.

Distributed source coding (Draper et al., 1999), Fuzzy vault (Juels and Wattenburg, 1999) and Reliable components schemes (Tuyls et al., 2005) are among a number of other template protection schemes that were proposed and can be considered to be key binding approaches.

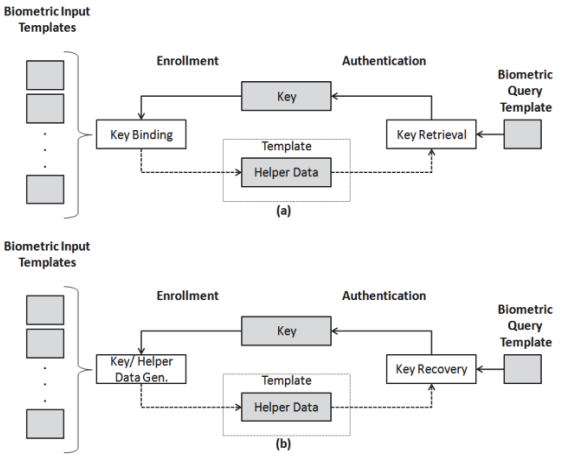

Figure 2: Overview concept of the Key generation cryptosystem (a) Key-binding and (b) Key-generation (adapted from (Ramu and Arivoli, 2012)).

2.2.2 Key-generation

In key-generation, helper data is created only and directly from the enrolled biometric template. The cryptographic keys are generated from the created helper data. The proposed schemes that allow secure keys to be generated from the helper data are fuzzy extractors and secure sketches, both are defined further by (Dodis et al., 2004) and (Verbitskiy et al., 2010).

A secure sketch solves the problem of error tolerance. It generates a random and unique bit string from the enrolled biometric template, that, and only reveals limited information about the enrolled template. It also allows the exact reconstruction of the enrolled template from any other input query template that is sufficiently close. Due to the error tolerance of this technique, it can only be effective with a lower level of variance of the subsequent query templates. A secure sketch, however, does not address nonuniformity of inputs (Dodis et al., 2004).

On the other hand, a fuzzy extractor solves both error tolerance and nonuniformity issues. It generates a uniformly random bit string from the enrolled biometric template with error tolerance. If the subsequent query templates change but remain close, the subsequent generated bit string remains exactly the same (Verbitskiy et al., 2010).

During authentication, a bit string (stored as helper data) is generated from the query biometric template, and the stored helper data is used to reconstruct the enrolled template bit string. If the

distance between the query biometric template and the enrolled biometric template is less than a specified parameter, given a query biometric template and the helper data from enrollment, the user will be accepted (Li, 2009).

3 FINGERPRINT TEMPLATE SECURITY SCHEMES

Biometric template protection schemes are designed to try and ideally fulfil the following four properties (Rathgeb and Uhl, 2010).

i) Diversity: the secure biometric template must enforce privacy by not being cross-matchable across databases.

ii) Revocability: it should be possible and straightforward to revoke a compromised biometric template and reissue a new one using the same biometric data.

iii) Irreversibility: It must be computationally hard to obtain the original biometric template from the secure template. This property prevents an attacker from creating a physical spoof of the biometric trait from a stolen template.

iv) Accuracy: the biometric template protection scheme should not degrade the recognition performance (False Acceptance Rate and False Rejection Rate) of the biometric system.

According to (Nagar et al., 2008), most existing approaches fulfil the above properties partially. It is indeed challenging to design a secure and high performance scheme that also meets the requirements of diversity and revocability. The major challenge is handling the intrauser variability in the acquired biometric data, since multiple acquisitions of the same biometric data do not result in the same feature set (Campisi, 2013).

4 OVERVIEW OF PROPOSED HYBRID SCHEMES

There are limitations reported on individual schemes. A single scheme is not sufficient to satisfy all the template protection requirements (Chen and Chen, 2010); (Ghany et al., 2012); (Liu et al., 2014), (Feng et al., 2008). Due to this, there are a number of hybrid schemes for fingerprint template security proposed in the literature. A hybrid biometric scheme is a combination of two or more biometric template protection schemes. The combination of the schemes is designed to meet more, ideally all, of the biometric protection requirements.

The following are some of the proposed hybrid fingerprint template protection schemes in the literature, and are not ranked in any way.

4.1 Fuzzy Vault and Password Hardening

(Nandakumar et al., 2007) proposed a hybrid approach where the biometric features are hardened using password before applying fuzzy vault technique. During authentication, the user needs to give both the password and the biometric data. The fuzzy vault scheme secures the template storage by binding the template with a uniformly random key, but the non-uniform trait of biometric data can reduce the vault security.

Advantages of the proposed fuzzy vault password-based hardening hybrid technique include revocability, prevention of cross-matching, improved vault security and a reduction in the False Accept Rate of the system without significantly affecting the False Reject Rate.

4.2 Cancelable Biometrics and Secure Sketches

(Bringer et al., 2008) introduced a hybrid scheme composed of Cancelable biometrics and Secure sketches. Their aim was to improve the security of the fingerprint templates while keeping the matching performance high. The cancelable biometrics technique is used to perform an irreversible transformation on biometric data, and attempt to perform matching in the transformed domain. According to (Bringer et al., 2008), the limitation of this techniques is that during transformation, the core structure of the template is modified, which leads to reduced performance accuracy.

However, for Secure sketches, matching relies on an error correction parameter. So by applying secure sketch with error correction to cancelable biometrics, allows the retention of good matching performance. Furthermore, the security advantages of both schemes are proved to accumulate.

4.3 Fuzzy Vault, Fuzzy Commitment and Minutiae Descriptors

(Nagar et al., 2010) proposed a hybrid scheme which uses the fuzzy vault scheme, fuzzy commitment scheme and incorporating minutiae descriptors in order to improve the recognition performance as

well as the security. They incorporated minutiae descriptors by embedding them in the vault construction using the fuzzy commitment technique. The minutiae descriptors capture ridge orientation and frequency information in a minutia's neighborhood.

They also experimentally demonstrated that by including the use of minutiae descriptors, the False Match Rate is reduced exponentially without degrading the Genuine Accept Rate significantly.

4.4 Key-generation and Cancelable Biometrics

(Lalithamani and Soman, 2009) discusses an effective scheme for generating irrevocable cryptographic keys from cancelable fingerprint templates. They initially extract minutiae points from the fingerprint image, then apply a cancelable biometric algorithm to get a cancelable fingerprint template. Thereafter, an irrevocable cryptographic key is generated from the cancelable fingerprint template.

The security of the proposed hybrid scheme is improved by two strong features; cancelable transformation and irreversibility. (Lalithamani and Soman, 2009) report that with the proposed scheme, in a case where the secure template is compromised, it can be cancelled and reissued with a different transformation parameters. Moreover, it is not possible to cross match the template across databases. They also indicate the inherent irrevocable nature of the scheme ensures that it is impractical to recover the cancelable template from the generated cryptographic key.

4.5 Fuzzy Vault and Regional Transformation

(Chen and Chen, 2010) proposed a hybrid scheme that combines biometric encryption (key-binding) and feature transformation (noninvertible), which is more secure than any single approach. For the biometric encryption, they apply fuzzy vault using a linear equation and chaff points on fingerprint template. Then for the noninvertible transformation, they apply a regional transformation for every minutia-centered circular region. The hybrid scheme enhances security, diversity, and revocability.

4.6 Minutiae Cylinder Code and Random Key

A hybrid scheme combining a transformation and a user key was proposed by (Mirmohamadsadeghi and Drygajlo, 2013) to provide the MCC-based fingerprint representation with improved security properties. They used a baseline fingerprint descriptor by employing minutiae cylinder code which provides rotation and translation invariant descriptors for accurate recognition. The main benefits of this hybrid technique is revocability, irreversibility and also reduces the size of the resulting template by half. Even if the key is stolen, the original biometric data remains protected (Mirmohamadsadeghi and Drygajlo, 2013).

5 PERFORMANCE RESULTS PRESENTATION OF VARIOUS HYBRID SCHEMES

5.1 Evaluation of Biometric Systems Performance

Several types of indexes are used to analyze and evaluate biometric systems performance. The following provides the common used indexes as basic measures of accuracy of a biometric system.

i) False Acceptance Rate (FAR): is the estimated probability at which a biometric sample will be incorrectly declared to belong to the claimed identity when it actually belongs to a different identity (false positive) (Valencia, 2003), FAR is also referred to as False Match Rate (FMR).

ii) False Rejection Rate (FRR): is the estimated probability at which a biometric sample will be incorrectly rejected as a claimed identity when it actually belongs to that identity (false negative) (Valencia, 2003), FRR is also referred to as False Non-Match Rate (FNMR).

iii) Equal Error Rate (EER): is the point at which FMR is equal to FNMR (Maio, Maltoni, Cappelli, Wayman and Jain, 2002).

iv) Genuine Accept Rate: The Genuine Accept Rate (GAR), also referred to as True Accept Rate (TAR), is an alternative to FRR. It is computed as 1 - FRR (Gamassi et al., 2004).

5.2 Biometric Hybrid Schemes Performance

Some hybrid schemes have been experimentally proven to reduce the FAR of a biometric system without significantly affecting the FRR. Other researchers presented hybrid schemes that are

designed to allow the retention of good matching performance. Table 1 below presents a summary of performance results presented in the proposals of the various hybrid schemes.

Table 1: Presentation of various Hybrid Schemes Performance Results.

Proposed by	Hybrid Scheme Components Used	Databases Used	Performance Results
Nandakuma, K. et al (2007) [36]	Fuzzy vault and password hardening	FVC2002 DB2	GAR = 81% FAR = 0%
		MSU-DBI	GAR = 73.8% FAR = 0%
Julien, B. et al. (2008) [38]	Cancelable biometrics and Secure sketch	FVC2000 DB2	FRR = 3% FAR = 5.53% ERR = 1.4%
Nagar, A et al. (2009) [35]	Fuzzy vault, Fuzzy commitment and Minutiae descriptors	FVC2002 DB2	GAR = 95% FAR = 0.01% FRR = 5%
Chen, H. et al. (2010) [29]	Fuzzy vault and Regional transformation	FVC2002 DB2	EER = 8.5%
Leila, M. et al. (2013) [37]	Minutiae cylinder code and Random key	FVC2002 DB1	FRR = 0.67% FAR = 1.39% EER = 0.72%

It should be noted that the results above were not found using the same data sets by various researchers, therefore no direct performance comparison can be made. The aim of the presentation of the results above is to report on the proven retention of accuracy while improving template security by these hybrid schemes.

6 CONCLUSION

We have presented various hybrid schemes for fingerprint template protection. Numerous researchers have stated the use of a single biometric template security approach may not be enough to meet all security requirements. Hence, hybrid schemes continue to be developed and tested. For each proposed hybrid scheme, experiments show that there is an improvement in the overall performance of the biometric system. We also listed the security requirements that each scheme must meet, and we finally presented the specific performance matrices measured for the various hybrid schemes.

REFERENCES

Jain, A. K., Ross, A., & Prabhakar, S., 2004. An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on, 14(1), 4-20.*

Cappelli, R., Maio, D., Lumini, A., & Maltoni, D., 2007. Fingerprint image reconstruction from standard templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(9), 1489-1503.*

Nagar, A., Nandakumar, K., & Jain, A. K., 2008. Securing fingerprint template: Fuzzy vault with minutiae descriptors. *In Pattern Recognition, 2008. ICPR 2008. 19th International Conference on (pp. 1-4). IEEE.*

Feng, Y. C., Yuen, P. C., & Jain, A. K., 2008. A hybrid approach for face template protection. *In SPIE Defense and Security Symposium (pp. 694408-694408). International Society for Optics and Photonics.*

Liu, H., Sun, D., Xiong, K., & Qiu, Z., 2014. A hybrid approach to protect palmprint templates. *The Scientific World Journal, 2014.*

Ratha, N. K., Connell, J. H., & Bolle, R. M., 2001. Enhancing security and privacy in biometrics-based authentication systems. *IBM systems Journal, 40(3), 614-634.*

Vacca, J. R., 2007. Biometric technologies and verification systems. Butterworth-Heinemann.

Ulaganathan, P., & Baskaran, J., 2015. Betterment of Fingerprint Template Protection Schemes–A Review. *In International Journal on Recent and Innovation Trends in Computing and Communication, ISSN: 2321-8169, Vol. 3 Issue: 2, pp 165–171.*

Jain, A. K., Nandakumar, K., & Nagar, A., 2013. Fingerprint Template Protection: From Theory to Practice. *In Security and Privacy in Biometrics (pp. 187-214). Springer London.*

Andrew Teoh Beng Jin and Lim Meng Hui, 2010 Cancelable biometrics. *Scholarpedia, 5(1):9201.*

Teoh, A. B. J., Toh, K. A., & Yip, W. K., 2007. 2^ N discretisation of biophasor in cancellable biometrics. *In Advances in Biometrics (pp. 435-444). Springer Berlin Heidelberg.*

Ratha, N. K., Chikkerur, S., Connell, J. H., & Bolle, R. M., 2007. Generating cancelable fingerprint templates. *Pattern Analysis and Machine Intelligence, IEEE Transactions on, 29(4), 561-572.*

Mwema, J., Kimwele, M., & Kimani, S., 2015. A Simple Review of Biometric Template Protection Schemes Used in Preventing Adversary Attacks on Biometric Fingerprint Templates. *International Journal of Computer Trends and Technology, 20(1), 12-18.*

Teoh, A. B., Kuan, Y. W., & Lee, S., 2008. Cancellable biometrics and annotations on biohash. *Pattern recognition, 41(6), 2034-2044.*

Cheung, K. H., Kong, A. W. K., You, J., & Zhang, D., 2005. An Analysis on Invertibility of Cancelable Biometrics based on BioHashing. *In CISST (Vol. 2005, pp. 40-45).*

Radha, N., & Karthikeyan, S., 2011. An evaluation of fingerprint security using noninvertible biohash. *International Journal of Network Security & Its Applications (IJNSA), 3(4).*

Ramu, T., & Arivoli, T., 2012. Biometric Template

Security: An Overview. *In Proceedings of International Conference on Electronics (Vol. 65).*

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K., 2004. Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE, 92(6), 948-960.*

Juels, A., & Wattenberg, M., 1999. A fuzzy commitment scheme. *In Proceedings of the 6th ACM conference on Computer and communications security (pp. 28-36). ACM.*

Draper, S. C., Khisti, A., Martinian, E., Vetro, A., & Yedidia, J. S., 2007. Using distributed source coding to secure fingerprint biometrics. *In Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on (Vol. 2, pp. II-129). IEEE.*

Juels, A., & Sudan, M., 2006. A fuzzy vault scheme. *Designs, Codes and Cryptography, 38(2), 237-257.*

Tuyls, P., Akkermans, A. H., Kevenaar, T. A., Schrijen, G. J., Bazen, A. M., & Veldhuis, R. N., 2005. Practical biometric authentication with template protection. *In Audio-and Video-Based Biometric Person Authentication (pp. 436-446). Springer Berlin Heidelberg.*

Dodis, Y., Reyzin, L., & Smith, A., 2004. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *In Advances in cryptology-Eurocrypt 2004 (pp. 523-540). Springer Berlin Heidelberg.*

Verbitskiy, E., Tuyls, P., Obi, C., & Schoenmakers, B., 2010. Key extraction from general nondiscrete signals. *Information Forensics and Security, IEEE Transactions on, 5(2), 269-279.*

Li, S. Z., 2009. Encyclopedia of Biometrics: I-Z (Vol. 1). *Springer Science & Business Media.*

Rathgeb, C., & Uhl, A., 2010. Adaptive fuzzy commitment scheme based on iris-code error analysis. *In Visual Information Processing (EUVIP), 2010 2nd European Workshop on (pp. 41-44). IEEE.*

Jain, A. K., Nandakumar, K., & Nagar, A. (2008). Biometric template security. *EURASIP Journal on Advances in Signal Processing, 2008, 113.*

Campisi, P., 2013. Security and Privacy in Biometrics. *London: Springer.*

Chen, H., & Chen, H., 2010. A hybrid scheme for securing fingerprint templates. *International Journal of Information Security, 9(5), 353-361.*

Ghany, K. K., Hefny, H. A., Hassanien, A. E., & Ghali, N., 2012. A Hybrid approach for biometric template security. *In Advances in Social Networks Analysis and Mining (ASONAM), 2012 IEEE/ACM International Conference on (pp. 941-942). IEEE.*

Liu, H., Sun, D., Xiong, K., & Qiu, Z., 2014. A hybrid approach to protect palmprint templates. *The Scientific World Journal, 2014.*

Feng, Y. C., Yuen, P. C., & Jain, A. K., 2008. A hybrid approach for face template protection. In SPIE Defense and Security Symposium (pp. 694408-694408). *International Society for Optics and Photonics.*

Rathgeb, C., & Uhl, A., 2011. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP Journal on Information Security, 2011(1), 1-25.*

Savvides, M., Kumar, B. V. K. V., & Khosla, P. K., 2004. Cancelable biometric filters for face recognition. *In Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on (Vol. 3, pp. 922-925). IEEE.*

Nagar, A., Nandakumar, K., & Jain, A. K., 2010. A hybrid biometric cryptosystem for securing fingerprint minutiae templates. *Pattern Recognition Letters, 31(8), 733-741.*

Nandakumar, K., Nagar, A., & Jain, A. K., 2007. Hardening fingerprint fuzzy vault using password. *In Advances in biometrics (pp. 927-937). Springer Berlin Heidelberg.*

Mirmohamadsadeghi, L., & Drygajlo, A., 2013. A template privacy protection scheme for fingerprint minutiae descriptors. *In Biometrics Special Interest Group (BIOSIG), 2013 International Conference of the (pp. 1-8). IEEE.*

Bringer, J., Chabanne, H., & Kindarji, B., 2008. The best of both worlds: Applying secure sketches to cancelable biometrics. *Science of Computer Programming, 74(1), 43-51.*

Lalithamani, N., & Soman, K., 2009. An effective scheme for generating irrevocable cryptographic key from cancelable fingerprint templates. *Int. J. Comput. Sci. Netw. Secur, 9(3), 183-193.*

Valencia, V. S., 2003. Biometric Testing: It's Not as Easy as You Think'. *In Biometric Consortium Conference.*

Maio, D., Maltoni, D., Cappelli, R., Wayman, J. L., & Jain, A. K., 2002. FVC2002: Second fingerprint verification competition. *In Pattern recognition, 2002. Proceedings. 16th international conference on (Vol. 3, pp. 811-814). IEEE.*

Gamassi, M., Lazzaroni, M., Misino, M., Piuri, V., Sana, D., & Scotti, F., 2004. Accuracy and performance of biometric systems. *In Instrumentation and Measurement Technology Conference, 2004. IMTC 04. Proceedings of the 21st IEEE (Vol. 1, pp. 510-515). IEEE.*