Betterment of Fingerprint Template Protection Schemes – A Review

Pradheeba Ulaganathan
Department of Computer Science
School of Engg., and Tech., Pondicherry University
Puducherry, India.
prathiba.ulaganathan@gmail.com

Jayashree Baskaran
Department of Computer Science
School of Engg., and Tech., Pondicherry University
Puducherry, India.
jbaskaran2@gmail.com

Abstract—Biometric security threat is an issue of dynamic attack against weakness in a biometric system. While biometrics may enhance security detached situations, in the same way as some other security system, it has vulnerabilities and it is vulnerable to threats. They are defenseless to outer vulnerabilities of biometric systems so that their shortcomings can be discovered and valuable counter measures against predictable attacks can be created. In this review, we have taken different categories of template protection methods and stated the evolution, usage, merits and demerits of each category along with comparison of the metrics GAR, FAR, FRR and EER in tabular form. This paper also suggests an ideology of a hybrid scheme of fingerprint template protection that will overcome the issues faced in prior approaches.

Keywords- *fingerprint recognition; hybrid template protection; fuzzy; cancellable;*

*****

I. INTRODUCTION

Biometrics alludes to measurements identified with human characteristics and traits. Biometrics authentication (or practical authentication) is utilized as a part of computer science as a manifestation of ID and access control. It is likewise used to identify individuals in gatherings that are under reconnaissance. So focused around the application, a biometric framework may work either in verification mode or identification mode. The verification mode is for approving an individual's personality by contrasting the captured biometric information and his/her own particular biometric template(s) put away in the system database. The identification mode perceives a single person via seeking the layouts of every last one of clients in the database for a match. Fingerprint identification is the system for identification utilizing the impressions made by the minutiae ridge termination or patterns found on the fingertips. Finger print pre-processing can be defined into image enhancement, binarization and thinning. However, fingerprint matching faces numerous intrinsic dangers; particularly the protection and security attentiveness toward the biometric template and prompts privacy threats. These drive the inspiration to plan a profoundly secure and private biometric template protection method. Brute force attacks and replay attacks are the forms the most part utilized for interrupting into the unique mark database. Among these issues, securing the client template that is put away either generally or centrally is a significant concern [1].

To build the security of biometric frameworks, another class of systems, specifically template protection mechanism is required which paves way to abolish the intruder attack. This tomb biometric incorporates distinctive sort of format security traps that incorporates fuzzy vault frameworks and cancellable template protection scheme. Fuzzy extractors change over biometric information into arbitrary strings, which makes it conceivable to apply cryptographic strategies for biometric security [2]. Cancellable biometrics alludes to deliberately repeatable distortion of biometric peculiarities so as to secure delicate client particular information. On the off chance that a cancellable peculiarity is compromised, the distortion attributes are changed, and the same biometrics is mapped to another layout, which is utilized hence. But our focus is to refine these things on diversity, revocability, accuracy, invertibility. If we handle, protection with feature transformation or bio-cryptosystems, the systems lags in accuracy or the level of invertibility. So in this review paper, we discuss the different strategies that each classification has taken so far and the subsequent improvement in each category. The pitfalls in some of the methods are also shown in this survey, plus we have given a hybrid scheme of fingerprint template protection scheme that will overcome the disadvantage of both the methods.

This paper is organized as follows. Section II describes the different finger print biometric authentication techniques as shown in fig. 1. Section III discusses the hybrid system architecture that will bring a solution to the current issues. The conclusion and future work is given in section IV. Fig.1 depicts the organization of the different finger print biometric authentication systems that we dealt before the proposed architecture.

II. FINGERPRINT TEMLATE PROTECTION TECHNIQUES

Biometric template protection methods can be divided into two categories, namely, feature transformation (cancellable biometrics) and biometric cryptosystem. Biometric cryptosystem works in two ways, i.e., it either secures the cryptographic key using biometric feature or directly generates the cryptographic key from biometric feature. On the other hand, the cancellable biometrics refers to the irreversible transform of the biometric template to ensure security and privacy. Instead of the original biometric data, only the transformed templates are stored as the storage of the original image occupying large amount of memory space and it is sufficient to store a small amount of date called template, which is a distinct feature that uniquely identify a person.

A. Fuzzy vault systems

Fuzzy vault systems do not store the original template in the database. Instead, a transformed version of the template only is stored with the help of cryptography. In [3], a brief description about this biometric cryptosystems, their issues

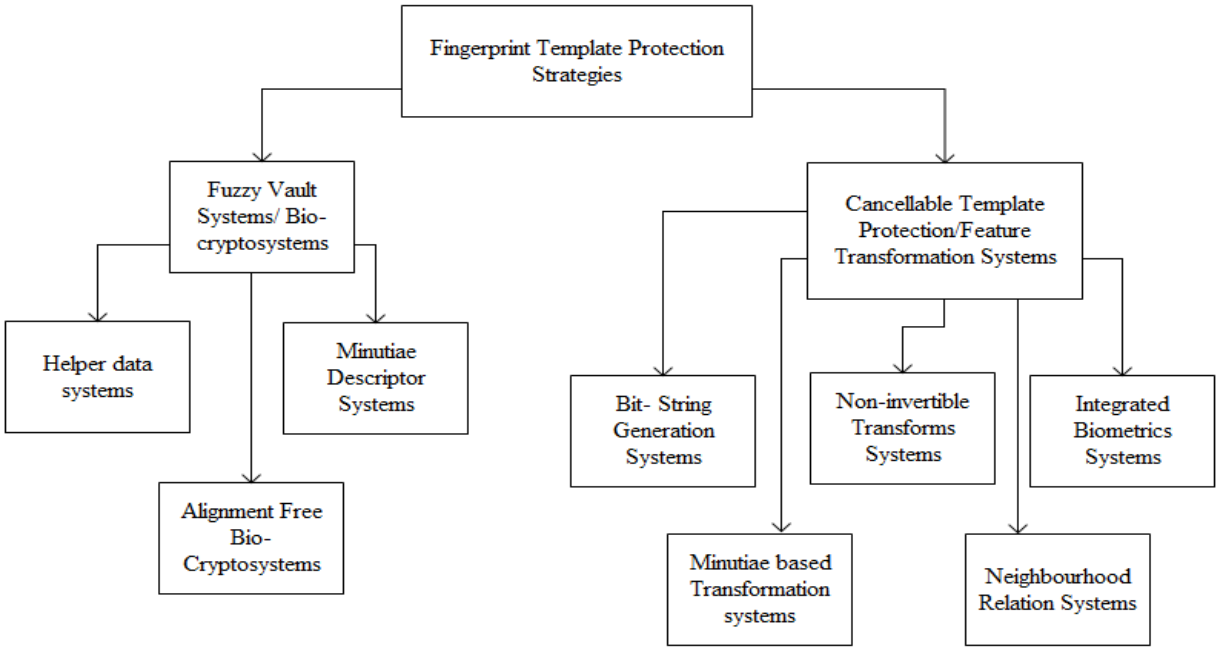

Figure 1. Classification of template protection techniques

and challenges is given. The brief introduction about fuzzy system is given by [4].

1) Introduction to Helper Data Systems

The helper data inclusion was proposed by J.P. Linnartz [5] and this is a modification made to [4] by finding a higher degree polynomial to the template which will only take the minutiae points form the genuine set. With the help of the work that are already schemed, Uludag [6] presented an implementation work of the paper by Juels et al [4] using some helper data [7] and showed how this helper data is helping to prevent the information leakage.

The system has three parts, namely, i) encoding and decoding - size of the secret key S depends on the type of data that we are locking and in their implementation, they locked the data with 128 bit key using AES symmetric encryption key. Cyclic redundancy code (CRC) is used to create as many number of candidate key set as possible. The decoding part runs with the help of CRC (after making the query minutiae to the form in which template minutiae exist) to check for errors. Once it is found that both templates are from the same finger, ii) constructing helper data - orientation field flow curves (OFFC) are obtained and curvature estimation is done and the helper data filtering is done by taking points at maximum and minimum curvature of OFFC and iii) ICP (Iterative closest point registration) based alignment - this phase is just a slight modification of the work proposed in [8]. With this, they had shown that 128-bit AES keys can be secured using the proposed architecture.

2) Fuzzy Logic with Minutia descriptors

Improvements over [4] are done through descriptors. J. Feng [9] paved a way for a matching algorithm that solves two problems: the correspondence and similarity computation. Fuzzy commitment schemes are trying to protect the biometric data by encrypting the polynomials evaluations. To this methodology, descriptors add some modification to bring more security.

Nagar et al [10] proposed a template that used fuzzy vault with minutiae descriptors. The encryption makes it difficult for an adversary to decode the vault even if the correct set of minutiae is selected. So they used minutiae descriptors - which capture orientation and ridge frequency information in a minutia's neighborhood, for securing the polynomial evaluations. Here, first they are enrolling the helper data through fuzzy vault encoder built with CRC error checker. To improve the security of vault in identifying the genuine set, the ordinate values are encrypted so that the adversary cannot reconstruct the polynomial even if he/she correctly guesses genuine points. Descriptors for chaff points are taken from database. Then an authentication system is finally employed to match two templates using XOR operation between the descriptors of both query and enrolled minutiae.

3) Alignment Free Bio-Cryptosystems

Fingerprint registration or alignment is essential to reduce intra-class variation in the unencrypted domain to compute alignment parameters. Generally, bio-cryptosystems can be divided into two categories, namely, alignment-based and alignment-free methods [11]. With the basement of Juels methods ([12],[13]), Yang et al [14] schemed a new system to solve out singular point deviation and minutiae changes using local Voronoi neighbor structures, an alignment-free bio-cryptosystem, based on fixed-length bit-string representations.

It passes through four stages, namely i) formation of VNS (Voronoi neighbor structures) ii) generation of modified VNS - for compensating local VNS structure caused by distortion iii) generation of fixed bit string representation - to represent a minutiae string using 3D array and finally iv) encrypted matching - encoding and decoding stages included to check for a match. The experimental results show that the encrypted domain has got additional security as they introduced a new scheme of encryption call PinSketch. This improved the overall performance of the bio- cryptosystem. To describe the comparison between various fuzzy vault algorithms that has evolved, we constructed the following table which contains the

information about those papers that are strictly following fuzzy logic taken.

B. *Cancellable biometrics*

Cancellable biometrics refers to systematically repeatable distortion of biometric features in order to protect sensitive user-specific data. If a cancellable feature is compromised, the distortion characteristics are changed, and the same biometrics is mapped to a new template, which is used subsequently [15]. The methods generally fall into two categories: (i) Biometric Salting and (ii) Non-invertible Transforms.

1) *Security in Non-Invertible Transforms*

K. Simoens in [16] provided a vision towards privacy weaknesses in which they put a question "whether one can undermine a user's privacy given access to biometrically encrypted documents", and they examined "if an attacker can determine whether two documents were encrypted using the same biometric". With this, they concluded the necessary conditions for the perfect distinguishability and perfect irreversibility from bounds on the adversary's advantages.

Y. Sutcu et al [17] proposed a method of one way transformation combined with secured cryptographic hash function. Actually, it is designed as a combination of various Gaussian functions to function as "robust hash". The cryptographic hash is used to secure the biometric templates stored in the database. They tested the algorithm using ORL face database and showed that, this scheme offers a valuable solution to one of the privacy and security weakness of template security.

So far, the algorithms that were proposed using cancellable domain still have some demerits. That is, they either avoid the distribution of biometric features or used an inefficient feature matching which leads to security threats. Hence, Nagar et.al [18] proposed a system for non-invertible fingerprint template transformation which takes "coverage effort curve" into account for measuring the number of guesses required by an adversary to find some portion of biometric identity. With this assumption, the non-invertible measure is calculated through three stages after performing Gaussian Transform: i) pre image identification - computing the pre-images transformed minutiae so that transformation would lead to the given transformed minutia, ii) minutiae likelihood computation - estimation of the relative probability of the minutiae transformed in the previous stage using kernel density estimation, and iii) non-invertibility measure computation: sorting the pre-images according to their likelihood and computing the coverage, i.e., the number of true pre-images guesses. As a result, the parameter setting leads to lower security risks and better matching performance.

2) *Minutiae based transforms*

Another set of work deals with minutiae based transforms under cancellable template protection. Chen, H. et al [19] gave a pragmatic work in which transform does not depend on application so that templates cannot be reused. The algorithm proceeds through three stages. The first stage is constructing circular region - each minutiae point is circled and only certain minutiae points are encrypted and stored in the distorted form. The second stage is the encryption of the circular region – all the circular regions are encrypted using non-invertible transformation using the algorithm stated in the above paper and the transformed template is stored. Third stage is matching using encrypted regions - Hong. et al.,[20] (using Alignment of Point Patterns, Aligned Point Pattern Matching phases), Jea and Govindaraju [21], (using partial fingerprint matching that consist of four stages, namely, secondary features, tolerance areas, feature matching and similarity score calculation) and Chen et al [22] (using matching algorithm that has been constructing minutia-centered circular regions, finding the first pair of corresponding regions, finding all pairs of corresponding minutiae regions) proposed methods that are meant for untransformed matching algorithms.

3) *Minutiae-based Transforms - Bit String Generation*

There are several methods proposed for protecting biometric template, yet it is not easy to design a method that satisfies the conditions as stated in Teoh, Goh and Ngo [23]: i) diversity ii) revocability iii) non-invertibility and iv) performance. After the analysis of basic requirements for these criteria, Z. Jin et. al [11] presented a method for generating a revocable fingerprint template in terms of bit-string through polar grid based 3-tuple quantization technique. The main process goes through four phase. The first phase is reference minutia based polar transform, based on chosen reference, others can be transformed and rotated. The second phase is a 3-tuple based quantization - polar grid quantisation on all minutiae. The third phase is bit-string generation and user-specific tokenized permutation - bit-string: if polar grid contains more than one minutia it is 1 otherwise 0. The final phase is matching - finding the intersection of two bit-strings. Two merits of this method are: alignment-freeness and performance.

4) *Minutiae based Transforms – Integrated Biometrics*

Fingerprint mosaicing leads to the accord of information acquired from two or more impressions of a finger by blending these impressions into a single mosaic, or by integrating the feature sets (viz., minutiae information) pertaining to these impressions which is explained in [24].

Chin et. al [25] proposed an algorithm that fused multiple biometric data at feature level to obtain integrated template to secure the fused templates using a hybrid template protection method. The proposed method is made up of two techniques known as random tiling and an equal-probable discretization scheme which can also be applied on multimodal biometrics [26]. The process starts with: i) feature level fusion, ii) random tiling and iii) feature discretization. In the beginning, a user registers his fingerprint and palm-print. The captured data will then be fused at the feature level. Based on the user-specified key, a random feature set is generated by applying random tiling.

At last, the random features are discretized to generate the bit-string. The matching module will compare the Hamming distance between the template bit-string and the query to verify.

5) *Minutiae based Transforms - Neighbourhood Relation*

Template protection can be done using the information derived from the neighborhood relation that are projected in a plane to generate string which is then encrypted using user's key. In [27], their contribution is the construction of M rectangles and multiline neighboring relation generation. They proposed an alignment free cancellable template generation by constructing M rectangles with different orientations around every reference minutiae followed by the calculation of rotation invariant and translation invariant neighboring relation, plane based quantization for bit string generation and

cancellable template generation is done with the help of neighbour minutiae found in the M rectangles to generate the multiline neighbouring relation for every minutia in the fingerprint. But some prior methods use only some minutiae whose distance is greater than the threshold that is selected for template generation [28] and after that the matching process begins. The proposed method fulfills the necessary and sufficient conditions which are the primary requirements of a cancellable template design like non-invertibility, accuracy, diversity and revocability.

III. THE PROPOSED ARCHITECTURE

This survey gives a projection of various kinds of template protection methods and their evolution through various stages. From the application perspective, it is clear that a single approach cannot solve all kind of theft issues. The selected biometric feature, its representation and intra-user variations also influences the choice of biometric template protection. In some cases, where variation in intra-user domain is huge, even a single biometric cryptosystem or non-veritable transformation won't help much. In such situations, more than one scheme can be employed. Before suggesting hybrid scheme, one should consider the biometric feature that involved in the system. Factors such as performance, memory requirements, and complexity in computation, co-operation, and user-friendly nature may also have influence in hybrid systems.

In this approach, two methods (that we have seen already in II) are combined at two stages with additional changes in the existing techniques. Enrollment is to enlist a hybrid fingerprint template protection utilizing biometric encryption and noninvertible change. On the customer side, the client checks his/her finger and gives C-Key and R-Key. On the other side, the framework first consolidates C-Key with unique finger impression particulars amid biometric encryption and afterward applies noninvertible change to the fluffy details with R-Key. The hybrid fingerprint template will be put away in the database.

A. *Enrollment phase:*

Bind C-Key to extracted original minutiae from the fingerprint. C-Key is some private key or password to be protected. We construct a multivariable linear equation, coefficients of which are determined by C-Key. C-Key is divided into *m* sub-keys, from which coefficients are generated one by one. (The entire enrolment process is given as Fig.2)

$$\text{C-Key} \Leftrightarrow (ck1, ck2, \ldots, ckn) \quad (1)$$

With the help of the above key, a polynomial equation is built and the solution for that is added to every minutia which is shown below.

$$ck1p1 + ck2p2 + \cdots + cknpn = b \quad (2)$$
$$\{(s1, mp1), (s2, mp2) \ldots (sNT, mpNT)\} \quad (3)$$

where s1,s2, . . . sNT are the solutions to the equation and p1, p2 . . . pNT are the co-efficient of those parts of the equation. Combination of these two values will give rise to C-Key.

After these duplicate points (r_{dup})are added to the original minutiae(r) to save the exact locations of minutiae points which holds the parts of the solutions of the polynomial equation. In order to avoid the overlapping of duplicate points on real minutiae that is having solution part, we have to place them with respect to the reference minutiae only when the threshold is less then fixed constant value. Here threshold refers to the maximum distance between two similar points.

$$|r_{dup} - r| > \text{threshold}(r) \quad (4)$$
$$|\theta_{dup} - \theta| > \text{threshold}(\theta) \quad (5)$$

If two points satisfies either (4) or (5) we can place the duplicate point in the coordinate. Then regional transformation has to be done. This is the second method of the template protection which needs the involvement of R-Key.

Our noninvertible transformation is described as below. (1) A circular region is built around every minutia and represented by a set of minutiae inside. The radius of regions is identical but the number of minutiae changes from region to region. (2) Regional transformation. It is a process of transform minutiae region by region. Suppose a region is represented as Reg *(r, θ, α*), then transform (Reg(*r, θ, α*), R-Key) = Reg (t1, t2) by

$$\begin{matrix} rk11, rk12, rk13 \\ rk21, rk22, rk23 \end{matrix} \mathbf{X} \begin{matrix} r \\ \theta \\ \alpha \end{matrix} = \begin{matrix} t1 \\ t2 \end{matrix} \quad (6)$$

B. *Verification Phase:*

Recognition means the performing matching in the transformed form and C-Key generation from the hybrid template. When user scans his/her finger and provides R-Key. Then the system first applies noninvertible transformation to the input minutiae with R-Key, and performs the matching in the transformed form. If the matching is successful, the system will find solutions of the linear equation, which are associated with matched minutiae, recover the original equation, and generate C-Key.

In our scheme, the system performs matching in the transformed space region by region. Let (t1, t2) be a minutia of Reg (t1, t2), which is a transformed region from the input fingerprint, (tem1, tem2) be a minutia of Reg (tem1, tem2), which is a transformed region from the template, (tem1, tem2) and (t1, t2) are matched only if

$$|t1 - tem1| \leq \text{threshold}(t1)$$
$$|t2 - tem2| \leq \text{threshold}(t2) \quad (7)$$

Reg (t1, t2) and Reg (tem1, tem2) are matched regions only if the number of matched points reaches threshold (Reg_match). Fig 3 explains the verification process. In this way both the template protection methods are used to encrypt the template and duplication is added to confuse the hacker while finding the key and only when the correct minutiae collection are found out , there occurs a match.

The algorithms discussed above are compared in the table shown below. It shows the evaluation of different template protection methods (that we have seen so far) along with the performance metrics like FAR (False Acceptance rate), FRR (False Rejection Rate), GAR (Genuine Acceptance Rate), and EER (Equal Error Rate). Almost all methods endeavourers to have less EER but it could not.

The evaluation results shows that the methods applied to one application is comparatively producing less performance. Among these vulnerabilities, an attack against stored biometric templates is a real concern because of the solid linkage

 ISSN: 2321-8169
165– 171

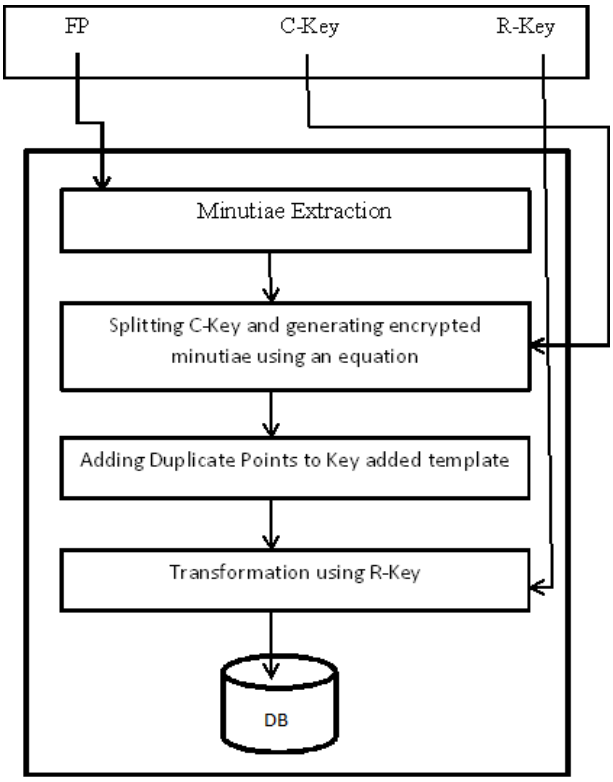

Figure 2. Enrollment Phase

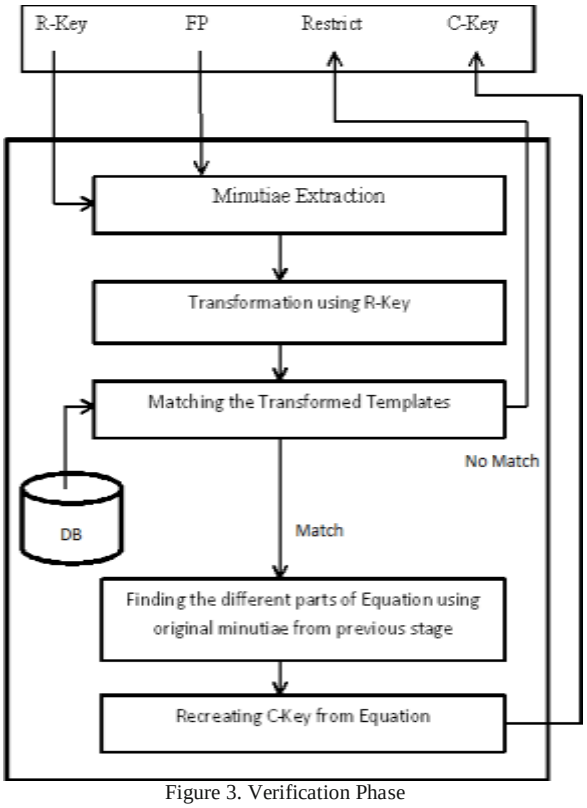

Figure 3. Verification Phase

TABLE I. EVALUATION OF VARIOUS FINGERPRINT TEMPLATE PROTECTION METHODS

Proposed BY	Methodology Used	Database Used	Success rate (GAR)	Success rate (FAR)/(FRR)	Error rate (EER)
Uludag, U. et al (2006) [6]	Fuzzy Fingerprint Vault, Constructing Helper Data, ICP based Alignment.	DB2 database of FVC 2002.	72.6%	0% FAR	-
Nagar, A., and Star, A. (2008) [10]	Helper Data Extraction, Authentication	FVC2002 DB2.	95% (degree of 6)	0.01%	-
Yang, W., Hu, J., Wang, S., and Stojmenovic, M. (2014) [14]	Formation of VNSs, Generation of modified VNSs, Generation of fixed-length bit-string representations, Encrypted matching	FVC2000DB1, all of the 4 databases) of FVC 2002, and FVC2004DB2.	-	-	14.30% 11.84% 10.38% 16.52% 15.63% 20.61%
Nagar, A., and Jain, A. K. (2009). [18]	Minutiae template transforms, non-invertibility measures.	FVC2002	92%	10%	-
Chen, H., and Chen, H. (2011) [19]	Construct circular Regions, Encrypt circular regions, Matching using encrypted regions	FVC2002 DB1 and DB2.	96.5% , 98.5% @ num level 18.	2% - DB1 2% - DB2 @ num level 18. (FAR)	-
Jin, Z., Jin Teoh, A. B. et al (2014). [11]	(PGTQ): Reference minutia based polar transform, tuple-based quantization.Bit-string generation and User-specific tokenized permutation, Matching.	FVC2002 DB1& DB2 FVC2004 DB1& DB2.	-	-	1.19% 6.94% 16.35% 8.66%
Chin, Y. J. Ong, T. S.et al (2014) [25]	Feature level fusion, Random tiling, Feature Discretization.	2 fp & 2 palm print databases. [47]	-	-	< 5%
Prasad, M. V. N. K., and Santhosh C. (2014). [27]	Multiline neighbouring relation generation, Plane based quantization and bit string generation, Cancellable template generation, Matching.	FVC 2002 DB1, DB2 and DB3.	-	-	0.62% 1.33% 2.64%

between a client's template and this character and the irreversible nature of biometric templates. That's why we have combined a fuzzy commitment scheme and robust hashing scheme in our system to achieve the desired results. These existing works already produced 95% and 98% [6, 19] of GAR so the new proposed system is expected to achieve more than these available techniques.

IV. CONCLUSION

Biometric systems are constantly and generally used to accomplish solid client validation, a discriminating part in personality administration. Anyway, biometric systems themselves are helpless against various attacks. In this paper, we have outlined different parts of biometric system security and examined systems to counter these threats.

The available template protection schemes have not yet sufficiently been developed for large scale development. They don't meet the prerequisites of assorted qualities, revocability, security and high recognition performance. So an investigation must be performed before the template security schemes are conveyed in basic true applications. A single template protection methodology may not be sufficient to meet all the application necessities. Subsequently, hybrid schemes that make utilization of the focal points of the distinctive template protection approaches must be created. Finally, with the becoming enthusiasm toward multi-biometric and multifactor verification systems, hybrid architecture is presented here which takes the advantage of both the classification template protection techniques. The future work is to implement this system to find out the betterment in template protection schemes.

V. REFERENCES

[1] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," pp. 223–228, 2001.
[2] Fuzzy Extractorlast modified 17th September 2014 [Online]. Available: http://en.wikipedia.org/wiki/Fuzzy_extractor.
[3] U. Uludag, S. Member, S. Pankanti, and S. Member, "Biometric Cryptosystems : Issues and Challenges," vol. 92, no. 6, 2004.
[4] A. Juels and M. Sudan, "A fuzzy vault scheme," Proc. IEEE Int. Symp.Inf. Theory, p. 408, 2002.
[5] J. Linnartz and P. Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," pp. 393–402, 2003.
[6] U. Uludag, "Securing Fingerprint Template : Fuzzy Vault with Helper Data ∗," 2006.
[7] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy Vault for Fingerprints," pp. 1–10,2005.
[8] G. C. Sharp, S. Member, S. W. Lee, and D. K. Wehe, "ICP Registration Using Invariant Features," vol. 24, no. 1, pp. 90–102, 2002.
[9] J. Feng, "Combining minutiae descriptors for fingerprint matching," Pattern Recognit., vol. 41, no. 1, pp. 342–352, Jan. 2008.
[10] A. Nagar and A. Star, "Securing Fingerprint Template : Fuzzy Vault with Minutiae Descriptors ∗," pp. 2–5, 2008.
[11] 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, May 2012.
[12] A. Juels, C. Drive, M. Wattenberg, and W. Street, "A Fuzzy Commitment Scheme," pp. 28–36.
[13] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," Des. Codes Cryptogr., vol. 38, no. 2, pp. 237–257, Feb. 2006.
[14] W. Yang, J. Hu, S. Wang, and M. Stojmenovic, "An alignment-free fingerprint bio-cryptosystem based on modified Voronoineighbour structures," Pattern Recognition., vol. 47, no. 3, pp. 1309–1320, Mar. 2014.
[15] Cancellable Biometrics, Andrew TeohBeng Jin and Lim MengHui (2010) [Online]. Available: http://www.scholarpedia.org/article/ Cancelable_biometrics
[16] K. Simoens, P. Tuyls, and B. Preneel, "Privacy Weaknesses in Biometric Sketches," 2009 30th IEEE Symp.Secur. Priv., pp. 188–203, May 2009.
[17] Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric Multimedia authentication scheme based on robust hashing," Proc. 7th Work. Secure. - MM&Sec '05, p. 111, 2005.
[18] A. Nagar and A. K. Jain, "On the security of non-invertible fingerprint template transforms Abhishek Nagar and Anil K . Jain ∗ Department of Computer Science and Engineering Michigan State University," pp. 81–85, 2009.
[19] H. Chen and H. Chen, "A novel algorithm of fingerprint encryption using minutiae-based transformation," Pattern Recognit. Lett., vol. 32, no. 2, pp. 305–309, Jan. 2011.
[20] L. Hong and E. Lansing, "On-Line Fingerprint Verification," pp. 596–600, 1996.
[21] T.-Y. Jea and V. Govindaraju, "A minutia-based partial fingerprint recognition system," Pattern Recognit., vol. 38, no. 10, pp. 1672–1684, Oct. 2005.
[22] H. Chen, H. Sun, and K. Lam, "A fast and elastic fingerprint matching algorithm using minutiae-centered circular regions," pp. 211–215, 2007.
[23] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs.," IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 1892–901, Dec. 2006.
[24] A. Ross, S. Shah, and J. Shah, "Image versus feature mosaicing : A case study in fingerprints," no. April, 2006.
[25] Y. J. Chin, T. S. Ong, a. B. J. Teoh, and K. O. M. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," Inf. Fusion, vol. 18, pp. 161–174, Jul. 2014.
[26] Y. J. Chin, T. S. Ong, A. B. J. Teoh, and M. K. O. Goh, "Multimodal biometrics based bit extraction method for template security," 2011 6th IEEE Conf. Ind. Electron. Appl., pp. 1971–1976, Jun. 2011.
[27] M. V. N. K. Prasad and C. Santhosh Kumar, "Fingerprint template protection using multiline neighboring relation," Expert Syst. Appl., vol. 41, no. 14, pp. 6114–6122, Oct. 2014.
[28] K. Nandakumar, S. Member, and A. K. Jain, "Fingerprint-Based Fuzzy Vault : Implementation and Performance," vol. 2, no. 4, pp.744–757, 2007.
[29] H. Yang and A. C. Kot, "Pattern-Based Data Hiding for Binary Image Authentication by Connectivity-Preserving," IEEE Trans. Multimed., vol. 9, no. 3, pp. 475–486, Apr. 2007.
[30] S. Li and A. C. Kot, "Privacy Protection of Fingerprint Database," IEEE Signal Process.Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.
[31] S. Li, S. Member, and A. C. Kot, "Fingerprint Combination for Privacy Protection," vol. 8, no. 2, pp. 350–360, 2013.

ISSN: 2321-8169
165– 171