International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 9 (2015) pp. 22765-22778

http://www.ripublication.com

A Survey on Biometric Template Security Schemes and Protection In Cloud Environment

Midhuna Jyothi R.[*] **N. Jeyanthi**
PhD Scholar, Associate Professor,
School of Information Technology and Engineering
VIT University, Vellore, Tamil Nadu
India ([*]e-mail: rmidhunajyothi@amaljyothi.ac.in)

Abstract

Rapid explosion of the biometric authentication systems into new domains each day has created security concerns all across the digital world. Among many known vulnerabilities and adversary attacks on biometric systems, tampering the template database is the critical one. Several biometric template protection techniques are in place exploiting the security features of cryptosystems, watermarking, steganography and biometric transformation at various levels and magnitude. This paper conducts an extensive survey on the significant biometric template security techniques, suggested and applied on different types of biometric systems. Also we discuss the security issues and measures for the cloud storage of biometric data which provides the greatest advantage of scalability.

Keywords: Biometric authentication system, template protection, security, cloud template storage

Introduction

The advent of reliable and efficient biometric authentication systems quickly overpowered the drawbacks and deficiencies of traditional digital authentication and security schemes. Consequently, biometric authentication systems were introduced into highly security sensitive and privacy sensitive applications to protect critical data. As like any security schemes, biometric authentication also faces severe threats, attacks and vulnerabilities apart from the selected biometric related and scheme related limitations.

There are some eight attack points on a biometric system and tampering template database is the crucial one among them. The template database attack includes identity theft, cross matching attack by tracking the individual in other applications , disclosure of sensitive private information, denial of service, replay attack etc.[1,2,3].

Literature Survey

The template database protection schemes so far devised can be categorized into:

A. Watermarking techniques
B. Template transformation techniques
C. Cryptographic techniques
D. Hybrid and multimodal techniques

A. Watermarking Techniques

Some of the relevant researches in applying watermarking techniques for biometric template protection were fragile invisible watermarking technique [4] and robust watermarking technique [24]

Fragile invisible Watermarking

Scheme of Implementation

Yeung and Minitzer [4] proposed a fragile invisible watermarking technique for fingerprint image verification with watermark insertion and extraction. At first the images were watermarked and then transformed into noise forms through chaotic functions. Later this can be retrieved by reverse transformation process and this extracted watermark could identify and locate tampering and illegal modifications on the biometric image.

Underlying principle

During insertion, the fingerprint image is implanted with a watermark image and pixel processing is done. For each pixel, a comparison between the values of required watermark and extracted watermark is made and if needed slight iterative modification is applied and the same is transmitted to unprocessed pixels. During extraction, a suitable extraction function on a suitable verification key [25] is calculated for different types of images. Each pixel is also subjected to this function and a watermark value is obtained which is then used for verification.

Detailed analysis

Features: (a) Implemented on fingerprint database

Advantages: No performance loss

Performance evaluation: Checked on 1000 fingerprint images[4] and showed almost the same accuracy as unwatermarked images [4]

Challenges: (a) The effectiveness will be application-specific. (b) Scalability need to be checked.

Robust Biometric Image Watermarking

Scheme of Implementation

The scheme by Vatsa etal.[24] has been implemented by merging DWT (Discrete Wavelet Transform) and LSB watermarking algorithms together with fingerprint as

the cover image and 2D Gabor filtered face template as the watermark. Two processes have been included- Watermark embedding and extraction. [24]

Underlying principle

During watermark embedding, the fingerprint image is applied with DWT twice and an approximation band is created. Then second LSB of the selected coefficient of the band is replaced by a bit of face template. A key has been created to find the cryptographic hash for blocks formed from selected bits. Face template is Gabor filtered [24] and then it is embedded in the fingerprint .Inverse DWT is applied to the embedded image to obtain the watermarked fingerprint image.

During watermark extraction, image synchronization is applied to the boundaries of the block. The cryptographic hash value is evaluated. Then using coefficients and the positions of the pixels, the watermark is extracted to obtain the face template and the original unwatermarked fingerprint image is retrieved by applying IDWT on the image.

Detailed analysis

Features: (a) Made use of potential benefits of DWT and LSB. (b) Separate algorithms as well as multimodal algorithm [26, 27,28] have been used for evaluation.

Advantages: (a) Protection against frequency and geometric attacks

Performance evaluation: Experimented with 750 fingerprint and face templates subjected to various frequency attacks and geometric attacks and performance evaluation conducted based on verification algorithms [26, 27,28].

Challenges: (a) Only the frequency and geometric attacks have been considered. The resiliency towards other template attacks were not evaluated. (b) Detailed investigation is required to guarantee the effectiveness of the verification algorithms [26, 27, 28] used.

Watermarking Based on Blockwise Multiresolution Clustering

Scheme of Implementation

Rabil et al [22] in their paper, presented a Blockwise Multi-Resolution Clustering (BMRC) framework for an intelligent watermarking technique maintaining quality, robustness, cost effectiveness, computational efficiency and adaptability.

Underlying principle

In the training process ,the method stored multi –objective optimization values for a group of high resolution training face images in an associative Block Cluster Memory (BCM).Then the optimal embedding band is obtained and the face images divided into blocks of 8x8 pixels are texture clustered. The number of clusters formed is shown by the resolution parameter of clustering. BMRC[22] adopted a continuous learning process during training so that the MRCs and the corresponding embedding parameters are recalculated each time.

In generalization process, the face images are subjected to texture feature extraction. The fitness of the watermark has been calculated to rank the solutions.

From many solutions available in the BCM, final decision making is withheld till watermarking ended.

Detailed analysis
Features: (a) Optimal watermark embedding values are obtained from a series of images in the training set. (b) Based on Associative memory recalls

Advantages: (a) Less complex and efficient computations compared to evolutionary techniques (b) Quality, adaptability and robustness maintained (c) Expensive re-optimizations are not required

Performance evaluation: (a) 93.5 % Complexity Reduction in evaluating the watermark fitness (b) Useful when search space is large and the solutions hide in smaller sub problems [29]

Challenges: Finding the relevant features of smaller problems in the candidate set which determines the overall optimization is a challenge.

B. Template Transformation Techniques

Scheme of Implementation
The feature template of the biometric image can be transformed in order to secure it. According to [30], the transformations can be invertible or non-invertible. When invertible (salting) transformation function based on a secret key is applied, the template can be withdrawn if it is tampered but it offers security only until the key is secret. For non-invertible transformation function, the template can be withdrawn and it is secure due to its non invertible nature. In a review of biometric template transformations [31], based on template representation, two transformation categories have been identified: vector based transformation and interest point based transformation. The paper also conducted a security analysis of biohashing and cancellable fingerprint schemes [31].

Application Specific Template Transformation

Underlying principle
Braithwaite et al [6] described application-specific techniques for protecting the biometric templates by introducing predetermined transformations on biometric data before or after the feature extraction. It prevents tracking attacks which traces the individual across multiple applications. The leaked templates can be revoked and new ones are reissued with the already available enrolled sample.

Detailed analysis
Features: Different transformations can be combined together and good availability of unique transformations provided sufficient template security against attacks. During matching process the template could remain in transformed state itself but in some cases the transformation is reversed and the exposed template can become a crucial vulnerability.

Advantages: (a) As the number of transformations increases, the level of security also increases. (b) Revocability is ensured (c) Templates can be reused and shared (d) No need of inverting the transformation for verification (e) Original templates undergo minimum exposure

Biometric Template Protection Using Chaotic Functions

Scheme of Implementation
The method uses a session key constructed from chaotic functions to encrypt and decrypt the biometric template to be protected [36].A permutation based transformation function is applied to the key and a resultant permuted session key is obtained. It is then hashed with biometric template. Further transformation on the hashed template and permuted session key yields a multi-encrypted biometric template.

Underlying principle
Chaotic function depends on initial values and its random yet deterministic nature makes it suitable for encryption of the session key.

Detailed analysis
Advantages: a) Session keys are not duplicated b) Attackers cannot retrieve the keys easily Challenges: a) Since it is an invertible transformation technique, knowledge of transformation procedure may pose threats

Ratha et al.[5] suggested the concept of cancelable biometrics in which the biometric template or image is subjected to non-invertible transformation function before it is stored. Here the input biometric image is modified either before or after the feature extraction process. When it is known that a template in the data store is tampered, then the present transformation function as well as the template are discarded or cancelled to adopt a new function to generate a new template from the existing biometric information. This method helps in preventing database cross-matching attack and user tracking by changing the function as specific to the application. The problem is that the pattern matching process is not well defined.

C. Cryptographic techniques

1. Visual Cryptographic technique

A few visual cryptography based biometric template protection schemes [32..35] with two shares and multiple shares provided a simple technique to secure different biometric templates like iris and fingerprint.

Scheme of Implementation
User enrollment and authentication phases complete the implementation for two share scheme[32]. In enrollment phase, the iris image is processed to extract a feature template which along with a binary image is fused as input to the visual cryptography module; the output being two cryptographic shares stored in different locations , one

being an ID card. In authentication phase, the two shares from different sources are again brought together to generate the original template. This is matched with the template of the newly acquired iris test image to make the authentication decision. An enhanced variation, threshold visual cryptography scheme[35] applied for fingerprint images ensure that n number of shares are generated and a threshold , say t number of shares are required for proper reconstruction of the template.

Underlying principle
According to Naor and Shamir's[33], visual cryptography scheme, two shares each with black and white subpixels are generated from a pixel in a binary image such that the shares do not reveal any information about the pixel. Then the shares are combined together and the combined pixel contrast can identify whether the pixel color is white or black. Pixel expansion and contrast are the issues which affect the performance of the scheme.

Detailed Analysis
Features:(a)Scheme is applied on iris and fingerprint database.(b) The threshold is kept as a secret.

Advantages: (a) Security is enhanced as availability of all the shares is required for authentication (b) Relatively simple computation involved (c) Share in the ID card can be compressed.

Performance evaluation: (a) Speed of authentication to be optimized (b)Efficient FAR and FRR rates(below0.2%).

Challenges: (a) generating meaningful shares (b) protecting the shares in the storage locations. The shares can be manipulated. To avoid that multiple servers can be identified(c) applying good quality visual cryptography schemes (d) Malpractices with the ID card could be critical in two share scheme.

Roja and Sawarkar [20] proposed the application of El Gamel encryption technique to protect biometric database. The method was experimented with binary, gray and colour facial images. The gray and colour images were encrypted in a single step where as the binary image encryption and decryption required two stages as El Gamel was followed by PN sequence. The approach derived a zero mean square error. But the scheme was directly applied on images and not on templates.

D. Hybrid Techniques

1. Invisible Watermarking and encryption technique

Scheme of Implementation
The biometric template is secured using watermarking followed by encryption technique[23].

Underlying principle
During watermarking, the personal information is taken as the watermark. The pixel positions to embed the watermark is pseudo randomly generated and using parity

checker, parity at the selected pixels are changed. The watermarked template is then encrypted and stored. The decryption and matching process is required for biometric authentication

Detailed analysis
Features: (a) Template watermarking with parity checking is further protected by encryption (b) Watermarking at four different places

Advantages: (a) Forged template could not identify the pixel positions where watermark is embedded (b) Decryption will not reveal original data (c) Scalable

Performance evaluation: Performance evaluation not yet done.

Challenges: (a) Security of the encryption algorithms used. (b) Personal data as watermark

Multimodal Technique

Rajibul et al [18] presented a biometric template protection scheme that generated a combined biometric template from two distinct biometric features like palmprint and fingerprint. This biometric identity is then protected with watermark embedding and hidden password encryption. The experimental analysis of the scheme revealed that several known attacks by impostors can be handled effectively without losing the privacy and security. But when both biometric features are compromised in any case, the authentication system will become vulnerable to attacks.

Malhotra and Verma [21] introduced a multimodal approach in which they combined a physiological trait such as fingerprint and behavioral characteristic like online signature to form a single biometric ID. Each trait is separately feature extracted, stored and matched and the multimodal merging takes place at the decision making level. The template security is ensured by the cryptographic fusion of a random secret key and the stored biometric template to obtain helper data. During authentication, the key retrieval algorithm extracts the key and then matching is done. The optimal level of fusion for a hybrid approach still remains as an issue.

Menariya and Ojha [19] presented an extension of fuzzy commitment scheme [13] with ECC for error correction and braid group for template security. Public and private cryptographic keys were generated and the data was encrypted with random braid and an invertible function. In the end fuzzy based ECC corrected any errors introduced in the biometric data transmitted across a communication channel. No experimentation with real biometric data has been reported in the paper.

Soutar [7] has recommended the use of quantized match scores to tackle the notorious hill-climbing attack since it applied technique that demanded numerous iterations of high time complexity in order to make a pattern matching decision. But Adler [8] demonstrated that the hill-climbing algorithm can be slightly altered to adjust the input to each iteration such that the quantized match score for the template gives interesting and potential information which a determined hacker can use wisely to reconstruct biometric images from the compromised templates.

Tuyls et al [10] suggested a Reliable Components Scheme for fingerprints, based on the concept of helper data which is divided into two sections. The first part is for

determining the reliable components with high SNR value from Gabor filtered biometric data of the fingerprint and the second part is for noise correction. During the enrollment phase, quantization is applied to obtain a binary configuration for the fingerprint image. The noise left out in quantization is corrected by mapping binary data to an ECC. This scheme recorded a good performance of EER 4.2% and secret size ≈ 40 bits on fingerprints, but the classification performance is poor.

Using fingerprint minutiae data, Uludag et al [11] worked on the actual implementation of fuzzy vault scheme[12] which is an enhancement of fuzzy commitment scheme[13]. The vault along with CRC code can protect any secret data (for eg: encryption keys like 128-bit AES keys) with fingerprint minutiae data. The minutiae is aligned as two sets of scrambled point lists in 2D space. One set is for the template called as genuine sets constructed with 16 bit polynomial and second one is chauff sets for the security. The authorized users can open the vault easily by giving valid fingerprint where as the attackers need complex computational efforts to do the same. The high time complexity calculations for the point combinations are a limitation during decoding.

Sutcu , Li and Memon [14] suggested an application of their secure sketch scheme [15] on face biometric templates to derive reliable keys. For each biometric sample of face image, the feature vector of a definite size is extracted. Then the feature vector components are quantized and then a sketch scheme is applied to generate a sketch from the vector. Later the quantized feature vector is reconstructed. In experimental analysis, they noted that the lone consideration of entropy is not adequate to determine the security strength as FRR and FAR are also significant.

Freire [16] proposed a biometric template security scheme for dynamic signature verification. It generated protected templates by using helper data system which contained supportive data to perform a pattern matching without exposing critical information to the impostor. Later binarized feature vector is generated and cryptographic transformation is applied. In order to practically implement biometric hashing, the feature subset is selected using genetic algorithm. The scheme could resist template database attacks. Usually redundant information is provided in lengthy hashes without any added security.

Sutcu et al [17] demonstrated the transformation of original fingerprint data into binary feature vectors, compatible with ECC codes designed for standard communication channels. The robust feature vectors represented the minutiae point positions and orientations and served as the template, resisting the biometric measurement noises. The syndromes or parity symbols derived from Low-Density Parity Check (LDPC) coding of the feature vectors improved the biometric system security. An important issue not handled by the authors is regarding user specific question correlations in the transformation process.

Table I shows a summary of significant biometric security schemes so far experimented.

Table 1: Summary of Significant Biometric Security Schemes

TECHNIQUE	FEATURES	MERITS	LIMITATIONS
Verification Watermarks on Fingerprint Recognition and Retrieval	Fragile invisible watermarking	No change in recognition accuracy. Scalable and consistent performance.	Scheme not checked for utility purpose
Cancelable Biometrics	Different transformations for each instance of enrollment	Cross matching and recovery impossible. Enhanced privacy	Liveness detection to be added
A Fuzzy Vault Scheme for fingerprint	128-bit AES keys can be secured with fingerprint minutiae data	FAR is 0% Corrects errors by polynomial interpolation	High time complexity for decoding. Inability to generate multiple nonlinkable templates from the same biometric data
Reliable Components Scheme	Splitting the helper-data into two- one part determines the reliable components and for noise correction	A performance of EER ≈ 4.2% and secret size ≈ 40 bits on fingerprints	Degrades the classification performance. Enrolled image quality dependent
Secure sketch for face templates	Quantization based sketch scheme with focus on entropy	Security measure in terms of entropy and sketch bit size for face templates	Computation of min-entropy and considering FAR and FRR.
Watermarking with Hidden Password Encryption	Combines watermarking with password scheme.	Stolen biometric information is not reusable. Protection against attacks and eavesdropping	Attack will be established when the biometric is compromised
El Gamel Encryption	Combination of El Gamel and PN Sequence Scheme	Mean square error zero for binary, gray and colour images	More encryption time for colour and binary image

Feature Transformation based on Error Correcting Codes	Feature transformation combined with Low-Density Parity Check (LDPC) codes	Implemented fingerprint based access control without storing original fingerprint template	Elimination of correlated question pairs and incorporation of other modalities required
Security framework for biometric templates	Braid group based cryptosystem with fuzzy commitment scheme	Accuracy comparable to K-NN classification	Experiments on real biometric data not done
Hybrid Approach for securing biometric template	Multimodal Approach with Keybinding Cryptosystem	Diverse, Revocable, Secure and Simple	choice of optimal fusion level and extracted features redundancy

Biometric template security in cloud environment

The cloud computing provides an immensely potential environment to handle big data with enough scalability and cost effectiveness. Many active research is going on in this domain to mitigate the security concerns and make cloud computing a vibrant platform for storage, processing and application development. As the amount of privacy sensitive biometric data enrolled or verified by biometric authentication systems increase day by day, the biometric security experts and cloud practitioners look upon cloud based biometric system as a viable solution for the future.

Cloud computing security based on private face recognition is mentioned in [40]. The encrypted input face image is sent to cloud and verification and decision ia also done in encrypted form resulting in a secure recognition. Even though it is credible, the authors suggest a more efficient algorithm to improve recognition performance.

According to [41], with data explosion, the design considerations for future biometric systems must be updated to handle voluminous data:

A. Interoperability with Different standards
B. Scalability and Flexibility
C. Availability and sharability
D. Fault tolerance and failure recovery
E. Performance improvement

The paper [39] suggests a cloud based template protection approach for voiceprint. The various steps in biometric recognition works on different cloud servers.The approach makes use of the benefits of RSA and homomorphic encryption [9] to create non-invertible cancelable templates with desirable performance levels.

Multi finger security model [37] works as follows: The user chooses three fingers and allot a digit with each and these three fingerprint images along with their digits are enrolled. The ECC algorithm encrypts the fingerprint data and the numbers and their associations are encrypted by RSA.

A combined method [38] is proposed with cancelable biometrics and forward error correction to protect the template from spoofing attacks and also provides error detection and correction.

Conclusion

The study encompassed the major security techniques applied in biometric authentication systems and it revealed that a concrete solution satisfying the security requirements has not yet realized. The future can expect more and more severe threats and adversary attacks on biometric systems and to guard the credibility of the biometric authentication and privacy of the individual we need to focus on a stronger solution. Our current research in this regard makes use of the potential of biometric template storage in cloud environment with a suitable security scheme.

References

[1] U. Korte, R. Plaga, "Cryptographic Protection of Biometric Templates: Chance, Challenges and Applications", Proceedings of the Special Interest Group on Biometrics and Electronic Signatures, July 2007, 12-13.

[2] Anil K. Jain , Karthik Nanda kumar "Biometric Authentication: System Security and User Privacy" IEEE Computer Society,2012, Vol. 45, no.11, p. 87-92.

[3] Ambalakat, P."Security of Biometric Authentication Systems", In: 21st Computer Science Seminar, SA1-T1, 2005, p 1-7

[4] Minerva M. Yeung ,Sharath Pankanti, "Verification Watermarks on Fingerprint Recognition and Retrieval" in Proceedings of SPIE Conference on Security and Watermarking of Multimedia Contents, January 1999, Vol. 3657 , USA, p. 66-78.

[5] N.K Ratha, J.H Connell, and R.M Bolle, "Enhancing security and privacy in biometrics-based authentication systems", IBM Systems Journal, 2001, Vol. 40, no. 3, p. 614–634.

[6] Michael Braithwaite, Ulf Cahn von Seelen, James Cambier, John Daugman, Randy Glass, Russ Moore, Ian Scott, "Application-Specific Biometric Templates", IEEE Workshop on Automatic Identification Advanced Technologies, NewYork, March 14-15, 2002, p.167-171

[7] C. Soutar, "Biometric system security," Available at:

[8] http://www.comp.hkbu.edu.hk/~ycfeng/project/Biometric%20System%20Security.pdf

[9] Andy Adler, "Reconstruction of source images from quantized biometric match score data" in Proceedings of Canadian Conference on Electrical and Computer Engineering, Canada, May 2004, p. 469–472

[10] X.G.Li, X.M. Chen, P. Zhu. "A method of homomorphic encryption". Wuhan University Journal of Natural Sciences, 2006,Vol. 11,p181-184.

[11] Pim Tuyls, Anton H.M. Akkermans, Tom A.M. Kevenaar, Geert-Jan Schrijen, Asker M. Bazen, and Raymond N.J. Veldhuis, "Practical Biometric Authentication with Template Protection" , Springer-Verlag Berlin Heidelberg, 2005, p.436-446

[12] U. Uludag, S. Pankanti, and A. K. Jain, "Fuzzy vault for fingerprints," Proceedings of Audio and Video based Biometric Person Authentication , New York, July 2005.

[13] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", Proceedings of IEEE International Symposium on Information Theory, 2002, p.408

[14] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme", Sixth ACM Conference on Computer and Communication Security,1999, p. 28-36.

[15] Yagiz Sutcu, Qiming Li and Nasir Memon "How to Protect Biometric Templates" Proceedings of SPIE, Vol. 6505, Security, Steganography, and Watermarking of Multimedia Contents IX, 650514 ,February 27, 2007

[16] Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates," in Asia crypt, Shanghai, December 2006.

[17] Manuel R. Freire "Biometric Template Protection in Dynamic Signature Verification" Procedings of IEEE International Conference on Acoustics, Speech and Signal Processing, March 2008

[18] Yagiz Sutcu, Shantanu Rane, Jonathan S. Yedidia, Stark C. Draper and Anthony Vetro,"Feature Transformation of Biometric Templates for Secure Biometric Systems based on Error Correcting Codes", Mitsubishi Electric Research Laboratories, Inc., TR2008-029, July 2008

[19] Md. Rajibul Islam,Md. Shohel Sayeed and Andrews Samraj, "Biometric Template Protection Using Watermarking with Hidden Password Encryption" IEEE Proceedings of the International Symposium on Information Technology, Malaysia, 26-29 August 2008, pp. 296-303

[20] Dilip Menariya and D. B. Ojha "A vital application of security with biometric templates", International Journal of Engineering Research and Applications, Vol. 2, Issue 5, September- October 2012, p.328-332

[21] M. Mani Roja and Sudhir Sawarkar, "El Gamel Encryption for Biometric Database Protection", International Journal of Computer Applications, Volume 68– No.6, April 2013

[22] Shweta Malhotra, Chander Kant Verma "A Hybrid Approach for Securing Biometric Template" International Journal of Engineering and Advanced Technology, Volume-2, Issue-5, June 2013

[23] Bassem S. Rabil, Robert Sabourin, and Eric Granger,"Securing Mass Biometric Templates Using Blockwise Multi-Resolution Clustering Watermarking" International Conference on Machine Learning and Data Mining,2013

[24] Shweta Malhotra, Chander Kant Verma, "A Novel Approach for Securing Biometric Template", International Journal of Advanced Research in Computer Science and Software Engineering,Vol.3,Issue 5 , May 2013

[25] Vatsa , Singh, Noore etal.,"Robust biometric image watermarking for fingerprint and face template protection", IEICE Electronics Express 2006, Vol.3, Issue 2, p. 23-28.
[26] M.M. Yeung, F.C. Mintzer, "An Invisible Watermarking Technique for Image Verification", Proceedings of International Conference on Image Processing 1997,p. 680-683.
[27] A.K.Jain, L.Hong, R.Bolle, "On-line fingerprint verification," IEEE Transaction on Pattern Analysis and Machine Intelligence, April 1997, Vol.19,no.4,p.302-314.
[28] R.Singh, M.Vatsa, A.Noore, "Textural feature based face recognition for single training images", IET Electronics Letters , Vol.41, Issue 11, May 2005, p. 640 – 641
[29] A.Ross and A.K.Jain, "Information fusion in biometrics":Pattern Recognitio Lett.,2003,Vol.24,no.13,p. 2115-2125.
[30] Rabil, B.S., Sabourin, R., Granger, E.,"Rapid blockwise multi-resolution clustering of facial images for intelligent watermarking", Springer, Machine Vision and Applications 2014, p. 277-300
[31] M. Grassi, M. Faundez-Zanuy, "A protection scheme for enhancing biometric template security and discriminability", In Proceedings of JRBP September 2010 , Spain.
[32] Abhishek Nagar, Karthik Nandakumar and Anil K. Jain, "Biometric Template Transformation: A Security Analysis" Proceedings of SPIE, Vol. 7541, Media Forensics and Security II, 75410O , January 27, 2010.
[33] Revenkar,Anjum,Gandhare,"Secure Iris Authentication Using Visual Cryptography", International Journal of Computer Science and Information Security,Vol. 7, No.3, 2010
[34] Moni Naor and Adi Shamir, "Visual cryptography" ,In Proceedings of the Advances in Cryptology– Eurocrypt, 1995,p. 1-12.
[35] Y.V. Subba Rao, Yulia Sukonkina, Chakravarthy Bhagwati, Umesh Kumar Singh , "Fingerprint based authentication application using visual cryptography methods (Improved ID card)", IEEE Region10 conference, Tencon 2008.
[36] Rajeswari Mukesh, V.J.Subashini,"Fingerprint Based Authentication System using Threshold Visual Cryptographic Technique", IEEE-International Conference on Advances in Engineering, Science and Management March 2012
[37] Maithili Arjunwadkar, R. V. Kulkarni,"Robust Security Model for Biometric Template Protection using Chaos Phenomenon" International Journal of Computer Applications (0975 – 8887) Vol. 3 – No.6, June 2010
[38] D.Pugazhenthi, B.Sree Vidya, "Multiple Biometric Security in Cloud Computing", International Journal of Advanced Research in Computer Science and Software Engineering , Vol. 3, Issue 4, April 2013
[39] S.Viswanadha Raju, P.Vidyasree, G.Madhavi,"Enhancing Security of Stored Biometric Template in Cloud Computing using FEC", International

Journal of Advanced Computational Engineering and Networking, Vol.-2, Issue-2, Feb.-2014

[40] Hua-Hong Zhu etal."Voiceprint-Biometric template design and authentication based on cloud computing security", IEEE International Conference on Cloud and Service Computing 2011

[41] Chenguang Wang, Huaizhi Yan, "Study of Cloud Computing Security Based on Private Face Recognition", IEEE International Conference on Computational Intelligence and Software Engineering, 2010.

[42] Edmund Kohlwey, Abel Sussman, Jason Trost, Amber Maurer, "Leveraging the Cloud for Big Data Biometrics-Meeting the performance requirements of the Next Generation Biometric Systems", IEEE World Congress on Services, 2011