Electronic Letters on Computer Vision and Image Analysis 13(3):28-40, 2014

Multitier biometric template security using cryptographic salts and personal image identification

Sarika Khandewal* and P.C.Gupta+

* *Research Scholar,Mewar University, Gangrar, Chittorgarh, India*
+ *CSE Department, Kota University , Kota, India*

Received 13th Nov 2013; accepted 27th Aug 2014

Abstract

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 serious threat and 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 tier of security. The saltcrypted templates are created and stored instead of storing the actual biometric sample.The algorithm has been analytically proved computationally simple compared to the existing template security mechanisms. The 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. The accuracy of the proposed method is equally good as the recent methods with less computational complexity.
Key Words: Cryptographically salted Fuzzy vault, Biometric template, PII(Personal image identification).

1 Introduction

Individual identification can be accurately done by measuring biological parameters termed as biometrics. Digital biometric identification is widely accepted technique for individual verification as compared to traditional manual method of personal identification. A basic biometric identification or verification system requires users biometric samples to be stored in the database which can be used for verification purpose. The most challenging aspect of this traditional biometric identification system is security of biometric samples that are stored in the database.Once a biometric sample is stolen or compromised; an individual identity is compromised forever. It cannot be changed as a normal alphanumeric password system or Personal Identification Number (PIN)system. Encrypted biometric samples can be used for authenticating a user without storing the actual biometric sample. This paper presents a novel and relatively less complex approach to secure a biometric template without storing them in a database. Fuzzy fingerprint vault is a secured construct used to store a critical data like secure PIN 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 PIN and a set of personal images. Along with that unique user id is also provided to the users. Storing a biometric sample

Correspondence to: <sarikakhandelwal@gmail.com>

Recommended for acceptance by <Manuele Bicego>
ELCVIA ISSN:1577-5097
Published by Computer Vision Center / Universitat Autònoma de Barcelona, Barcelona, Spain

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,only then 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 provided personal images and a secret key.

2 Template protection scheme survey:

Using biometrics and cryptography independently plays vital role in security. But if both of these approaches are used together, can add higher level of security.Different methods to protect the biometric data exist, which can be classified into four categories:Cancellable biometrics, biometric salting, fuzzy encryption and biometric hardening passwords. Cancellable biometric transform the original biometric sample into non invertible template.No relation exists between the sample and template [1]. Generally cancellable biometrics applies a transform function on the template and outputs a transformed template. The transform has to be irreversible for best security. The transforms used are mathematical in nature; they have very less share of the user customization for security. Biometric salting as described by Ratha et al. uses random patterns to convolute biometric data [2]. In biometric encryption, described in [3],a correlation filter is used to extract features from biometric samples and subsequently both the features and the filter is multiplied with a noise value, providing a masked reference before embedding a random key (the pseudo identity) in the reference using a lookup table. Similarly, in the bio-hashing algorithm by Roberge et al. [4], features are derived using an integrated wavelet and Fourier-Mellintransform framework (WFMT) before the inner product of the feature and a sequence of orthogonal random patterns are calculated and binarized. The resulting bit string constitutes the pseudo identity of the subject. The mechanism requires the use of a long bit string, typically stored in a token; verification is possible only if both token and the authorized biometrics are present. Biometric hardening passwords can only be used in keystroke or voice recognition systems [5]. The spoken or typed key is verified and combined with the key generated from biometric features. This method has poor generalizability in comparison with other categories, which can be applied on different kinds of biometric modalities. Fuzzy encryption combines cryptographic protocol with error correction codes(ECC), which is used to compensate for variations in measurements stemming from either acceptable changes in the data source such as aging and environmental influences, or differences in the signal acquisition pathway such as measurement and signal processing, concentrating on features remaining invariant under these influences and noise. The fuzzy commitment scheme was proposed by Juels and Wattenberg[6], which demonstrate the use of cryptographic hash functions.In [7], a reliable biometric authentication model so called shielding function or helper data scheme using cryptographic function for noisy data is introduced as well as its properties. All these method have used biometric sample and cryptography to convert it into the template. Use of PII to add more security to the ATM application is described by Santhi[8]. PII is used as an alternate when biometric samples are damaged.The PII is used to generate transaction ID for the particular transaction. All the methods described previously are dealing with template protection where actual biometric sample is transformed into template using some complex calculation of cryptography. This paper proposes a method to transform a biometric sample into template just like cancellable biometrics but it binds a secret key with the template also ensuring the feature of fuzzy vaults. It is an attempt to use cryptography and PII together on a biometric sample. Multiple samples of single or multiple biometric modalities are combined to enhance the security of the system.To make it more concrete, a random Salt is added using PII. It proves added levels of the security and relation of the proposed algorithm with the cancellable biometric and fuzzy vault system. Fig (1) describes various methods to protect biometric samples.

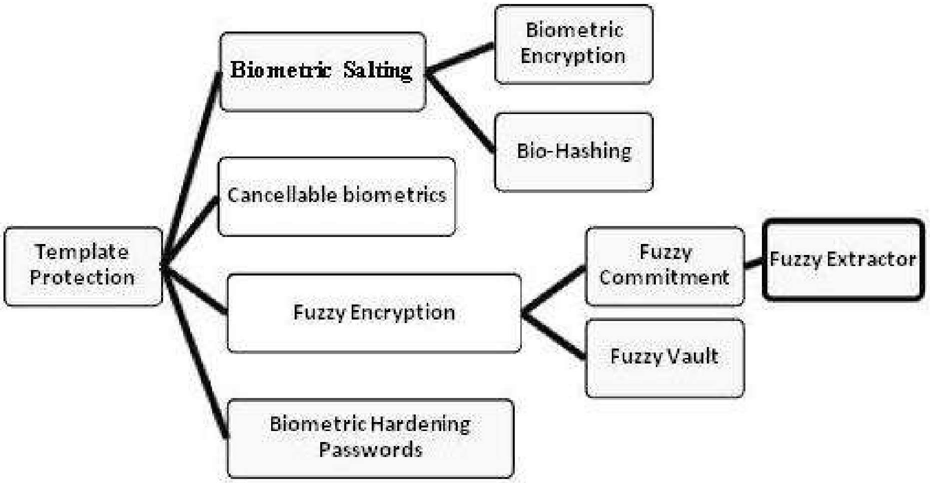


Figure 1: Methods to protect biometric samples.

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 randomly. Salt need not to be kept 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.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. 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.

3.1 Benefits of Salt:

- If two users who choose the same password will have different entries in the system password file.
- Salt is random data that helps protect against dictionary and brute force attack for cracking large number of password much slower. An attacker could build a dictionary of common password and just look up the original password if there were no salt.

4 Personal image identification (PII):

PII is an identification mechanism based on the images selected by the user at the time of enrollment.If the same image is selected by the user at the time of verification then it proves that the user is genuine.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. It also adds security customized to the user since each user selects different images. This leads to unique security parameters for all.

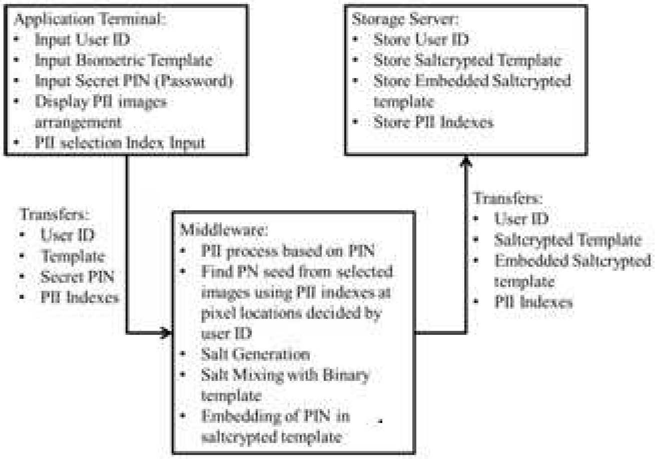

Application Terminal:
• Input User ID
• Input Biometric Template
• Input Secret PIN (Password)
• Display PII images arrangement
• PII selection Index Input
Storage Server:
• Store User ID
• Store Saltcrypted Template
• Store Embedded Saltcrypted template
• Store PII Indexes
Transfers:
• User ID
• Template
• Secret PIN
• PII Indexes
Middleware:
• PII process based on PIN
• Find PN seed from selected images using PII indexes at pixel locations decided by user ID
• Salt Generation
• Salt Mixing with Binary template
• Embedding of PIN in saltcrypted template
Transfers:
• User ID
• Saltcrypted Template
• Embedded Saltcrypted template
• PII Indexes

Figure 2: Abstraction module of proposed system architecture

4.1 Improved PII verification:

Adding a new dimension to the secure architecture PII also adds the complexity for the user to remember the registered images whereas biometric system's prime goal was to eliminate the complexity of remembering the secret keys. So to use the advantages of PII and maintaining the prime requirement of biometrics, in this paper we used modified PII to generate random cryptographic salt that will be added to the biometric sample.Here user is asked to register three personal images out of N available images at the time of enrollment. These images are arranged in a random order which is specific for the password of the user. 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.

5 Proposed system architecture:

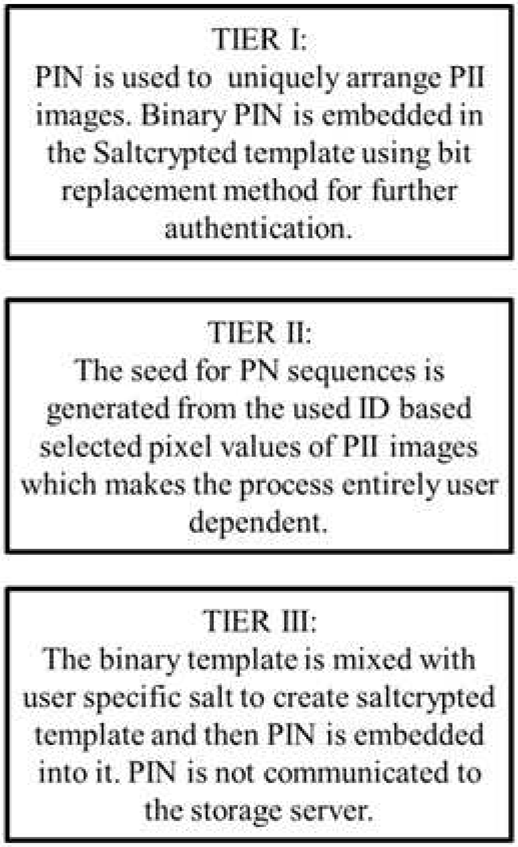
Proposed system consists of three abstraction layers. The layered architecture has been adopted to match requirements of a real time system that is up gradable and scalable.

1. Application Layer: This is user side layer which interacts with the user to take inputs. The main inputs are mentioned in figure b. This displays the PIN specific arrangement of the PII images. It takes input of the selected PII image indexes and transfers them to the Middle ware.

2. Thick Middle ware: Both middle ware and application layer physically exist on the same system (e.g. ATM Machine). Complete logic is implemented through proposed middle ware due to which it is termed as thick middle ware. PII and salt cryptography modules are its embedded parts.

3. Storage Server: This is preferably a remote storage, backing up all the registered data. A new entry is created for new registrations and access queries are generated if a match is successful. This also serves the back-end purpose for database matching. It matches the query saltcrypted template prepared by the middle ware with all the stored saltcrypted templates. A user is authenticated if the distance is less than a predefined threshold.

All the three abstraction modules of proposed system architecture is shown in fig.2 The multitier architecture of proposed system is shown in fig.3



TIER I:
PIN is used to uniquely arrange PII images. Binary PIN is embedded in the Saltcrypted template using bit replacement method for further authentication.

TIER II:
The seed for PN sequences is generated from the used ID based selected pixel values of PII images which makes the process entirely user dependent.

TIER III:
The binary template is mixed with user specific salt to create saltcrypted template and then PIN is embedded into it. PIN is not communicated to the storage server.

Figure 3: Multi-tier security architecture

6 Proposed algorithm:

This paper proposes a method to secure the biometric template using salted cryptography where biometric traits i.e. fingerprint is stored in the form of transformed template. We are targeting the key release mode where a secret key is released for further authentication to any other system if the query and stored templates matches. The main objective behind the proposed method is not to store the actual template in the system with user need to remember only ATM PIN which is almost equivalent to the ATM scenario at present. The algorithm for enrollment of user and selection of PII is given as under:There are two phases: Registration phase and matching phase.

6.1 Steps for phase I(Registration/Enrollment Phase):

Inputs:

- User ID
- Secret password (e.g. ATM PIN).
- PII image selection.
- biometric samples.

1. During enrollment phase biometric samples are taken let theses two samples be f1 and f2.
2. User ID and corresponding secret key (password) is taken from the user for registration.

3. Personal image registration: User is asked to select the personal image from uniquely arranged images on the basis of input password. Here three images are selected by the user from given set.
4. User ID of the customer is used to locate and extract the PII seed of the Pseudo-random (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.
5. Salt is generated using this seed for PN sequence generator after resetting the generator state.
6. Individual binary templates are combined and mixed with salt. The resultant saltcrypted template is stored.So no original templates are being stored.
7. Password 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.
8. Now f3=f1 XOR f2 and f4=f3 XOR salt, this f4 will be stored.
9. Embed the secret PIN binary sequence inside the salted template f4 by simple bit replacements at locations determined by an insertion guidance sequence.
10. Store the embedded salted fingerprints

6.2 Steps for phase II(Matching):

Inputs:

- User ID
- Secret password (ATM PIN)but no need to communicate with Storage server, only needed for PII image arrangement
- biometric samples

Steps of algorithm is as under :

1. During Verification phase biometric samples are taken f1, f2.
2. User is asked to enter the user ID and Password.
3. PII images are arranged in order dependent on the password PIN. This arrangement will be same as arrangement during registration only if the password entered by the user is same registered password.
4. PII key will be extracted from the images at the stored indexes in the arrangement.
5. The PN sequence generator seed is extracted from the pixel locations determined by user ID from the selected three images.
6. Salt is generated by seeding PN sequence generator by seed in step 5.
7. Salt is mixed with binary query templates to create saltcrypted query template f4. Now f3=f1 XOR f2 and f4=f3 XOR salt
8. f4 is matched with all stored saltcrypted templates T.
9. Bit Distance and correlation is found between these binary templates.

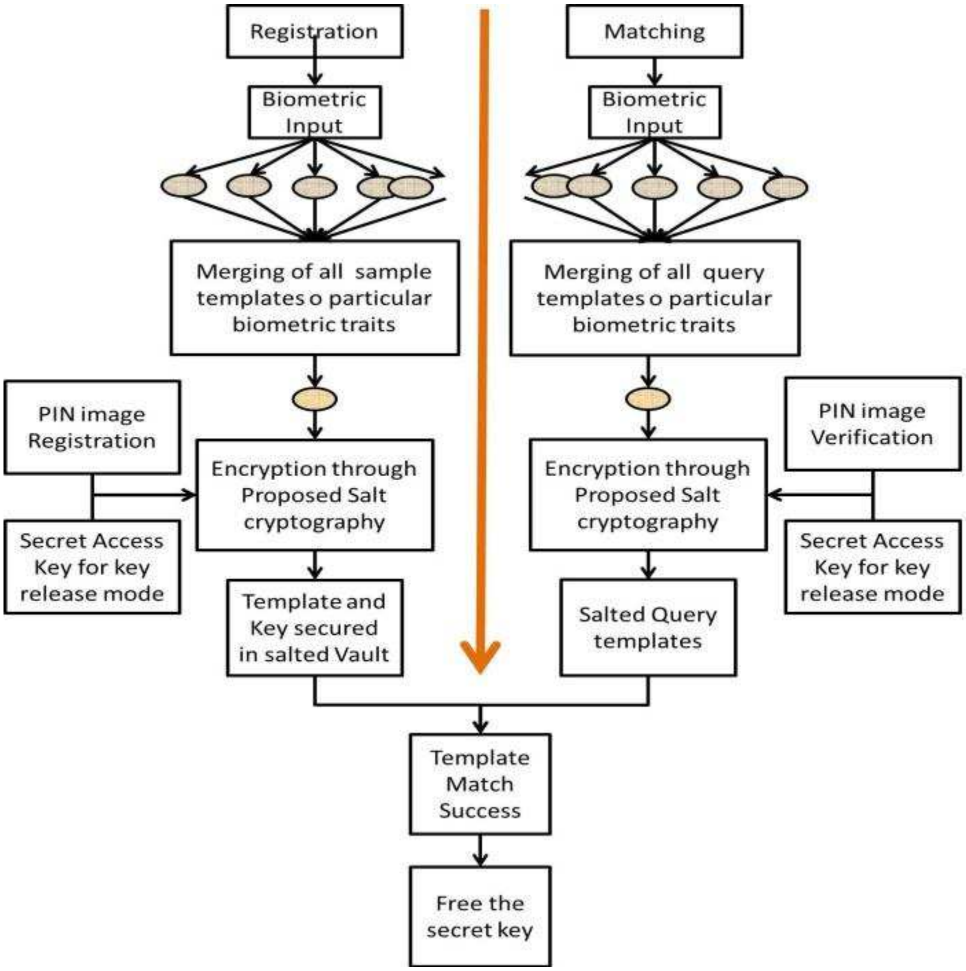

Registration
Biometric Input
Merging of all sample templates o particular biometric traits
PIN image Registration
Encryption through Proposed Salt cryptography
Secret Access Key for key release mode
Template and Key secured in salted Vault
Matching
Biometric Input
Merging of all query templates o particular biometric traits
PIN image Verification
Encryption through Proposed Salt cryptography
Secret Access Key for key release mode
Salted Query templates
Template Match Success
Free the secret key

Figure 4: Proposed algorithm(Phase-I registration,Phase-II Matching phase)

10. The stored templates with which the distance is minimum and correlation is maximum and also less than a match qualifying threshold is termed as match.

11. If match occurs then the PIN is extracted from the embedded saltcrpyted template and used for further authentication needs.

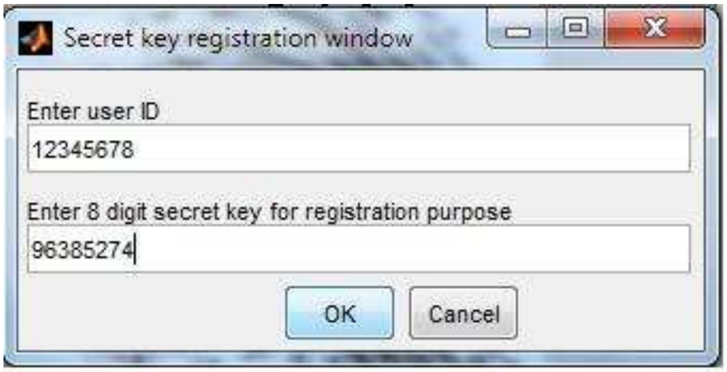
Fig 4 shows the flowchart of both registration and matching process. This scheme can be compared to cancellable biometrics[2] where a transformation of the actual template is stored in the system not the actual template. Still complete template exists on the system in a permuted form which is reversible to generate the actual template whereas proposed method is completely irreversible with no secret information stored in the system. Another advantage that proposed method adds is multiple tiers of security. The system is secured using a secret PIN as it is done in present systems PINs are traditionally stored as encrypted numbers but here it is done without storing the secret PIN in any form. Next tier of security is added by proposed method through involving personal selection of the PII images by users. A unique arrangement of images is created on the basis of input password PIN. The indexes of the selected images are stored only. If any intruder steals these indexes even then he cannot detect any useful information regarding the PIN.
The PIN embedded into the saltcrypted template is freed only if the templates match. There will be no matching of the extracted PIN and PIN input during query. The query PIN is known only to the middle-ware. No transfer of PIN occurs between the middle-ware and storage server. Similarity of the PINs is implicit only if the extracted PIN is authenticated successfully.

Figure 5: input fingerprint sample

7 Simulation results:

Single modality (fingerprint) and multiple instances have been used. For this we have chosen the images of two fingers (index finger and thumb). User has no need to remember order of fingers during sampling process. Fig 6 shows ID and Key registration window fig. 7 displays the Personal image selection window that is used for selecting personal images out of the given images at the time of enrollment. The algorithm has been simulated in MATLAB v12.The algorithm has been tested on 1242 persons fingerprint images obtained from several data sets[10].Another data sets used for fingerprint biometric are 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 fingerprints images are shown in figure 5. Randomly selected 1000 images were used to train the system. Each of the persons has enrolled his 5 fingers. Proposed algorithm is trained for thumb and index fingers out of the five. Remaining images are used for checking of false acceptances. 100000 random trial runs of the MATLAB simulation of the proposed algorithm are conducted, where images are selected randomly from the available images. Multiple instances of a single trained person are also tested to check system behavior towards false rejection. The training and matching has been done using the algorithms proposed in previous section. The matching is done using two parameters, first is bit by bit matching. This is used to identify local noise at bit level. Another method used is 2D-correlation; here both the query and the stored template are correlated with each other to get the similarity. Templates with highest similarity are the target match. A valid match only occurs if value of similarity is higher than 0.65 obtained through several experiments.

False acceptance rate (FAR): This is defined as the number of times a fingerprint is taken as a match even it is of some other person.



Secret key registration window

Enter user ID

12345678

Enter 8 digit secret key for registration purpose

96385274

Figure 6: ID and key registration window

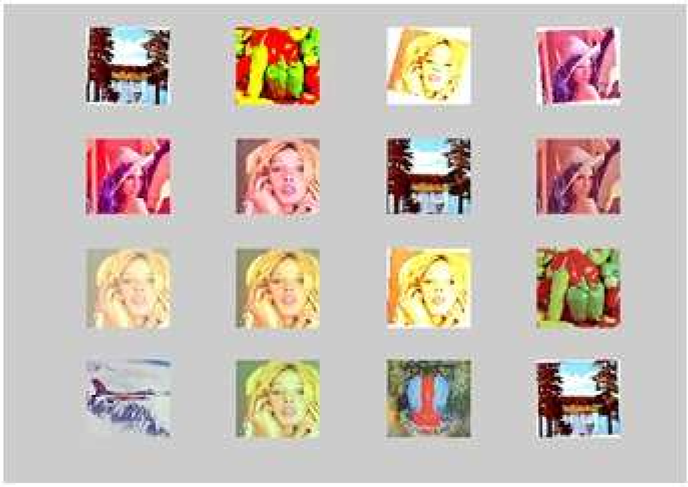


Figure 7: Personal image selection window

FAR=False accepted queries/Total Queries False rejection rate (FRR): It is the number of times a fingerprint of the genuine person is declared unmatched.
FRR=False rejection queries/Total Queries
FAR is 0.002% which may be due to bad quality of some fingerprint images. This is dataset problem and can be filtered if the fingerprints templates are taken properly. FRR is 0.016Table 1 shows the comparison results for the FAR and FRR of the proposed algorithm with other approaches. The results are satisfactory to prove the proposed method a successful biometric recognition method. Table 1: Comparison of the FAR and FRR with recent approaches.
Results in Terms of Accuracy: Fig 8 presents accuracy comparison of the proposed algorithm with other methods and found satisfactorily matching with previous approaches. AC=100- (FAR+FRR)/2 fig. 9 shows the salted and merged template after the key is embedded in it.

8 Analysis:

Average noise added to salted template can be estimated through Peak Signal to Noise Ratio (PSNR). More the noise added in the signal in comparison with the original signal lesser is the PSNR. The average PSNR of the proposed algorithm is 71.12 dB which is very high. This PSNR is enough to hide the Key inside the template

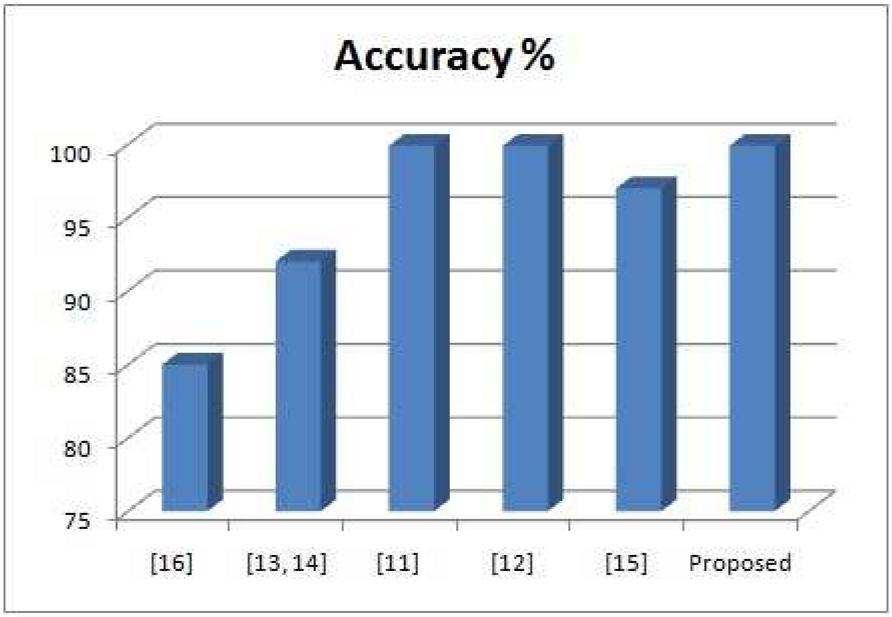


Figure 8: Accuracy comparison of various approaches

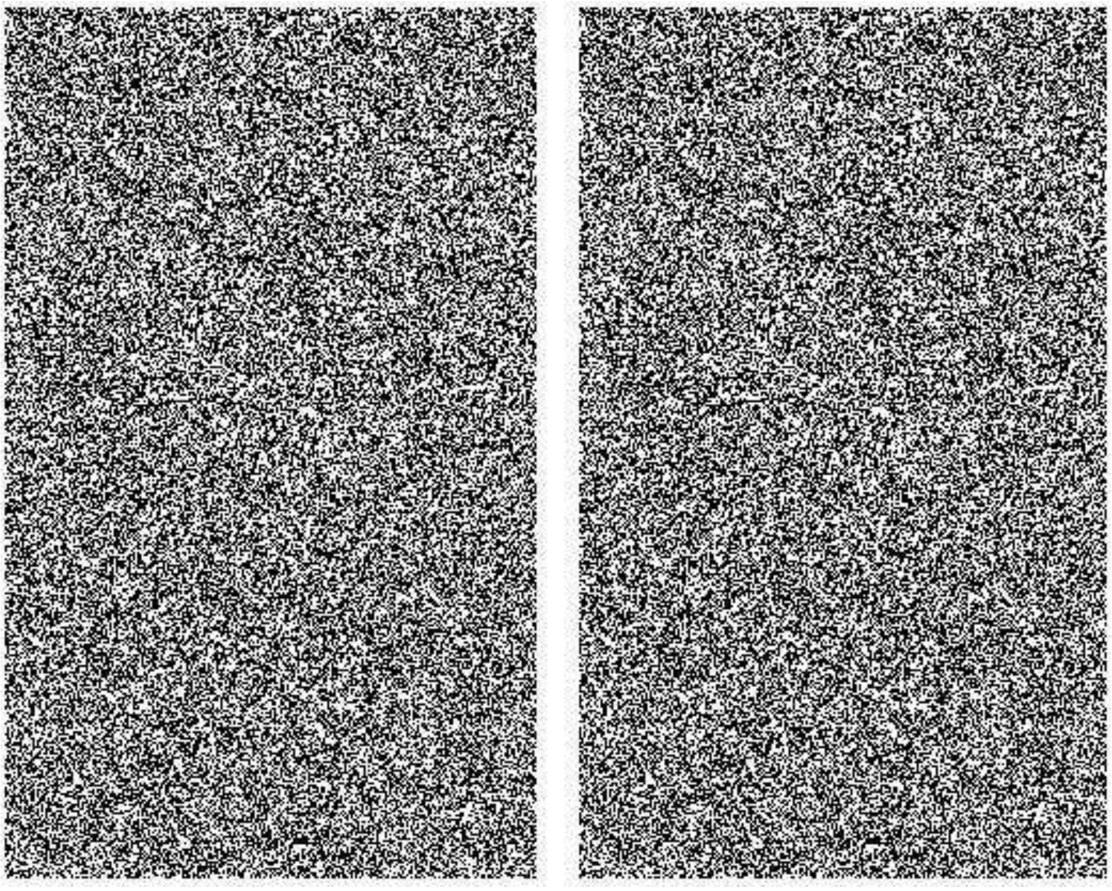


Figure 9: (a)Salted and merged template (b) Embedded saltcrypted template

Approach	FRR	FAR
[11]	0.0016	0.05
[12]	0	0.21
[13,14]	7.1	7.15
[15]	4	2
[16]	14.1	15.98
proposed	0.002	0.16

Table 1: Comparison of FAR and FRR of proposed scheme and recent approaches

without being detected because of quality. **Analysis:** The major advantage of the algorithm is the complexity of detection of actual template from the salted template using brute force attack.

1. Fingerprint image size = m*n
2. Salt1 size = m*n
3. Salt2 size = bin_key_length= L =64 bits
4. Computational Complexity to know exact salts= 2^{m*n+L}= O(2^{n^2+L})if m==n
5. Complexity of whole approach =O(m*n)
   If m==n then O(n^2)
6. Complexity of Embedding and extraction O(L)
7. Complexity to find exact embedding locations

- No. of images in PII database=P=16
- No. of different arrangements = P!
- No. of images selected = k = 3
- Image Selection ways =$\binom{P}{k}$*P!
- of digits in user ID = N
- Complexity of extracting user dependent info from the PII images using brute force attack = $\binom{P}{k}$*P!*10^N= seed generation complexity, here 10 is for base of decimal digits.

Now the proposed method needs to be compared with state of the art methods for template encryption. The complexities of Rivest-Adleman-Shamir (RSA), Advance Encryption Standard (AES), Digital Encryption Standard (DES) and Triple DES and other cryptography methods used in literature are larger than the proposed algorithm. The RSA algorithm, public key operations take O(n^4) steps, private key operations take O(n^6) steps, and key generation takes O(n^8) steps, where n^2 is the number of bits in the modulus. Attack on AES works on the 8-round version of AES-128, with a time complexity of 2^{48}, and a memory complexity of 2^{32} [17] which is much easier to do in comparison to the proposed method. The mathematical process is also easier than existing processes to be implemented in hardware and low cost devices.DES is generally at least 100 times as fast in software and between 1,000 and 10,000 times as fast in hardware but Differential-linear-crypt analysis attack can break 9-round DES with $2^{15.8}$ chosen plain texts and has a $2^{29.2}$ time complexity which is very less than the proposed work since linear crypt analysis needs the key bits that have a high bias but in proposed method it is impossible to reach to a high bias key guess. Triple-DES usually needs thrice the computing power as DES with complexity O(n^2).Blowfish is known for its quite slow key schedule so quite slow for comparison. Overall, the combination of PII image and salted templates make the exact PN sequences determination impossible.

9 Conclusion and future work:

The proposed algorithm has shown advantage in terms of complexity and compared to standard algorithms. The approach has very less complexity when it is required to implement on low cost hardware O(n^2) like fingerprint sensing devices. On the other hand the seed generation and localization of the secret key in the salted templates are is near to impossible to achieve if exact secret keys and the generation algorithms are unknown, so intrusion is almost impossible.Another advantage is that there is no point of time where the actual fingerprint templates 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 no where. The comparison of the stored saltcrypted template and query saltcrypted template is done and the embedded key is released only if they match. There is no need to remember the PII images by the user as it was mandatory in the original PII algorithm. The future work lies to improve the performance of the algorithm if the fingerprints are sampled and queried in different seasons. This is a common problem with fingerprint biometric modality. This approach is simplest and can be applied to any other biometric modality like vein images, iris patterns etc. We are currently evaluating this algorithm on other modalities. Results are in pipeline for publishing.

10 Acknowledgment

I would like to thank my organization Geetanjali Institute of technical studies for making all the resources available to carry out this work.I would like to thank everyone who helped me directly or indirectly to make this work possible.

References

[1] A. Jain, A. Ross, and U. Uludag,"Biometric template security:Challenges and solutions",In Proceedings of European Signal Processing Conference (EUSIPCO), 469-472,(2005).

[2] N.K.Ratha,S.Chikkerur,J.H.Connell, R.M.Bolle,"Generating cancelable fingerprint templates", IEEE Transactions on Pattern Analysis and Machine Intelligence29 (April 2007).

[3] C.S.D.Roberge,A.Stoianov, R.Gilroy,B.V. Kumar,"Biometric encryption",ICSA Guide to Cryptography, ch. 2 (1999).

[4] A.T.B.Jin,D.N.C.Ling,A.Goh," Bio-hashing: two factor authentication featuring fingerprint data and tokenized random number", Pattern Recognition Issue 11(37),2245-2255 (2004).

[5] F.Monrose,M.K.Reiter,S.Wetze,"Password hardening based on keystroke dynamics", International Journal on Information Security 1, 69-83 (2002).

[6] A.Juels,M.Wattenberg,"A fuzzy commitment scheme",6th ACM Conference on Computer and Communications Security, pp. 28-36 (1999).

[7] E.Verbitskiy,P.Tuyls,D.Denteneer,J.P.Linnartz,"Reliable biometric authentication with privacy protection" 24th Benelux Symp. on Info. Theory (2003).

[8] B.Santhi,K.Ramkumar "Novel hybrid Technology in ATM security using Biometrics" Journal of Theoretical and Applied Information Technology, Vol. 37 No.2 ISSN: 1992-8645.

[9] http://www.nist.gov/index.html

[10] FVC2004 fingerprint database.

[11] D.moon,S.Lee,S.Jung,Y.Chung,M.Park,O.Yi"Fingerprint Template Protection Using Fuzzy Vault"Computational Science and Its Applications ICCSA 2007,International Conference, Kuala Lumpur, Malaysia, August 26-29, 2007. Proceedings. Part III pp 1141-1151

[12] U.Uludag,S.Pankanti,A.K.Jain,"Fuzzy Vault for Fingerprints." AVBPA 2005. LNCS, vol. 3546, pp. 310-319(2005)

[13] T.B.Long,L.H.Thai,T.Hang,"Multimodal Biometric Person Authentication Using Fingerprint, Face Features" PRICAI 2012,LNAI 7458 pp 613-624 2012.

[14] H.A.Qader,A.R.Ramli,S.A.Haddad,"Fingerprint Recognition Using Zernike Moments", The International Arab Journal of Information Technology, 4(4) (October 2007)pp.372-376.

[15] R.Shrivastava,S.Thakur "Performance Analysis of Fingerprint Based Biometric Authentication System using RSA",Engineering Universe for Scientific Research and Management vol. 6 ,Issue 2 Feb. 2014

[16] H.Benaliouche,M.Touahria "Comparative Study of Multimodal Biometric Recognition by Fusion of Iris and Fingerprint" The Scientific World Journal Volume 2014, Article ID 829369.

[17] H.Gilbert,T.Peyrin (2009-11-09). "Super-Sbox Cryptanalysis: Improved Attacks for AES-like permutations". Retrieved 2010-03-11.