Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Novel approach for securing biometric template

Shweta Malhotra
Department of computer Science & applications
Kurukshetra University, Kurukshetra, India.

Dr.Chander Kant
Department of computer Science & applications
Kurukshetra University, Kurukshetra, India.

***Abstract-** Template and database are critical parts of biometric systems. Attacker usually afflict biometric template. There can be various attacks on different modules of biometrics system and communication links among them. Securing templates from these attacks have become very important or imperative issue. Security is achieved by methods of cryptography, which deals with encryption of data. Encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In this paper, we present an approach to enhance the invisible watermarking technique with cryptography. The biometric trait is modified using invisible watermark information and is further secured using cryptography. The encryption algorithm which has been used is highly suitable for multimedia as well as text data. We can use different encryption techniques like AES, MAES etc .The template is made more secure using encryption and finally stored in database.*

***Keyword-** biometric template security, biometric cryptosystem, template protection, invisible watermarking approach.*

I. INTRODUCTION

The process of identifying an individual using security systems is called authentication. It simply ensures that the individual is who he or she claims to be, but tells nothing about the access rights of the individual. Current authentication methods can be classified into three main areas [1]

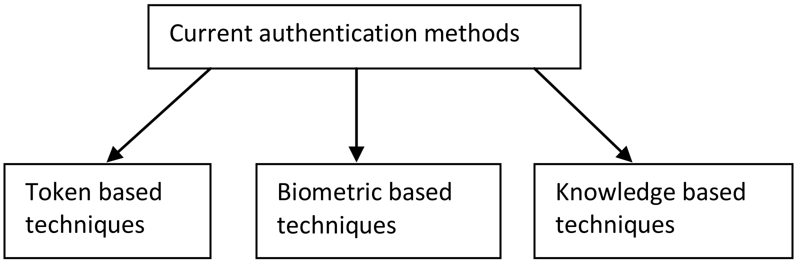

Current authentication methods
Token based techniques
Biometric based techniques
Knowledge based techniques

Figure 1: Current authentication methods

Token based techniques are widely used for authentication using key cards, bank cards and smart cards. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number. Knowledge based techniques are the most widely used authentication techniques. These techniques include both text-based and picture-based passwords. Biometric based authentication techniques uses a biometric authentication system which is essentially a pattern recognition system that operates by acquiring biometric data from an individual such as fingerprints, iris scan, or facial recognition, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. However, this technique provides highest level of security. Passwords and cards can be shared and thus cannot provide reliability. Biometric identifiers cannot be shared, misplaced, and they intrinsically represent the individual's identity [2]. Consequently, biometrics is not only an important pattern recognition research problem but is also an enabling technology that will make our society safer, reduce fraud and lead to user convenience. Templates are used during the biometric authentication process where a biometric template (or simply template) is a digital reference of distinct characteristics that have been extracted from a biometric sample. A biometric authentication system mainly comprises following functional units. Sensor device for acquisition of biometric raw data, feature extraction for template creation, matcher to compare the actual biometric template with the stored templates and system database for storing the biometric templates.

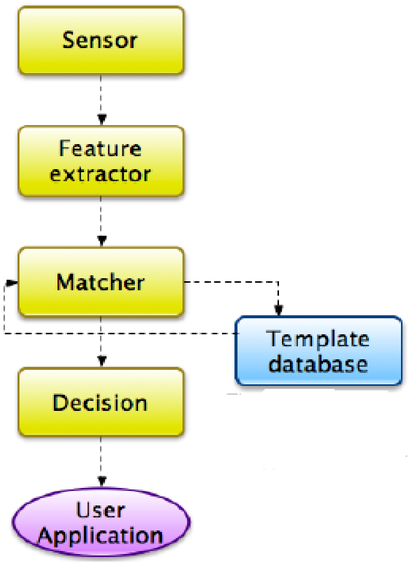


Figure 2: Basic biometric authentication system

Biometric systems serve one of two foundational purposes either verification/authentication or identification. Identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file (using only the biometric data). This is often referred as a "one-to many" match. Biometric verification or authentication involves a "one-to-one" search whereby a live biometric sample presented by an individual is compared to a stored sample (on a smart card or contained in a database) previously given by that individual and the match confirmed.

The biometric system can also be attacked by the outsider or unauthorized person at various points. These points can be listed as under [3]:

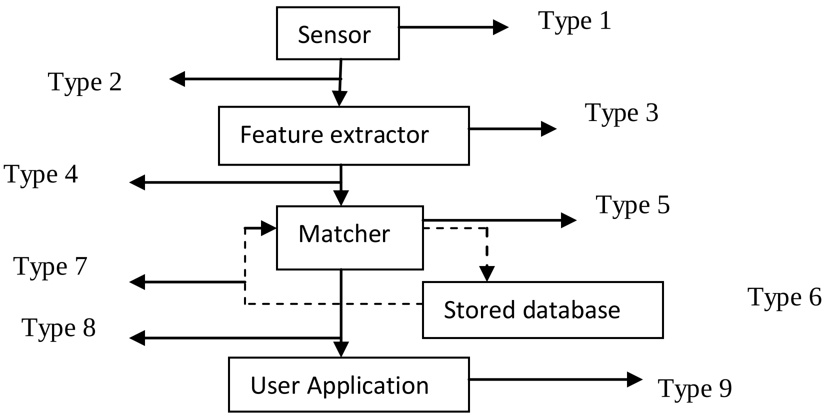


Figure 3: Various Attacks in biometric system

Type 1: The attack on sensor module. Physically destroying scanner or fake the recognition and cause a denial of service. Type 2: The attack on the channel between sensor and feature extractor. Biometric traits are stolen and stored somewhere else. Type 3: The attack on feature extractor module. The attacker using Trojan horse sends some selected features to matcher module. Type 4: The attack on channel between feature extractor and matcher. The attacker steals feature values and resends them to the matcher module later. Type 5: The attack on matcher module. The matcher module is replaced with a Trojan horse which can produce the high or low matching score. Type 6: The attack on the stored database. The attacker modifies database where all the templates are stored. Type 7: The attack on the channel between system database and matcher. The attacker either steals replays or alters the data. Type 8: The attack on channel between matcher and user application. The attacker either steals replays or alters the data. Type 9: The attack on user application.

When a biometric system is compromised, it can lead to following effects [1] [3]:

Denial of Service: It is an attempt to make system resources unavailable to its intended users. Circumvention: The act of prevailing over another by arts, address, or fraud. The authorized user does not get access to resources. Repudiation: Act, intention or threat of disowning or rejection of an agreement already accepted or agreed to. Covert acquisition: Here the knowledge of authorized person has been stolen and used by the intruder. Collusion: In order to cheat, a secret agreement between two parties which helps the intruder to modify the system‘s parameter to permit incursions. Coercion: The act of compelling by force of authority. An authorized user is compelled by intruder to give him access to the system

II. Related Work

To overcome all the above effects and attacks, various protection schemes have been defined. The major challenge in designing a biometric template protection scheme is the need to handle intruder variability in the acquired biometric identifiers. To handle intruder variability, an ideal biometric template protection scheme should possess the four properties diversity, revocability, security, performance. [1][3].

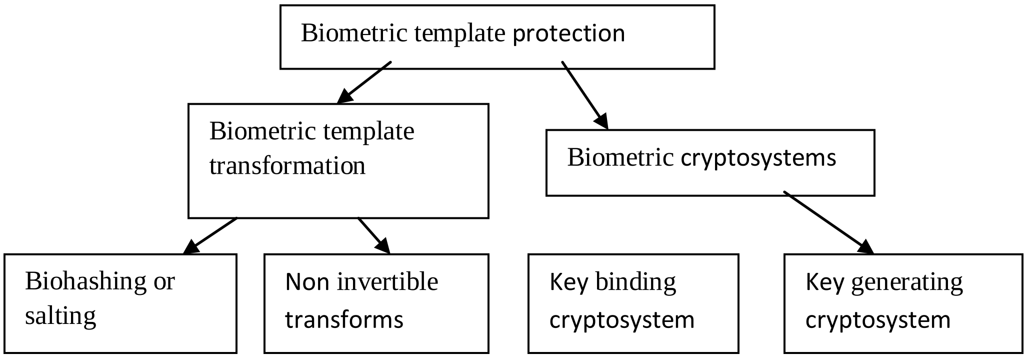

Biometric template protection
Biometric template transformation
Biometric cryptosystems
Biohashing or salting
Non invertible transforms
Key binding cryptosystem
Key generating cryptosystem

Figure 4: Various biometric protection techniques.

Biometric cryptosystem: In these techniques, the biometric template is encrypted using an encryption key, possibly derived from a password, during enrollment. During authentication, the stored data is decrypted using the corresponding decryption key and is matched with the captured query. Two different kinds of encryption techniques can be used: symmetric and asymmetric. The symmetric encryption, such as the Advanced Encryption Standard (AES), is the simplest form of encryption where the decryption key is the same as the encryption key but in case of asymmetric encryption, both the keys are different. Since the encryption key may be discarded after constructing the secure template, the adversary would not be able to replace the existing encrypted templates even if he steals the decryption key. Key binding cryptosystem: The key-binding cryptosystem is the simple encryption scheme in which the template is secured by binding it with a key .The same key is used to extract the biometric trait from encrypted data. A number of other template protection techniques like fuzzy vault [4], shielding functions [5], and distributed source coding [6] can be considered as key binding biometric cryptosystems. The fuzzy vault scheme proposed by Juels and Sudan [4] has become one of the most popular approaches for biometric template protection and its implementations for fingerprint, face, iris, and signature modalities have been proposed.

Key generating cryptosystem: The Key generating cryptosystem involves generation a key from biometrics trait. It is an attractive approach but also difficult problem which suffers from low discriminability. Discriminability refers to number of different keys which can be generated by the same biometric features. Biometric key generation schemes introduced by Chang et al. [7] and Veilhauer et al. [8] employed user-specific quantization schemes. Dodis et al. [9, 10] introduced the concepts of *secure sketch* and *fuzzy extractor* in the context of key generation from biometrics. Further, Li and Chang [11] introduced a two-level quantization-based approach for obtaining secure sketches. Sutcu et al. [12] discussed the practical issues in secure sketch construction and proposed a secure sketch based on quantization for face biometric. The problem of generating fuzzy extractors from continuous distributions was addressed by Buhan et al. [13]. Secure sketch construction for other modalities such as fingerprints, 3D face, and multimodal systems (face and fingerprint) has also been proposed. Various protocols for secure authentication in remote applications [14, 15] have also been proposed based on the fuzzy extractor scheme. Biometric template transformation: In these techniques, during enrollment, the template is transformed using the user’s password and during authentication, the query is also transformed using the same password before being matched with the transformed template. Salting, the transform is invertible, so the security is based on the function which is defined by user specific key or password. In this technique, the authors first extract the most discriminative projections of the face template using fisher discriminant analysis [17] and then project the obtained vectors on a randomly selected set of orthogonal directions. This random projection defines the mechanism for the scheme called salting. This technique was proposed by teoh.et.al [16][17]. Non-invertible transform is as the name specifies not invertible. It is a one-way function where it is very difficult to invert a transformed template to original template even if the key is known. [18] Ratha et al. [19] proposed and analyzed three noninvertible transforms for generating cancelable fingerprint templates. The three transformation functions are cartesian, polar, and functional. These functions were used to transform fingerprint minutiae data such that a minutiae matcher can still be applied to the transformed minutiae. [20][21]

III. Invisible watermarking technique

In this system, we used the watermarking for security of biometric template. Biometric template can be replaced or forged by attacker. But, in this system, if attacker tries to replace or forge the biometric template then he must have the knowledge of pixel values where watermark information is hidden. If attacker changes the secure biometric template (i.e. Biometric template with watermark information) with forge biometric template then it gives the clue to database manager that something has gone wrong with biometric template because in forge biometric template either the watermark will not be present or will be present at wrong pixel positions. For the insertion of watermark information in biometric template the Parity Checker Method has been used [22]. Also, the watermark information has been inserted four times in biometric template so that if attacker is able to change watermark at one place, the watermark at other places remain intact. The process of securing the biometric template is shown in figure 5. [23]

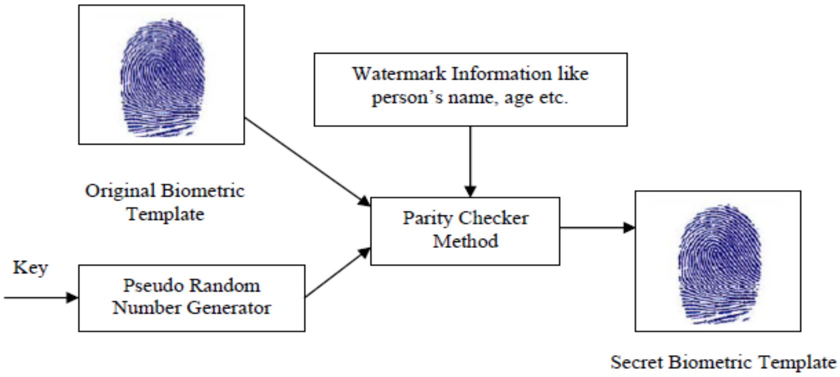
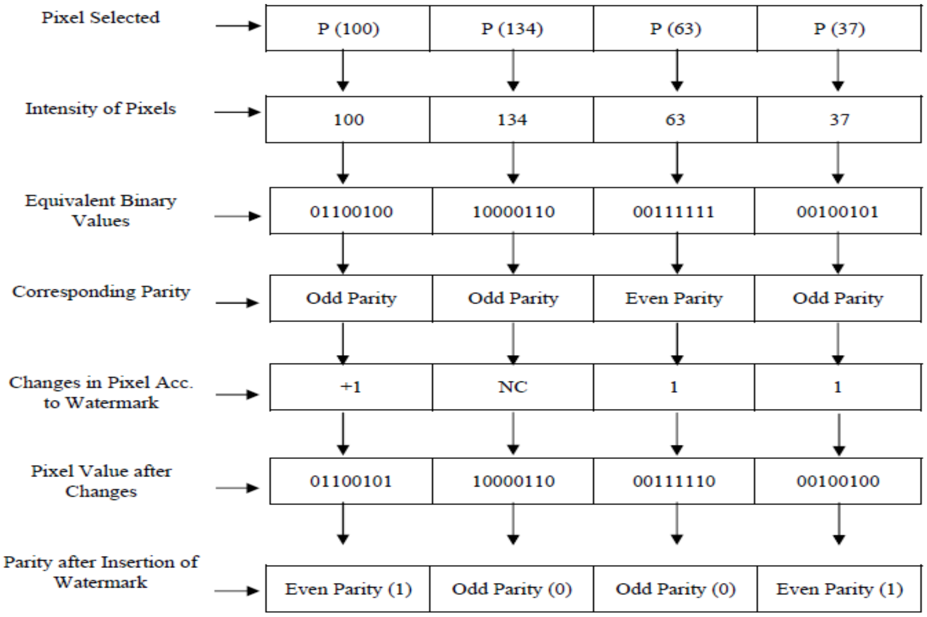

Watermark Information like person's name, age etc.
Original Biometric Template
Parity Checker Method
Key
Pseudo Random Number Generator
Secret Biometric Template

Figure 5: Invisible watermarking technique.

Algorithm:

I. Step 1: Read the watermark information that we want to hide in the biometric template.
II. Step 2: Read the biometric template
III. Step 3: Find out the pseudorandom pixel location in the biometric template where watermark is to be inserted by using pseudorandom number generator which is seeded with the secret key.
IV. Step 4: If at a pixel location we want to hide 0, then go to step 5 else go to step 6.
V. Step 5: a) Check whether there exists odd parity at the selected pixel location, then insert 0 at the pixel location (no change in pixel value is required in this case). Go to END. b) If even parity exists, then make the odd parity at that location by adding or subtracting 1 to that pixel location (change in pixel is required in this case). Go to END.
VI. Step 6: a) Check whether there exists even parity at the selected pixel location, then insert 1 at the pixel location (no change in pixel value is required in this case). Go to END. b) If odd parity exists, then make the even parity at that location by adding or subtracting 0 to that pixel location (change in pixel is required in this case). Go to END.
VII. Step 7: END.



Pixel Selected	P (100)	P (134)	P (63)	P (37)
Intensity of Pixels	100	134	63	37
Equivalent Binary Values	01100100	10000110	00111111	00100101
Corresponding Parity	Odd Parity	Odd Parity	Even Parity	Odd Parity
Changes in Pixel Acc. to Watermark	+1	NC	1	1
Pixel Value after Changes	01100101	10000110	00111110	00100100
Parity after Insertion of Watermark	Even Parity (1)	Odd Parity (0)	Odd Parity (0)	Even Parity (1)

Figure 6: an example for watermarking insertion.

IV. PROPOSED WORK

The paper presents a novel approach for securing biometric template using invisible watermarking approach and cryptography. The watermarking avoids the forging and replacement of biometric template by the attacker. But there is a very less change in the original template and hence changes in a few pixels by the attacker will lead to insecure biometric template. To enhance the security of the template, cryptography is applied. The template is mixed with a random generator (key) which is further applied with watermarks using parity checker method [23]. This template is encrypted using encryption algorithm. This will help to reduce the robustness of previous system.

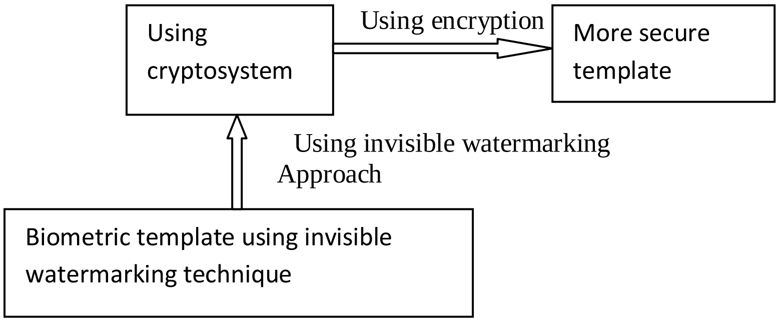

Using cryptosystem
Using encryption
More secure template
Using invisible watermarking Approach
Biometric template using invisible watermarking technique

Figure 7: Basic approach for proposed work.

A. Architecture

The architecture of the proposed approach is described as in figure 8. The proposed approach is based upon two approaches cryptography and invisible watermarking technique [22, 23]. As biometric system defines two phases i.e. template enrollment and template authentication, our proposed approach works in these two phases. During biometric enrollment, the biometric trait is sensed by the sensor module, the feature extractor module extracts the characteristics features.

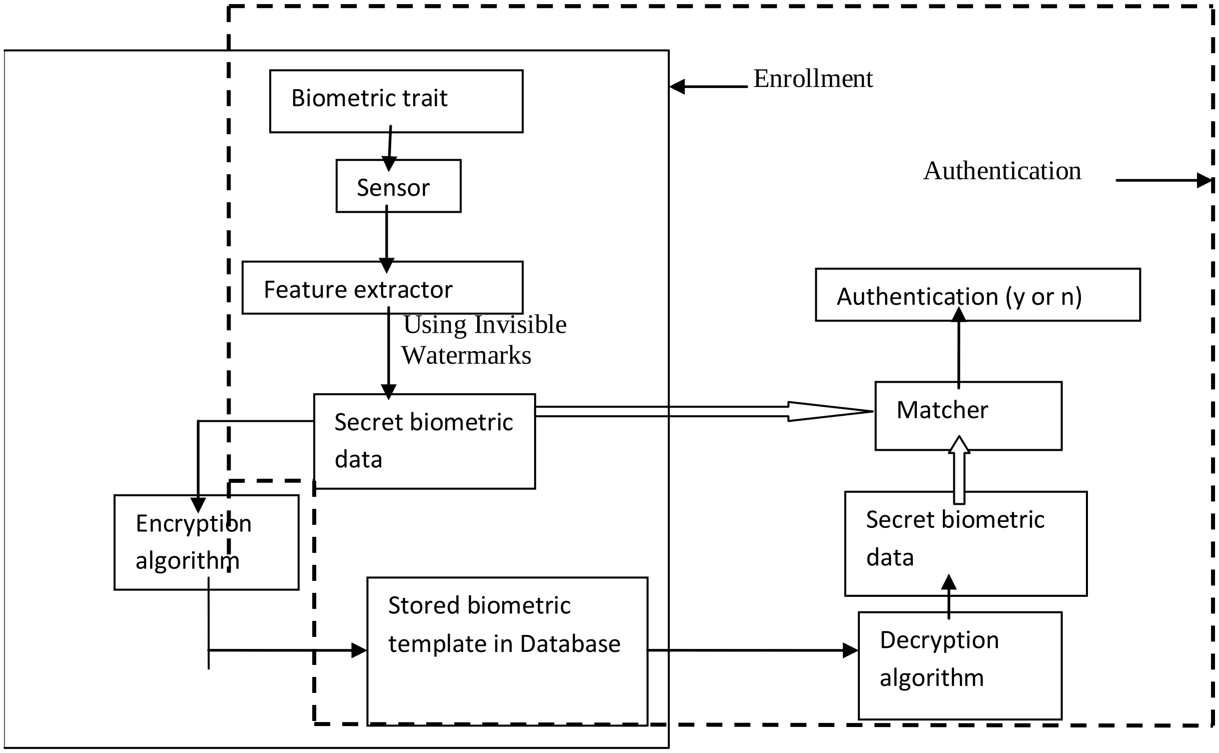


Figure 8: Architecture of proposed work.

1) Encryption algorithm: The following encryption algorithm has been used for cryptography. It is used because of its simplicity as it uses matrix multiplication and inversion for enciphering and deciphering, its high speed, and high throughput an encryption technique in which a key can be generated for the encryption of a biometric template. This algorithm generates the different key matrix for each block encryption instead of keeping the key matrix constant. This

increases the secrecy of key. The new matrix we obtain after modification of the key matrix is called the encryption matrix [25].

1. Let ID be the unique identification number of the individual (Assume ID = 7)
2. Generate a random number R in range [2, ID] (Assume R = 5)
3. Create a magic matrix of random size key X key, where key = R X ID (then key = 7 X 5 = 35 and random Magic matrix = 35 X 35)
4. Add magic matrix with template to create BE template.
5. Shuffle the BE template

2) Decryption Algorithm: The following decryption algorithm has been used.

1. Read BE template from the database corresponding to the ID. (E.g. retrieve the BE template corresponding to the ID = 7)
2. Rearrange the BE template in the original order.
3. Subtract the new Template so created at the time of authentication from original BE template.
4. Then the difference matrix should satisfy preset threshold value.
5. The size of the magic matrix is retrieved (key retrieved = 35).
6. Key is divided by ID, if result obtained through division lies in the range [2, ID], and then the user is authenticated. (Here result = 35/7 = 5 which lies in the specified range).
7. After subtracting magic matrix from BE template, it is matched with the new template in order to make the system more robust.

3) Matcher: The matcher helps us to authenticate the right person. The new biometric is matched with the stored template. If the matching value is less than the threshold value then the person is not authenticated.

B. Proposed protection scheme theoretical results

The major challenge in designing a biometric template protection scheme that satisfies all the below mentioned requirements is the need to handle intruder variability in the acquired biometric identifiers. The proposed protection scheme also satisfies these properties and hence is an ideal approach.

1) Diversity: It means understanding that each individual is unique, and recognizing our individual differences. The proposed protection scheme provides uniqueness for each and every template. Many Different templates can be formed using the proposed approach.
2) Revocability: It means to review. The proposed protection scheme has ability to reissue a new data based on the same biometric data as different watermarks can be added to same biometric trait.
3) Security: The prevention of template and protection against danger. Using proposed protection approach it is computationally hard to obtain the original biometric template from the secure template as the data is modified two times (using invisible watermarking approach and cryptography). Hence stealing of data is difficult.
4) Performance: The biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system. The proposed protection approach provides good performance.

V. **Conclusion**

In this paper, we have applied cryptography on biometric template which have already been modified using invisible watermarking approach. The biometric template is much more secure than before as there was just little change in biometric template using parity check method used in watermarking technique. Here the modified data is encrypted and hence while decryption real data is not exposed which also overcomes encryption disadvantage. It provides good security and is suitable for any large scale data. In future, we can apply these techniques to different attack areas to protect attacking on these areas**.**

References

[1]. Wikipedia, http://www.wikipedia.org/, http://en.wikipedia.org

[2]. A. K. Jain, R. Bolle, and S. Pankanti, eds., *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Publishers, 1999.

[3]. Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2008, Article ID 579416, 17 pages doi:10.1155/2008/579416 "*Review Article* Biometric Template Security "Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar.

[4]. A. Juels and M. Sudan, "A fuzzy vault scheme," in *Proceedings of the IEEE International Symposium on Information Theory*, p. 408, Piscataway, NJ, USA, June-July 2002.

[5]. P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis, "Practical biometric authentication with template protection," in *Proceedings of the 5th International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA '05)*, vol. 3546 of *Lecture Notes in Computer Science*, pp. 436–446, Hilton Rye Town, NY, USA, July 2005.

[6]. S. C. Draper, A. Khisti, E.Martinian, A. Vetro, and J. S. Yedidia, "Using distributed source coding to secure fingerprint biometrics," in *Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '07)*, vol. 2, pp. 129–132, Honolulu, Hawaii, USA, April 2007.

[7]. Y.-J. Chang, W. Zhang, and T. Chen, "Biometrics-based cryptographic key generation," in *Proceedings of the IEEE International Conference on Multimedia and Expo (ICME '04)*, vol. 3, pp. 2203–2206, Taipei, Taiwan, June 2004.

[8]. C. Vielhauer, R. Steinmetz, and A. Mayerh¨ofer, "Biometric hash based on statistical features of online signatures," in *Proceedings of the International Conference on Pattern Recognition*, vol. 1, pp. 123–126, Quebec, QC, Canada, August 2002.

[9]. Y.Dodis, R. Ostrovsky, L. Reyzin, andA. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," Tech. Rep. 235, Cryptology ePrint Archive, February 2006.

[10]. Y. Dodis, L. Reyzin, and A. Smith, "Fuzzy extractors: how to generate strong keys from biometrics and other noisy data," in *Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '04)*, vol. 3027 of *Lecture Notes in Computer Science*, pp. 523–540, Interlaken, Switzerland, May 2004.

[11]. Q. Li and E.-C. Chang, "Robust, short and sensitive authentication tags using secure sketch," in *Proceedings of the 8th Multimedia and Security Workshop (MM and Sec '06)*, pp. 56–61, Geneva, Switzerland, September 2006.

[12] Y. Sutcu, Q. Li, and N. Memon, "Protecting biometric templates with sketch: theory and practice," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 503–512, 2007.

[13] I. Buhan, J. Doumen, P. Hartel, and R. Veldhuis, "Fuzzy extractors for continuous distributions," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security (ASIACCS '07)*, pp. 353–355, Singapore, March 2007. X.

[14] Boyen, Y. Dodis, J. Katz, R. Ostrovsky, and A. Smith, "Secure remote authentication using biometric data," in *Proceedings of the 24th Annual International Conference on Advances in Cryptology (EUROCRYPT '06)*, vol. 3494 of *Lecture Notes in Computer Science*, pp. 147–163, Aarhus, Denmark, May 2005.

[15] I. R. Buhan, J. M. Doumen, P. H. Hartel, and R. N. J. Veldhuis, "Secure ad-hoc pairing with biometrics: SAfE," in *Proceedings of 1st InternationalWorkshop on Security for Spontaneous Interaction (IWSSI '07)*, pp. 450–456, Innsbruck, Austria, September 2007.

[16]. 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 Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 1892–1901, 2006.

[17]. P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces versus fisherfaces: recognition using class specific linear projection," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 9, no. 7, pp. 711–720, 1997.

[18]. R. M. Bolle, J. H. Connell, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, vol. 35, no. 12, pp. 2727– 2738, 2002.

[19]. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 29, no. 4, pp. 561–572, 2007.

[20]. Y. Sutcu, H. T. Sencar, and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proceedings of the 7thMultimedia and SecurityWorkshop (MMand Sec '05)*, pp. 111–116, New York, NY, USA, August 2006.

[21]. A. B. J. Teoh, K.-A. Toh, and W. K. Yip, "2*N* discretisation of BioPhasor in cancellable biometrics," in *Proceedings of 2nd International Conference on Biometrics*, pp. 435–444, Seoul, South Korea, August 2007.

[22]. Rajkumar Yadav, Rahul Rishi & Sudhir Batra, "A New Steganography Method for Gray Level Images using Parity Checker",International Journal of Computer Applications (0975-8887) Volume 11-No. 11, December 2010

[23]. Rajkumar Yadav et al. / International Journal on Computer Science and Engineering (IJCSE)

[24]. D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Springer, Berlin, Germany, 2003. A.

[25]. biometric template encryption by A.K.Mohapatra1, Madhvi Sandhu2 IGIT,GGSIP University,Kashmere Gate,Delhi *Published in International Journal of Advanced Engineering & Application, Jan. 2010.*