Implementation of Secure Biometric Fuzzy Vault Using Personal Image Identification

Sarika Khandelwal[1] and P.C. Gupta[2]

[1] Mewar university, Gangrar, Chittorgarh,Rajasthan, India
sarikakhandelwal@gmail.com
[2] Kota University, Kota, Rajasthan, India
pc.gupta26@gmail.com

Abstract. Biometric is proved to be an exceptional tool for identifying an individual. Security of biometric template is the most challenging aspect of biometric identification system. Storing the biometric template in the database increases the chance of compromising it which may lead to misuse of the individual identity. This paper proposes a novel and computationally simpler approach to store a biometric sample in the form of template by using cryptographic salts. Use of Personal Image Identification (PII) makes the proposed algorithm more robust and adds another level of security. The saltcrypted templates are created and stored instead of storing the actual sample behaving as a fuzzy vault. The algorithm has been analytically proved computationally simple compared to the existing template security mechanisms. The fuzzy structure of saltcrypted template is entirely dependent on user interaction through PII. Actual template is not stored at any point of time which adds new dimension to the security and hence to individual identity.

1 Introduction

The major problem with password based verification system is that, passwords or PINS can be stolen or lost[1].The suggested way for individual identity verification which seems to be robust and always available is use of biometric traits such as fingerprint, iris etc. Since the biometric templates are stored in the database, security of biometric template is major area of concern. Biometric template stolen once simply means that an individual's identity is stolen, as you cannot change this identity like passwords. This paper is an attempt to store a biometric in the form of template which is more secure and cannot be broken easily even though one gets an access to the template. A novel and relatively less complex approach to secure a biometric template without storing them in a database are proposed.

Fuzzy fingerprint vault is a secured construct used to store a critical data like secure key with fingerprint data. The secure template that is generated from a biometric sample is dependent on the attributes selected by the user. The two user selected attribute which are used in this paper are secret key and personal image. Along with that unique user id is also provided to the user which may be public.

S.C. Satapathy et al. (eds.), *Emerging ICT for Bridging the Future – Volume 1,*
Advances in Intelligent Systems and Computing 337, DOI: 10.1007/978-3-319-13728-5_35

Storing a biometric sample in the secured template form will avoid loss of privacy which could be there if the samples are stored in the database. Use of personal image identification along with biometric sample and secret key has made a system more robust in terms of security of a template.

Fuzzy vault binds biometric features and a secret key together without storing any of them. Thus it adds extra noise in the key as well as biometric sample and creates a fuzzy template for storage. At the time of verification, if both the saltcrypted stored template and query template are matched, then only the key can be released for further authentication. This work presents a novel approach to secure a biometric template using cryptographically salted fuzzy vault. The secured template that is generated using this cryptographically salted fuzzy system is dependent on the user defined personal images as well the secret key provided by the user.

2 Approaches to Secure Biometric Templates

Different strategies that are available to secure biometric template are generally based on cryptographic key binding/key generation mode. It includes transformations like salting or bio-hashing, cryptographic framework like Fuzzy vault, fuzzy commitment, secure sketches, fuzzy extractor etc.

A. Transformation: To secure a template it can be transformed into another form using either invertible or non-invertible transformations. Some of such transformations are salting or bio-hashing.

Salting: It is a template protection scheme in which template is converted or transformed into a different form using user specific key[2]. The random multi-space quantization technique proposed by Teoh et al. [3] is good example of salting. Salting can be done by extracting most distinguishing features of a biometric template and then obtained vectors can be projected in randomly selected orthogonal direction. This random projection vectors serves the basis of salting [4]. Another approach is noninvertible transform in which, the template is transformed into some other form using a key. Ratha et al [5] have proposed a method for noninvertible transformation of fingerprints.

B. Fuzzy vault: Fuzzy vault is biometric construct used to bind key as well as template together in a single framework. In order to secure a template using fuzzy vault, a polynomial is evaluated using secret key and some identifying points say minutia points in fingerprint templates are added to it to form a fuzzy vault. Some chaff points are also added to enhance the security. The security of fuzzy vault is based on infeasibility of polynomial reconstruction problem [6]. V.Evelyn Brindha[7] has proposed a robust fuzzy vault scheme in which fingerprints and palm prints are combined together to enhance the security of the template.Some results using fuzzy fingerprint vault have been reported [8-13].However, the major problems with all these approaches are that these do not consider all possible issues of fingerprint alignment, verification accuracy etc. Some of the difficulty and importance of alignment problem related to rotation in fuzzy fingerprint vault is explained by P. Zhang[14]. Chung and Moon [10-12] proposed the approach to solve the

auto-alignment problem in the fuzzy fingerprint vault using the idea of the geometric hashing [15].Yang and Verbauwhede [16] has used the concept of automatic alignment of two fingerprints of fuzzy vault using the idea of reference minutia. Jin Zhe[17] has proposed protected template scheme which is alignment free. In his work, each minutia is decomposed into four minutiae triplets. From these triplets a geometric feature is extracted to construct a fingerprint template.The experimental result shows that it is computationally hard to retrieve minutia information even when both protected template and random matrix are known. Besides that, the scheme is free from alignment and light in complexity.

Another problem that is reported in literature with fuzzy vault is that, Fuzzy vault is susceptible to correlation attack. That is two fuzzy vault created using same fingerprints can be correlated to reveal fingerprint minutiae hidden in the vault.

3 Salt Cryptography

The purpose of salt is to produce a large set of keys corresponding to a given password among which one is selected as a random. Salt need not to keep secret, it should only be random. Its only purpose is to inflate the potential number of combinations for each individual password in order to exponentially increase the effort required to crack it. However, a salt has only little impact when an individual password is attacked with brute force.

Salt can also be added to make it more difficult for an attacker to break into a system if an attacker does not know the password and trying to guess it with a brute force attack. Then every password he tries has to be tried with each salt value. If the salt has one bit this makes the encryption twice as hard to break in this way, and if the salt has two bit this makes it four times harder to break. If the salt is 32 bits long for instance there will be as many as 2 ^ 32 keys for each password from which we can imagine how difficult to crack passwords with encryption that uses a 32 bit salt.[18]

4 Personal Image Identification (PII)

PII is commonly used identification mechanism based on the image selected by the user at the time of enrolment. If the same image is selected by the user at the time of verification then it proves that the user is genuine [19].This PII can be used to create transaction specific password or it can be combined with other biometric verification system to make it more secure. The basic application of Personal image identification (PII) is to provide enriched security to the ATM system. To use PII in authentication, user has to select the personal image out of the given N number of images. At the time of verification the same has to be selected by the user.PII adds second level of security to the existing identification system.

In this paper PII is used to generate random salt that has to be added to the biometric sample. Here user is asked to register three personal images out of 16 available images at the time of enrolment. Based on these images and the password

provided by the user, salt is generated which can be used for further processing to create the template.

Figure 1 gives the details of the process used for registration of PII and its subsequent processing.

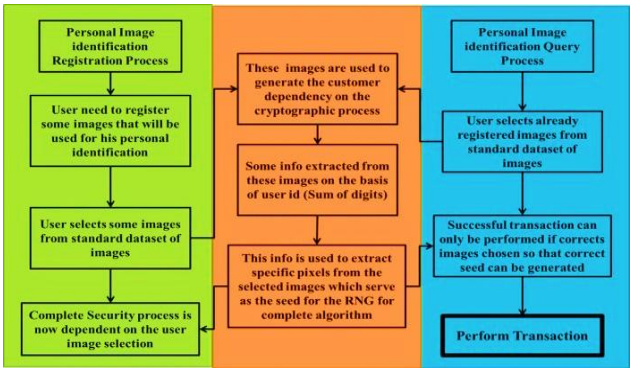

Fig. 1. Block schema of the PII registration and query process

5 Proposed Algorithm

This paper proposes a method to create a vault using salted cryptography where biometric traits i.e. fingerprint is stored in the form of transformed template. At the time of verification if the stored template and input template are matched then only key is released. The main idea behind the proposed method is not to store the actual template in the system. The algorithm for proposed verification system has two phases. Registration phase and matching phase. Figure 2 shows the phases of proposed algorithm.

5.1 Steps for Phase I (Registration/Enrollment Phase)

1. Input: Two fingerprint samples are merged together say f1 and f2 ,User ID and corresponding secret key for one time registration.
2. Personal image registration: User is asked to select the personal image from available images. Here three images are selected by the user from available set.
3. User ID of the customer is used to locate and extract the PII seed of the PN sequence generators from the pixels of PII images. Here we have used sum of digits of user ID to extract PII seed from the registered personal images.
4. Salt is generated using this seed for PN sequence generation after resetting the generator state.
5. Individual templates are combined and mixed with salt. The resultant saltcrypted template is stored. So no original templates are being stored.
6. Key taken while registration is to be embedded to the salted templates such that this embedding is guided by a pixel moving salt generated taking PII seed.

7. Now f3=f1 XOR f2 and then f4=f3 XOR salt, this f4 will be stored.
8. Embed the secret key inside the salted template.
9. Store the embedded salted fingerprints.

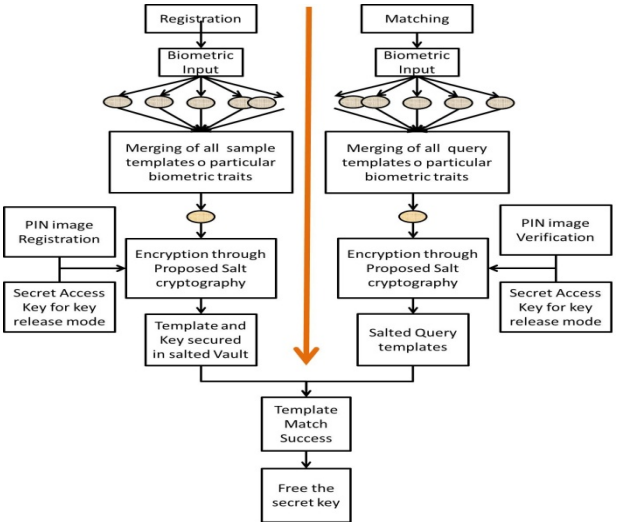

Fig. 2. Proposed algorithm (Phase –I Registration, Phase-II Matching phase)

5.2 Steps for Phase II(Matching phase)

1. During Verification phase biometric samples are taken. This is similar to enrolment phase.
2. User is asked to enter the user ID and to select the personal images.
3. Applying the same procedure as that of enrolment, the template is created.
4. This created saltcrypted template T' is matched with stored template T.

6 Simulation Results

The dataset used for fingerprint biometric is downloaded from NIST [9]. Any real time images can also be used. There is no restriction of the image size. But currently both the sample and query images must have same sizes. The sample fingerprint images are shown in figure. User need not to give the samples and queries in the same order. Any finger sample can be taken in any order. The algorithm has been simulated in MATLAB v12. Figure 3 shows the user ID and key registration window. The Personal images are selected through PII selection window. The user has to select three images out of the available 16 images. Personal image selection window is shown in figure 4.

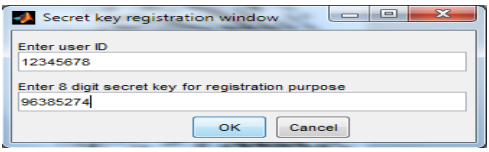

Fig. 3. ID and key registration window

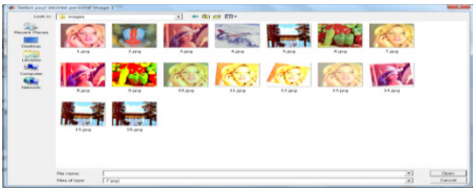

Fig. 4. Personal Image Selection Window

False acceptance rate : It is defined as the number of times a fingerprint is taken as a match even it is of some other person. FAR=False accepted queries/Total Queries
False rejection rate : It is the number of times a fingerprint of the genuine person is declared unmatched. FRR is acceptable up to some extent but FAR is not acceptable at all. FRR=False rejection queries/Total Queries.

The algorithm has been tested on variety of fingerprints images (more than 1000). FAR is 0.003% which may be due to bad quality of fingerprint image. FRR is a bit high 0.02% which is acceptable.

Table 1 shows the comparison of FAR and FRR with the existing approaches and proposed approach.Fig. 5(a) and 5(b) shows salted merged template and embedded saltcrypted template respectively.

Table 1. Comparison of the FAR and FRR with recent approaches

Approach	FAR	FRR
[20]	0.0016	0.05
[21]	0	0.21
[22,23]	7.1	7.15
[24]	4	2
Proposed	0.003	0.2

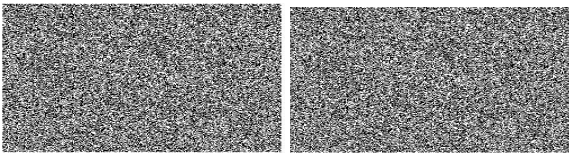

Fig.5.(a). **Fig. 5**(b).

Fig. 5. (a) Salted and merged template
Fig. 5.(b) Embedded saltcrypted template.

7 Analysis

First of all the major advantage of the algorithm needs discussion which is the complexity to get the actual template from the salted template.

1. Fingerprint image size = m*n,Salt1 size = m*n,Salt2 Size = bin_key_length= L
2. Complexity to know exact salts= 2m*n+L
3. Complexity of whole approach = $O(m*n)$; If m==n then $O(n^2)$
4. Complexity of Embedding and extraction O(L)
5. Complexity to find exact embedding locations

a. No of images in PII database = P,Concurrent selection = k = 3,No of digits in user ID = N

b. Complexity of extracting user dependent info from the PII images = $k*10^N$= seed generation complexity.

The complexities of RSA, AES and other cryptography methods used in literature fuzzy vault are much larger than the proposed algorithm. The mathematical process is also easier than the existing process to be implemented in hardware and low cost devices. The combination of PII image and salted templates make the exact PN sequences determination impossible.

8 Conclusion and Future Work

The proposed algorithm has shown advantage in terms of complexity. The approach has very less complexity. On the other hand the seed generation and localization of the secret key in the salted templates is very hard to do if exact secret keys and the generation algorithms are unknown, so intrusion is almost impossible. Other advantage is that,nowhere actual fingerprint are stored. Only the salted templates are kept in storage with embedded key. Even the matching process is independent of the actual templates. User need to give the fingerprint template at run time, it is stored nowhere. The comparison of the stored saltcrypted template and query saltcrypted template is done and the embedded key is released only if they match.

Future work lies in eliminating need of the user to remember the three personal images which seems to be difficult. Another can be in improvement of the algorithm to identify the images taken in different seasons for enrolment and verification. This approach is simplest and can be applied to any other biometric modality. We are currently evaluating this algorithm on other modalities. Results are in pipeline for publishing.

References

1. Jain, A., Ross, A., Uludag, U.: Biometric template security: Challenges and solutions. In: Proceedings of European Signal Processing Conference (EUSIPCO), pp. 469–472 (2005)
2. Jain, A.K., Nandakumar, K., Nagar, A.: Review Article Template Security. EURASIP Journal on Advances in Signal Processing 2008, Article ID 579416, 17 (2008), doi:10.1155/2008/579416

3. Teoh, A.B.J., Goh, A., Ngo, D.C.L.: Random multispace quantization as an analytic mechanism for BioHashing of biometric and random identity inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 28(12), 1892–1901 (2006)
4. Belhumeur, P.N., Hespanha, J.P., Kriegman, D.J.: Eigenfacesversusfisherfaces: recognition using class specific linear projection. IEEE Transactions on Pattern Analysis and MachineIntelligence 9(7), 711–720 (1997)
5. Ratha, N.K., Chikkerur, S., Connell, J.H., Bolle, R.M.: Generating Cancelable Fingerprint Templates. IEEE Transactionson Pattern Analysis and Machine Intelligence 29(4), 561–572 (2007)
6. Juels, A., Sudan, M.: A Fuzzy Vault Scheme. In: Proceedings of IEEE International Symposium on Information Theory, vol. 6(3), p. 408 (2002)
7. Brindha, E.: Biometric Template Security using Fuzzy Vault. In: IEEE 15th International Symposium on Consumer Electronics (2011)
8. Clancy, T., et al.: Secure Smartcard-based Fingerprint Authentication. In: Proc. of ACM SIGMM Multim., Biom. Met. & App., pp. 45–52 (2003)
9. Uludag, U., Pankanti, S., Jain, A.K.: Fuzzy vault for fingerprints. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 310–319. Springer, Heidelberg (2005)
10. Nandakumar, et al.: Fingerprint-based Fuzzy Vault: Implementation and Performance. EEE Transactions on Information Forensics and Security 2(4), 744–757 (2007)
11. Yang, S., Verbauwhede, I.: Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme. In: Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 5, pp. 609–612 (2005)
12. Chung, Y., Moon, D.-s., Lee, S.-J., Jung, S.-H., Kim, T., Ahn, D.: Automatic Alignment of Fingerprint Features for Fuzzy Fingerprint Vault. In: Feng, D., Lin, D., Yung, M. (eds.) CISC 2005. LNCS, vol. 3822, pp. 358–369. Springer, Heidelberg (2005)
13. Moon, D., et al.: Configurable Fuzzy Fingerprint Vault for Match-on-Card System. IEICE Electron Express 6(14), 993–999 (2009)
14. Zhang, P., Hu, J., Li, C., Bennamound, M., Bhagavatulae, V.: A Pitfall in Fingerprint Bio-Cryptographic Key Generation. In: Computers and Security. Elsevier (2011)
15. Wolfson, H., Rigoutsos, I.: Geometric Hashing: an Overview. IEEE Computational Science and Engineering 4, 10–21 (1997)
16. Yang, S., Verbauwhede, I.: Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme. In: Proc. of IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 5, pp. 609–612 (2005)
17. Zhe, J.: Fingerprint Template Protection with Minutia Vicinity Decomposition. ©2011 IEEE (2011) 9781- 4577-1359-0/11/$26.00
18. Sharma, N., Rathi, R., Jain, V., Saifi, M.W.: A novel technique for secure information transmission in videos using salt cryptography. In: 2012 Nirma University International Conference on Engineering (NUiCONE), December 6-8, pp. 1–6 (2012)
19. Santhi, B., Ramkumar, K.: Novel hybrid Technology in ATM security using Biometrics. Journal of Theoretical and Applied Information Technology 37(2) ISSN: 1992- 8645
20. Moon, D.-s., Lee, S.-J., Jung, S.-H., Chung, Y., Park, M., Yi, O.: Fingerprint Template Protection Using Fuzzy Vault. In: Gervasi, O., Gavrilova, M.L. (eds.) ICCSA 2007, Part III. LNCS, vol. 4707, pp. 1141–1151. Springer, Heidelberg (2007)
21. Uludag, U., Pankanti, S., Jain, A.: Fuzzy Vault for Fingerprints. In: Kanade, T., Jain, A., Ratha, N.K. (eds.) AVBPA 2005. LNCS, vol. 3546, pp. 310–319. Springer, Heidelberg (2005)

22. Long, T.B., Thai, L.H., Hanh, T.: Multimodal Biometric Person Authentication Using Fingerprint, Face Features. In: Anthony, P., Ishizuka, M., Lukose, D. (eds.) PRICAI 2012. LNCS, vol. 7458, pp. 613–624. Springer, Heidelberg (2012)
23. Qader, H.A., Ramli, A.R., Al-Haddad, S.: Fingerprint Recognition Using Zernike Moments. The International Arab Journal of Information Technology 4(4) (October 2007)
24. Shrivastava, R., Thakur, S.: Performance Analysis of Fingerprint Based Biometric Authentication System using RSA. Engineering Universe for Scientific Research and Management 6(2) (February 2014)