AN EVALUATION OF FINGERPRINT SECURITY USING NONINVERTIBLE BIOHASH

N.Radha[1] and S.Karthikeyan[2]
[1]Department of Computer Science, Karpagam University,Tamil Nadu
lakshmin02@sify.com
[2]Department of Information Technology,College of Applied Sciences,
Sohar, Sultanate of Oman
skaarthi@gmail.com

ABSTRACT

Biometric analysis for identifying verification is becoming a widespread reality. It is a very challenging and tedious task to develop a biometric template protection scheme which is anonymous, revocable and noninvertible while maintaining decent performance. Cancellable biometrics is one of the best methods used to resolve this problem. In this paper, a new method called as BioHashing which follows the technique of cancellable biometrics in the fingerprint domain is proposed. This proposed method does not require the re-alignment of fingerprints as all the minutiae are translated into a pre-defined two dimensional space based on a reference minutia. After that, the proposed Biohashing method is used to enforce the one-way property (non-invertibility) of the biometric template. The proposed approach is very much resistant to minor translation error and rotation distortion. An Equal Error Rates (EER) of less than 1% is achieved in this approach and performance of the approach is also significant.

KEYWORDS

Biohashing, Fingerprint Biometrics, Cancellable Biometrics, Non-Invertible Transformation

1. INTRODUCTION

Biometric approaches for the identification of the authorized users are becoming a widespread reality. These approach necessitate large-scale capture and storage of biometric data, which raises serious issues in terms of data privacy and (if such data is compromised) identity theft. These problems can be solved by the usage of biometric data, which unlike other traditional authentication methods like secret passwords or physical tokens cannot be refreshed or reissued if compromised. Cancellable biometrics [4] technique was introduced to denote biometric templates that can be cancelled and replaced. BioHashing technique was introduced as a form of cancellable or replaceable biometrics, in which a set of user-specific random numbers are integrated with biometric features to address the problem of privacy and security.

Fingerprint is a strong biometric feature in terms of its recognition performance, both theoretically and empirically. However, the security and data privacy in traditional fingerprint biometric techniques are not significant [19]. Although the digital encoding of a fingerprint pattern can be encrypted, if the encryption is ever broken the true biometric feature is lost forever. In the same way, by using the Trojan horse type attack, the true biometric feature can be harvested at the matching stage when the system has already decrypted it. The fingerprint feature can be feasibly used in a replay attack to break into the system, if the true fingerprint is disclosed. In worst cases, the same true fingerprint could possibly be used to break into other, unrelated systems that were also keyed to the person's fingerprint. This results in insecurity and the privacy of the data is also not protected. There may also be a problem that the same fingerprint can be used to illegally gain access to multiple databases, such database cross matching [24] may also be performed for gathering business intelligence. The individual would have far more privacy if each of the databases was keyed to incompatible fake fingerprints derived from the true fingerprint of the user.

DOI : 10.5121/ijnsa.2011.3411

Usually in assessment of the fingerprint [27] biometric systems High false rejection of valid users is often neglected which results in low false acceptation. Denial of access [20] in the biometric approaches can have a great impact on the usability of the system as it fails to identify an authorized user. This will greatly affect the public acceptance of biometrics in the emerging technology. The technique of Multimodal biometrics can significantly reduce the probability of denial of access without sacrificing the false acceptation performance. In order to solve the problem of high false rejection, a novel two-factor authenticator technique is proposed which is based on iteration of the inner products between tokenized pseudo-random number and the user specific fingerprint features. This proposed method provides a set of user specific compact codes which is named as Biohash code.

Cancellable biometric technique is the best method which provides solution of reusing the biometric template. This means that, even if the biometric template is lost, it is still revocable and replaceable. This provides more significant benefits to the users in terms of security and privacy. Thus in the proposed cancellable biometric approach, the true biometric pattern of the user never leaves the client computer. After the necessary biometrics preprocessing, such as segmentation and encoding, the unwrapped fingerprint pattern [21, 3] image or fingerprint code is intentionally distorted using a non-invertible transform. These new versions of the fingerprint are very much secure because the original fingerprint pattern can not be recovered even from the stored representation. They are also cancellable because another totally different pattern or code can be generated by the transform procedure by simply supplying a different set of distortion parameters. In this way one or two fingerprints can be multiplied into thousands of different virtual fingerprints.

In this paper, an improved BioHashing approach which uses the non-invertible technique for fingerprints without pre-alignment on the registration point of the fingerprint image [9] is proposed. In the non-invertible technique, the cancellable fingerprint templates are utilized to generate a unique non-invertible key [22]. As the key generated [18] is non-invertible, the proposed approach makes it computationally hard to invert the transformed template without presenting the unique personal key. Besides, in the case that the transformed template is compromised, a new one can be regenerated by simply assigning a different key to the biometric template for better results. BioHashing approach achieved a zero EER rate based on the impractical hidden assumption of no stealing of the Hash key.

2. RELATED WORK

Tee Connie et al., [1] proposed a novel cancellable biometric approach, known as Palm Hashing, to solve the non-revocable biometric issue. The proposed method hashes palm print templates with a set of pseudo-random keys to obtain a unique code called palm hash. The palm hash code can be stored in portable devices such tokens and smartcards for authentication. Ying-Han Pang et al., [2] proposed a cancellable palm print authentication system proposed in this paper specifically designed to overcome the limitations of the contemporary biometric authentication system. In this proposed system, Geometric and pseudo Zernike moments are employed as feature extractors to transform palm print image into a lower dimensional compact feature representation.

T. B. J. Andrew et al., [3] proposed a novel method to secure cryptographic private key binding and retrieving from fingerprint data using Biohash, Reed-Solomon error code (RSC) and the threshold secret sharing scheme. King-Hong Cheung et al., [17] proposed that one of the aims of cancellable biometrics is to protect privacy. In order to protect privacy, cancellable biometrics is preferably to be non-invertible such that no information can be revealed from the cancellable biometrics template, which is stored in databases for personal identification/verification. One way to achieve the non-invertibility is through the use of non-invertible transforms. Recently,

some new cancellable biometric approaches are proposed based on BioHashing. Those approaches are utilizing non-invertible transforms to achieve cancellable biometrics and thus non-invertibility is also attained.

Alessandra Lumini et al., [10] proposed some ideas to improve the base BioHashing approach in order to maintain a very low equal error rate when nobody steals the Hash key, and to reach good performance also when an "impostor" steals the Hash key. Sunil V. K. Gaddam et al., [5] puts forth a fresh methodology for the secure storage of fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption with the aid of cancellable biometric features. In this paper the author propose a technique to produce cancellable key from fingerprint so as to surmount these problems. The flexibility and dependability of cryptography is enhanced with the exploitation of cancellable bio-metric features.

Russell Ang et al., [6] proposed how to measure the success of a particular transformation and matching algorithm for fingerprints. The author considers a key–dependent geometric transform that is applied to the features extracted from a fingerprint, to generate a key–dependent cancellable template for the fingerprint. The author also investigates the performance of an authentication system that uses this cancellable fingerprint when a fingerprint matching algorithm is used for detection. Y. J. Chang proposed [7] a new method to protect face biometric data using one-way transformation in which original face images cannot be retrieved. The secure and reusable templates are generated by utilizing the Radon transformed signatures of the face biometric and a multi-space random projection. Using an image-based statistical algorithm, authentication is conducted on the transformed templates without the need to reverse them back.

Biometrics- based cryptographic key generation is proposed by Chang et al., [7]. As an alternative for using PINs and passwords as cryptographic keys that are either simple for fail to remember or susceptible to dictionary attacks, easy-t-camy and difficult-to-transfer keys can be created according to the user-specific biometric information. The author presents to create stable cryptographic keys from biometric data that is unbalanced in nature. The presented framework varies from prior work in that user-dependent transforms are used to create more condensed and distinguishable characteristics. Thus, a longer and steadier bitstream can be created as the cryptographic key. Evaluation is carried out using one face database to confirm the feasibility of the presented technique. The output obtained is highly cheering.

Implementation and Performance of Fingerprint based Fuzzy Vault is presented by Nandakumar et al., [8]. Dependable information protection techniques are needed to contest the increasing magnitude of identity theft in the society. Although cryptography is a commanding technique to realize information security, one of the chief disputes in cryptosystems is to preserve the secrecy of the cryptographic keys. Although biometric authentication can be helpful in ensuring that only the legitimate user has admittance to the secret keys, a biometric system itself is susceptible to a number of threats. A critical matter in biometric schemes is defending the template of a user that is characteristically stored in a database or a smart card. The fuzzy vault build up is a biometric cryptosystem which secures both the secret key and the biometric template by creating them inside a cryptographic framework. This paper provides a fully automatic functioning of the fuzzy vault technique according to the fingerprint minutiae [25]. As the fuzzy vault stores just a transformed version of the template, aligning the query fingerprint with the template is a difficult mission. The author take out high curvature points obtained from the fingerprint orientation area and utilize them as helper data to line up the template and query minutiae. The helper data itself does not disclose any data about the minutiae template, yet consists of enough data to align the template and query fingerprints perfectly. Additional, this paper utilized a minutiae matcher in the process decoding to account for non-linear distortion and this guides to noteworthy enhancement in the genuine accept rate. This paper shows the performance of the vault

implementation on two different fingerprint databases. This paper also provides that performance improvement can be obtained with the help of multiple fingerprint impressions during enrollment and verification.

Combining minutiae descriptors for fingerprint matching is suggested by Feng [9]. A new minutiae-based fingerprint matching technique is presented in this paper. Minutiae matching technique has to resolve two difficulties: correspondence and similarity computation. For the correspondence difficulty, this paper allocates all the minutia two descriptors: texture-based and minutiae-based descriptors, and utilizes an alignment-based greedy matching technique in order to establish the correspondences among minutiae. For the purpose of similarity computation, this paper take out a 17-D feature vector from the matching outcome, and translate the feature vector into a matching score with the help of support vector classifier. The presented technique is tested on FVC2002 databases and compared to all participators in FVC2002. In case of equal error rate, the presented technique ranks first on DB3, the most complicated database in FVC2002, and on the average ranks second on all 4 databases.

Performance evaluation of fingerprint verification systems is performed by Cappelli et al., [11]. The author focuses on the performance assessment of fingerprint verification techniques. Following a starting classification of biometric testing initiatives, this paper investigate both the theoretical and practical subjects associated with the performance evaluation by presenting the result of the latest Fingerprint Verification Competition (FVC2004). FVC2004 was controlled by the authors of this work for the function of assessing the state-of-the-art in this demanding pattern recognition function and creating available a novel frequent benchmark for an unambiguous comparison of fingerprint-based biometric systems.FVC2004 is an independent, powerfully supervised evaluation carried out at the evaluators' site on evaluators' hardware. This permits the test to be completely controlled and the computation times of various techniques to be fairly compared. The experience and comment gathered from previous, comparable competitions (FVC2000 and FVC2002) permits us to enhance the organization and technique of FVC2004 and to imprison the attention of a importantly higher number of academic and commercial institutes (67 algorithms were submitted for FVC2004). A novel, "Light" competition class was integrated to approximation the loss of matching performance resulted by means of imposing computational constraints. The author provides data collection and testing protocols, and includes a comprehensive analysis of the outcomes. The author establish a straightforward however efficient technique for comparing techniques at the score level, permitting to segregate difficult cases (images) and to learn error correlations and technique "fusion." The large quantity of information obtained, that includes a structured categorization of the submitted techniques according to their characteristics, creating it likely to better understand how present fingerprint recognition techniques work and to define helpful better techique.

Draper et al., [12] define a technique to encode fingerprint biometrics securely for utilization, e.g., in encryption or access control. The system is secure since the stored data does not adequate to rebuild the initial fingerprint biometric. Hence, a violation in database security does not result in loss of biometric information. Meanwhile, the stored information is adequate to validate a search fingerprint. The technique in this paper is according to the utilization of distributed source coding methods implemented with graphbased codes. This paper provides a statistical model of the relationship among the enrolment biometric and the (noisy) biometric measurement considering in the process of authentication. This paper provides the ways to accept or refuse a candidate biometric probe provided the query and the stored encoded information. The author describes the effectiveness of the proposed technique as tested on a database containing 579 data sets, all consists approximately 15 measurements of a single finger. This paper thus shows a working secure biometric method for fingerprints.

Farooq et al., [13] provides anonymous and revocable fingerprint recognition. Biometric identification has various merits comparing to the old ID and password systems; on the other hand, the need for anonymity and revocability of biometric templates is of consideration. Various techniques have been presented to tackle these issues. Various conventional techniques need a specific registration ahead of matching in the anonymous domain. This paper provides binary string indications of fingerprints that prevent the requirement for registration and can be matched straight. The author provides various methods for creating anonymous and revocable representations with the help of these binary string representations. The match performance of these representations is measured with the help of a large database of fingerprint images. This paper confirms that provided an anonymous representation, it is practically not feasible to invert it to the original fingerprint [26], thus preserving privacy.

An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancellable Fingerprint Biometrics is proposed by Lalithamani et al., [22]. The main disadvantage of the conventional cryptographic algorithms is the preservation of their key's secrecy. Incorporating the users' biometric features in the generation of strong and repeatable cryptographic keys has gained huge popularity among researchers. The randomness of the user's biometric features, incorporated into the generated cryptographic key, makes the key in order that it can not be cracked by the attacker lacking noteworthy information of the user's biometrics. However, if a person's biometric is missed once, it will be helpful for the attackers everlastingly as it is naturally belong to the user. To deal with this problem, cancellable biometrics can be used as an effective answer for cancelling and re-issuing biometric templates. Here, this paper presents an innovative and efficient technique to create a non-invertible cryptographic key from cancellable fingerprint templates. In the beginning, a one-way transformation is applied on the minutiae points obtained from the fingerprints, to accomplish a set of transformed points. Consequently, the transformed points are made use of to produce cancellable templates. The cancellable fingerprint templates are then used to create a unique non-invertible key.

Takahashi et al., [23] put forth a new technique for creating cancellable fingerprint templates with verifiable security based on the well-known chip matching algorithm for fingerprint verification and correlation-invariant random filtering for transforming templates. Ratha et al., [4] demonstrate different techniques to create multiple cancellable identifiers from fingerprint images. In essence, a user can be given as many biometric identifiers as required by issuing a new transformation key. The identifiers can be cancelled and replaced when cracked by attackers. The performance of several algorithms such as Cartesian, polar, and surface folding transformations of the minutiae positions are compared.

3. BIOHASHING

The concept of BioHashing is a form of cancellable or replaceable biometrics technique. In this approach, a set of user-specific random numbers are integrated with biometric features to deal with the security and performance of the biometric approach. In the BioHashing approach, the same user fingerprint data can result in highly correlated bit strings because of the high tolerant of data capture offsets. Moreover in this approach, there is no deterministic way to get the user specific code without having both token with random data and user fingerprint feature. Thus this feature of bio hashing would protect our system against any biometric fabrication. Thus the unauthorized users can be easily identified by this approach. This approach provides the revocable property in the biometric traits. Thus the possibility of leakage of the original biometric template is eliminated. The BioHashing [14] has significant functional advantages over solely biometrics like zero error rate point and clean separation of the genuine and imposter populations, thereby allowing false accept rates elimination without suffering from increased occurrence of false reject rates. The proposed Biohashing approach uses non-invertibility technique for better security and performance.

3.1Non-Invertibility and Bio-Hashing

The Security and privacy concern of a feature transformation technique can be enhanced and evaluated based on technique of non-invertibility. It is a technique which refers to the complexity in recovering the original biometric feature given the secure template. The *non-invertibility* [14] of the transform determines the security of the feature transformation based template protection schemes. Thus it is very important to propose a measure of the non-invertibility which estimates the likelihood of an opponent being able to guess the original template given the transformed template. Bio-hashing or salting is one of the invertible transformation biometric protection scheme approaches, in which the factors used for transformation is user specific key or password. In this approach the key needs to be stored in a secure manner or the password needs to be remembered by the user to present it during authentication checking. This non-invertible technique is very much important for the authentication purpose, as it enhances the security of the biometric template space by employing a transformation process to reset the order or position of the biometric feature. The progression of Biohashing is shown in figure 1. As mentioned in the figure, the discussion is as follows. Initially the fingerprint undergoes transformation and the features in the fingerprint are extracted. The feature vectors contain various features of the provided fingerprint which are used for generating the hash code. Then the Tokenised Random Number (TRN) is supplied to the system. The supplied Tokenised Random Number (TRN) is combined with the feature vectors obtained form the finger print. The inner product resulted for the combination is nothing but the Hashcode generated for the provided fingerprint and the tokenised random number.

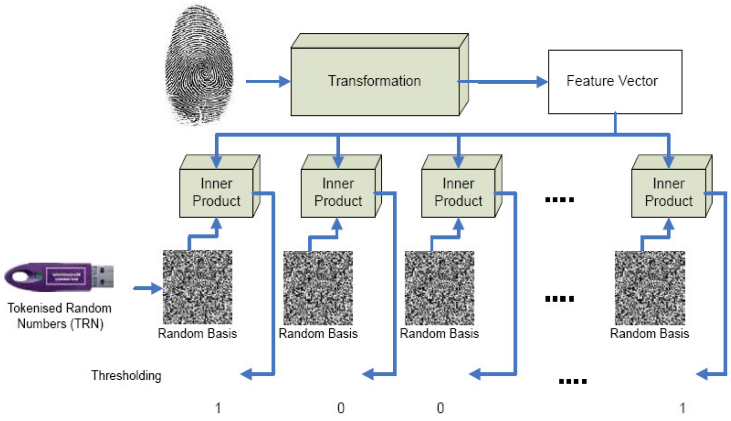

Figure 1: Progression of Biohashing

3.1.1Non-Invertible Transformation

Non-invertible transform [17] is used in this proposed technique. This transformation, does not stores the original fingerprint image. A one-way function is used for the transformation of the fingerprint. The non-invertible transformation occurs in the same signal or feature space as the original fingerprint. For example when an intentional distortion of a fingerprint signal based on a chosen transform function was introduced; it distorts the fingerprint signal in the same fashion at each presentation, that is, during enrolment and for every subsequent authentication checking. Thus in this method, every instance of enrolment can use a different transform function which makes cross-matching almost impossible. Moreover, in this approach, if one variant of the biometrics is compromised, then the transformation can be changed to create a new variant for re-enrolment.

In Non-invertible transformation, a many-to-one function f is designed to modify a raw biometric image intentionally into a new form within the context of feature or signal space. The

function f serves as an agent in the context of template security allowing for template non-invertibility, reusability and diversity. Since f does not have direct interaction with raw biometrics, the main advantage of this approach is that f does not need to be kept secret. In Fig. 2, Architecture of BioHashing is shown in which the two main processes, feature domain random transformation and quantization are explained. Various biometrics approaches exploits different signal acquisition, preprocessing and feature extraction techniques. The feature domain random transformation process remains the same that includes the generation of random matrix, orthonormalization and feature transformation. Quantization is performed afterwards based on a threshold (τ).

Feature domain random transformation and discretization is conducted as follows

- Employ the input token to generate a set of pseudo-random vector, $\{P_i \in \Re^M | i = 1, \ldots\ldots, m\}$ based on a seed.
- Apply the Gram-Schmidt process to $\{P_i \in \Re^M | i = 1, \ldots\ldots, m\}$ to obtain, a set of orthonormal vectors $\{r_i \in \Re^M | i = 1, \ldots\ldots, m\}$.
- Calculate the dot product of $\boldsymbol{v}$, the feature vector obtained from first step and each orthonormal vector, P_i such that $\langle v, r_i \rangle$.
- Use a threshold τ to obtain Biocode, $B = \{b_1, \ldots., b_i, \ldots\ldots, b_m\}$ and its elements are defined as

$$b_i = \begin{cases} 0 \; if \; \langle v, r_i \rangle \leq \tau \\ 1 \; if \; \langle v, r_i \rangle > \tau, \end{cases}$$

where i is between 0 and m, the dimensionality of B. Two BioCodes are compared by hamming distance.

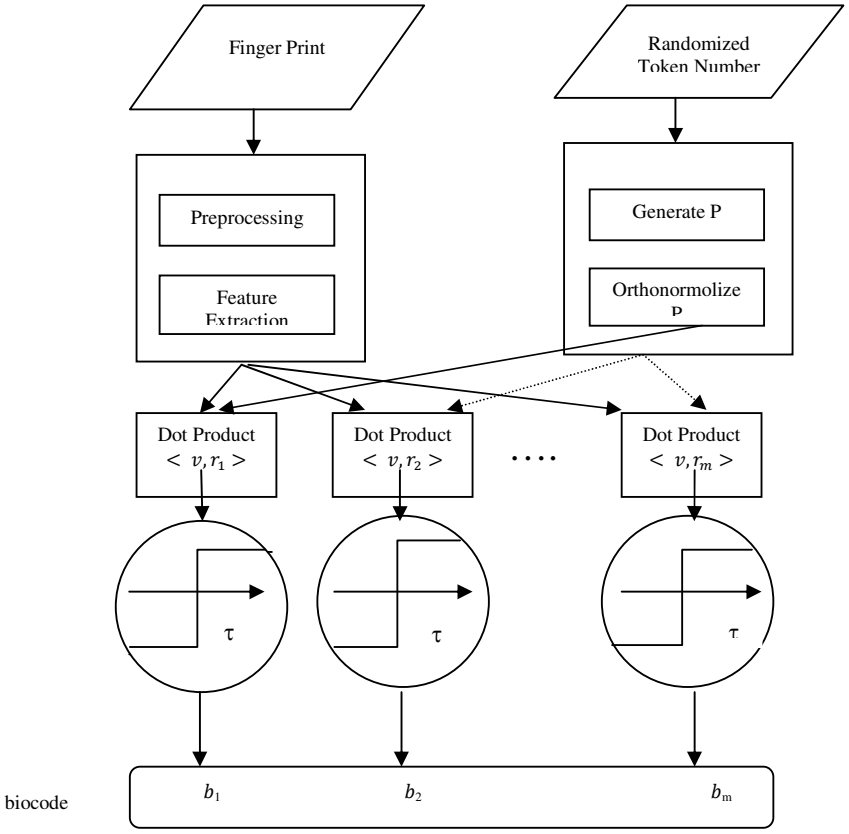

Figure 2: Architecture of bio hash

4. EXPERIMENTAL RESULTS

For the experimental set up, Eigen feature is adopted as the fingerprint feature extractor. A subset of 400 users, each having six essentially normalized fingerprint images with variations in pose, scale and illumination are randomly selected.

For the generation of the impostor distribution, the first Biohash of each subject is matched against the first Biohash of all other subjects, and the same matching process was repeated for subsequent BioHashes, leading to $(400\times399)/2\times6=478,800$ impostor attempts. Similarly for the generation of the genuine distribution, each Biohash of each subject is matched against all other BioHashes of the same subject, leading to 6000 ((5×6)/2 attempts of each subject×400). For the pseudo-genuine I distribution, the worst case scenario where the impostors always manage to steal the same genuine token is assumed. It means that only a set of TRN is mixed with all the fingerprint images and the matching is done based on the above described impostor matching.

The genuine vs. impostor distributions enable us to calculate the EER for the genuine-token, stolen-token, and stolen-biometrics scenarios. EER refers to the average value of two error rates, i.e. False Acceptance Rate (FAR) and False Rejection Rate (FRR). The same procedure is iterated for ten times and the results are averaged to avoid fluctuations. In this paper, pca and pcab-m denote Eigen values and Biohash, respectively, with m bit length. It is to be observed that the feature length of pca, n is taken as 100 for this experiment. Biohash with length 20, 40, 60, 80, and 100 are taken for this experiment.

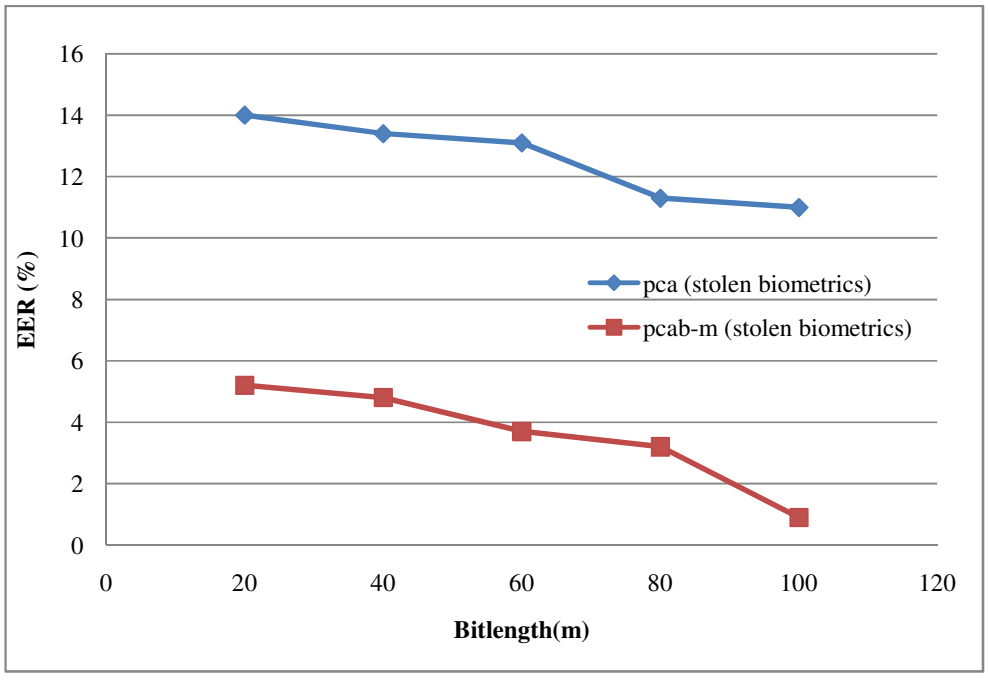

Figure 3: The Performance Comparisons for pcab-*m*, pca for Stolen Biometrics

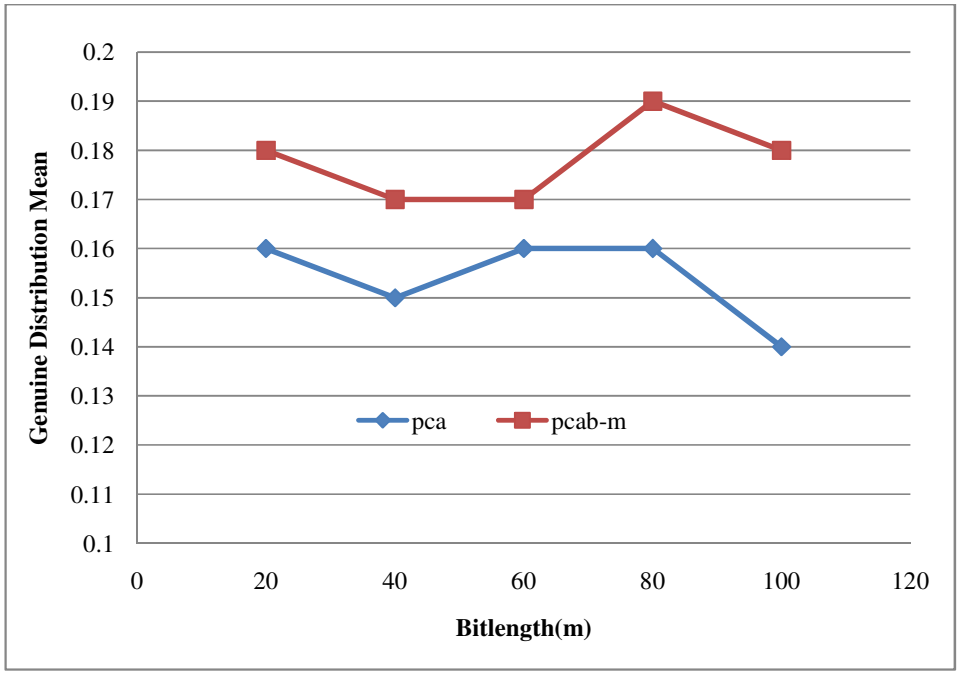

Figure 4: Genuine Distribution Mean for pcab-*m* and pca

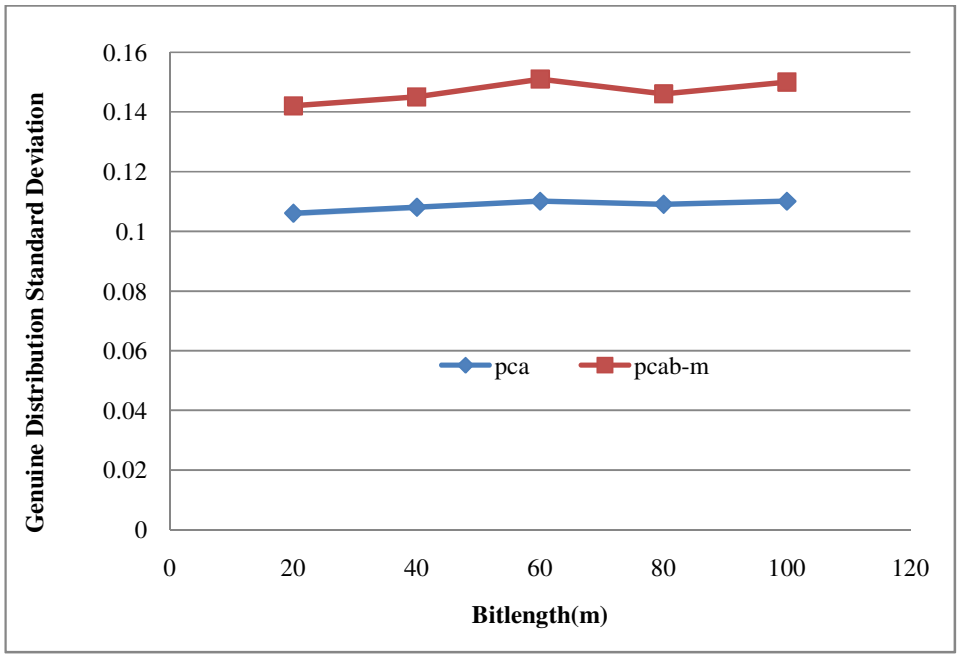

Figure 5: Genuine Distribution Standard Deviation for pcab-*m* and pca

From the experimental result, it is observed that FAR is almost zero and FRR is very minimum. So EER is less than 1% which is very significant. From Figure 3, it is observed that the EER of pcab-m is better than pca. Thus the performance of this proposed approach is very much satisfactory compared to the traditional biometric approach.

Figure 4 shows the Genuine Distribution Mean for pcab-m and pca. From the figure, it can be observed that the Genuine Distribution Mean value resulted for the proposed technique is higher than the existing technique. Figure 4 shows the Genuine Distribution Standard Deviation for pcab-m and pca. As indicated in figure 4, the Genuine Distribution Standard Deviation for the proposed technique is better than the existing technique. This result is true not only for particular bit length; rather it is true for all the size of bit length.

Thus the experiment result shows that this proposed approach provides greater security and accuracy. Apart from the good recognition capabilities, the proposed approach has the advantages of security (revocable templates) and privacy protection not realizable if only biometric feature is considered.

5. CONCLUSION

The proposed approach uses the technique which combines cancellable biometrics and the concept of non-invertibility. Cancellable biometrics provides a solution for protecting the privacy of the user. Since the user's true biometric feature is never revealed in the authentication process. Biohashing is used for the better security and accuracy. These BioHashes are cancellable through straightforward revocation and then refreshment of the token, thereby protecting against interception of biometric data. In the privacy and security domains, the proposed method fulfills three requirements, namely performance in terms of False Rejection Rate (FRR) and False Acceptance Rate (FAR), non-invertibility and revocability. The proposed technique makes it computationally hard to invert the transformed template without presenting the unique personal key. From the results obtained it is clear that the proposed approach provides a very low EER (less than 1%). Thus the approach is very much is secured.

The Biohash thus provides a substantive improvement over recognition based purely on biometric feature extraction and complex classifier. This approach can be enhanced to higher level in order to further improve the security. This work can be extended in future by using the highly secure non invertible transform such as Baker Non-Invertible Transform. The usage of this Baker Non-Invertible Transform will result in strong mixing of feature points and it will be very hard to break by the attackers and thus it can provide better security.

REFERENCES

[1] T.Connie, A.Teoh, M.Goh and D.Ngo,(2004) "Palm Hashing: a novel approach to cancelable biometrics", Information Processing Letter 93(1), -5.

[2] Y.H.Pang, B.J. Andrew Teoh and C.L. David Ngo,(2005) "Palm print based cancelable biometric authentication system", International Journal of Signal Processing 1(2), 98-104.

[3] T. B. J. Andrew, N. C. L. David, and G. Alwyn,(2006) "Biohashing: two factor authentication featuring fingerprint data and tokenized random number," Pattern Recognition, Pattern Recognition Soc., Elsevier Science, to be published.

[4] Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle,(2007) R.M, "Generating Cancelable Fingerprint Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, Special Issue on Biometrics 29(4), 561–572.

[5] Sunil V. K. Gaddam and Manohar Lal,(2010) "Efficient Cancellable Biometric Key Generation Scheme for Cryptography", International Journal of Network Security, Vol.11, No.2, PP.57-65.

[6] R. Ang, R. Safavi-Naini, L. McAven,(2005) "Cancellable key-based fingerprint templates," ACISP, pp.242-252.

[7] Y. J. Chang, Z. Wende, and T. Chen,(2004) "Biometrics- based cryptographic key generation," IEEE International Conference on Multimedia and Expo, vol. 3, pp. 2203-2206.

[8] Nandakumar, K., Jain, A. K., and Pankanti, S.,(2007) "Fingerprint based Fuzzy Vault: Implementation and Performance," IEEE Transactions on Information Forensics and Security 2, 744–757.

[9] Feng, "Combining minutiae descriptors for fingerprint matching," Pattern Recognition 41(1), 342–352, 2008.

[10] A. Lumini and L. Nanni,(2007) "An improved BioHashing for human authentication," Pattern Recognition 40(3), 1057–1065.

[11] R. Cappelli, D. Maio, D. Maltoni, J. Wayman and A. Jain,(2006) "Performance evaluation of fingerprint verification systems," IEEE Transactions on Pattern Analysis and Machine Intelligence 28(1), 3–18.

[12] Draper, S. C., Khisti, A., Martinian, E., Vetro, A., and Yedidia, J. S.,(2007) "Using Distributed Source Coding to Secure Fingerprint Biometrics," in Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP)], 2, 129–132.

[13] Farooq, F., Bolle, R., Jea, T., and Ratha, N.,(2007) "Anonymous and revocable fingerprint recognition," in Proc. Computer Vision and Pattern Recognition.

[14] Y. Sutcu, H. T. Sencar, and N. Memon,(2005) "A Secure Biometric Authentication Scheme Based on Robust Hashing," in Proc. ACM Multimedia and Security Workshop, New York, pp. 111–116.

[15] J.D. Golic and M. Baltatu,(2008) "Entropy analysis and new constructions of biometric key generation systems," IEEE Trans. Information Theory, vol. 54, no. 5, pp. 2026–2040.

[16] C. Lee, J. Y. Choi, K. A. Toh, and S. Lee, (2007)"Alignment-Free Cancelable Fingerprint Templates Based on Local Minutiae Information," IEEE Trans. Systems, Man, and Cybernetics, Part B, vol. 37, no. 4, pp. 980–992.

[17] King-Hong Cheung, Adams Kong, Jane You and David Zhang.,(2005) "An Analysis on Invertibility of Cancelable Biometrics based on BioHashing", CISST, pp 40-45.

[18] L. Ballard, S. Kamara, F.Monrose, and M. K. Reiter,(2008) "Towards practical biometric key generation with randomized biometric templates," in Proc. 15th ACM conference on Computer and communications security, New York, pp. 235–244.

[19] K. Simoens, P. Tuyls, and B. Preneel,(2009) "Privacy Weaknesses in Biometric Sketches," in Proc. IEEE Symposium on Security and Privacy.

[20] L. Rila, "Denial of access in biometrics-based authentication systems", (2000)In: Proceedings of International Conference of Infrastructure Security (Infrasec 2002), Bristol, UK, 1–3.

[21] Y. Isobe, Y. Seto, M. Kataoka, (2001)"Development of personal authentication system using fingerprint with digital signature technologies", In: Proceedings of the 34th Hawaii International Conference on System Sciences.

[22] Lalithamani, N. and Soman, K.P., "An Efficient Approach for Non-Invertible Cryptographic Key Generation from Cancelable Fingerprint Biometrics", International Conference on Advances in Recent Technologies in Communication and Computing, Pp. 47-52, 2009.

[23] Takahashi, K. and Hitachi, S.H.,"Generating Provably Secure Cancelable Fingerprint Templates based on Correlation-Invariant Random Filtering", IEEE 3rd International Conference on Theory, Applications, and Systems, Pp. 1-6, 2009.

[24] Ratha, N.K., Connell. J.H. and Bolle, R.M., "An Analysis of Minutiae Matching Strength," Proceedings of Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA), 2001, Pp. 223–228, 2001.

[25] Ross, A.K., Shah, J. and Jain, A.K., "From Templates to Images: Reconstructing Fingerprints from Minutiae Points," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 4, Pp. 544–560, 2007.

[26] Cappelli, R., Lumini, A., Maio, D. and Maltoni, D., "Fingerprint Image Reconstruction from Standard Templates," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 29, No. 9, Pp. 1489–1503, 2007.

[27] Boult, T.E., Scheirer, W.J. and Woodworth, R., "Fingerprint Revocable Biotokens: Accuracy and Security Analysis," Proceedings of IEEE Computer Society Conference on Computer Vision and Pattern Recognition, Pp. 1–8, 2007.