International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:268
Vol.2, No.6, June 2013 DOI:10.15693/ijaist/2013.v2i6.37-40

Biometric Privacy Using Non Expansible Visual Cryptography Scheme

Biruntha.S
PG student,
Department of Computer Science and Engineering,
SNS College of Technology
Coimbatore, Tamilnadu,

Dhanalakshmi.S
Associate Professor,
Department of Computer Science and Engineering,
SNS College of Technology
Coimbatore, Tamilnadu,

Abstract

Biometric system is more security and convenient than password authentication system. A biometric system operates by acquiring raw biometric data from a subject, extracting a feature set from the data and comparing the feature set against the template stored in a database in order to identify person. At the same time there is a possible to intruder can access the database which stored the biometric data. So the security and privacy of biometric system is a major concern due to their issues like fake biometric, override matcher and etc. In this paper the visual cryptography scheme is used for biometric data security.The original biometric data image converted into two shares ,and second share rotated into 180°.So we store the shares in the database instead of the original image.These shares are overlapped, and matched whenever user entering, and matching with the biometric data generated by the system.

Keywords_Biometrics,watermarking,steganography, cryptography , Visual cryptography,Pixelexpansion.

I.INTRODUCTION

Biometric is one of the authentication system it comes from the greek words 'bios and metricos' which means 'life measure'.It is the science of establishing the identity of on individual based on physical or behavioral traits such as face, fingerprint, Iris.It is more reliable,consistent and also user friendly.So it is used for many application such as computer login control, passport control,border crossing,secure e-banking,ATM, credit cards,airport ,etc.The biometric data classified as physiological or behavioral. Physiological biometrics based on the physical part of the body such as fingerprint,iris,eye retina,face,palm,hand. Behavioral type is based the behavior of human such as voice,signature and keystroke.

A.*The Properties of Biometric Template*

a**.** Security**:** This property prevents the biometric template from stolen template

b. Diversity: The secure template must not allow cross matching across databases.

c. Revocability: It should be straightforward to revoke a compromised

d. Performance: The recognition performance of the biometric system should not reduced by biometric template protection scheme.

B.*Modules in Biometric System*

There are basically two phases in biometric system.There are enrollment phase and authentication phase.In this two phases there are four modules.The **sensor module** is used in extracting the biometric data which may be image, audio or video. The **feature extraction module** is used in obtaining the template that is generated from the features of the biometric data. Each feature is labeled with a user's identity. The **Matching module** is used in authentication phase, where the template data is compared with data which is obtained from user and that it estimates the similarity between these data. These similar elements are processed in **Decision making module** which is used to identify the individual.

C.*Vulnerabilities in Biometric system*

The biometric system failures are classified into two types, intrinsic system and adversary attack. Intrinsic attack is due to the incorrectness in the decision making of biometric system which may lead to false accept and false reject. In adversary attack the hacker will try to circumvent the biometric system for personal gains. These are classified into three types administrator attack, Non-secure Infrastructure and Biometric Overtness [1].

II.RELATED WORKS

Neha Agrawal and Marios Savvides Carnegie Mellon University Pittsburgh,they presented the steganography technique for biometric template security. The main objective of steganography is to securely communicate in a way that is not detectable by intruder. The covers used in steganography method is digital images, audio, video and other computer files that contain perceptually redundant or irrelevant information. After the embedding of secret image into cover image we have obtained a image called stego.

Here the original image is embed in digital image using a key which is done by stegno encoder system. The stego or covered image is than transmitted over a channel to the destination where the same key is employed to decode this stegno image by stegno decoder system. By this the biometric template is preserved. But this steganography is used highly during the transmission of biometric data.

Rajkumar Yadav,Rohtak, Kamaldeep and Ravi Saini presented the technique of water marking for biometric Template protection. Water marking is one of the security technique which is defined as embedding information (watermark) in the host signal.

Pravin M.Sonsare and Shubhangi Sapkal suggest the another technique to secure the biometric template using stegno-cryptosystem with RSA.

III.EXISTING SYSTEM

In the existing system, the use of visual cryptography is explored to preserve the privacy of biometric data by decomposing the original image into two images in such a way that the original image can be revealed only when both images are simultaneously available; further, the individual component images do not reveal any information about the original image.

However the fingerprint image is divided into two shares which means each pixel is divided into two sub pixels using visual cryptography.Each share stored in two different databases which is done in Enrollment phase.In authentication phase,each share requested from that corresponding database,then two shares are overlaid. Using XOR operation we get target image which will be compared with original image get from the user whenever entering.

When two shares are overlaid the original pixel value can be determined.If the pixel is black,then we will get two black pixels.If it is white pixel then we will get one black and one white subpixel.so the reconstructed image 50% loss in contrast.

This technique is also used for iris codes.So the visual cryptography scheme is more secure for biometric template security.But it requires more space for storing sheets due because of pixel expansion.

IV.PROBLEM STATEMENT

The results demonstrate the difficulty of exposing the identity of the secret image by using only one of the sheets; further individual sheets cannot be used to perform cross-matching between different applications. Increasing the pixel expansion factor can lead to an increase in the storage requirements for the sheets. In the recent literature there have been some efforts to develop a VCS without pixel expansion . But no such scheme currently exists for generating sheets that are not random noisy images. Thus, more work is necessary to handle this problem.

V.PROPOSED SYSTEM

In the proposed system the modules are,

- Biometric data input
- Converting into two shares
- Rotating the 2nd share into 180 degree
- Overlapping the two shares
- Decrypting the Original Image
- Comparing the biometrical data

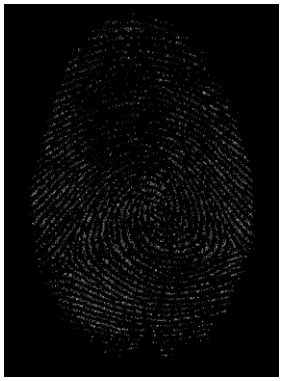
A.Biometric Inputs

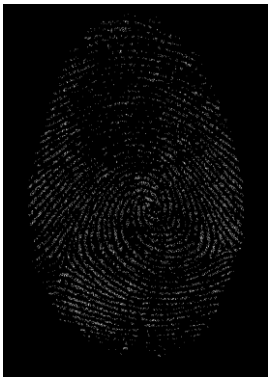
For irides and fingerprints, the biometric image is decomposed by the visual cryptography scheme and two noise-like images known as sheets are produced. In the case of securing an iris template, the iris code is encrypted instead of the iris image.Here the finger print image is used.

B.Converting into two shares

Black and white image: each pixel divided in 2 sub-pixels. Randomly choose between black and white. If white, then randomly choose one of the two rows for white. If black, then randomly choose between one of the two rows for black. The two subpixels per pixel variant can distort the aspect ratio of the original image.

Original Image

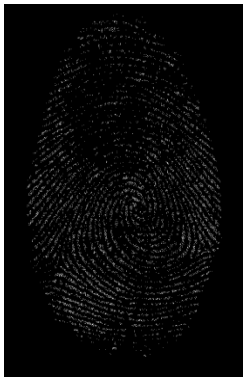


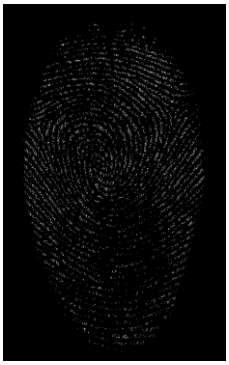


Share1 Share2

C.Rotating the 2nd share into 180 degree:

In this, the function was to stick the subsets obtained by DSP to generate the share images, and two subsets of secret image S1 were stuck to share images Share1 and





Share 2 **After Rotation**

Share2, respectively. The first subset of SE2 was directly stuck on the corresponding position of S1 while, the second subset of Share2 was rotated with 180 degree and stuck to the corresponding position of Share2.

D.Overlapping the two shares:

The sticking operation executes logic ‘‘OR” operation between the separated subset and the share images during the sticking process depicted. The goal is to build the patterns of two blocks for share images S1 and S2. The sticking results are generated according to the decrypting function. By the defined decrypting process in our proposed scheme, secret image SE1 is revealed by directly stacking share images S1 and S2. But, it needs to rotate the share image S2 with 180_ angle and stack with S1.

Overlapping share1& Rotated Share2

E.Decrypting the Original Image:

According to the rule of the decrypting process, the two subsets, C1 and C3, separated from DSP for secret images SE1 and SE2, respectively, can be stuck together to build one corresponding block for share image S1. In order to build the corresponding block of share image S2, the whole matrix, with C4 separated from share image S2 by DSP, must be rotated 180 degree and stuck with the corresponding block of C2, which is another separated subset of S1, to generate share image S2. It was obvious that every pixel was moved from one position to another related position by the 180 degree rotation angle. For example, the pixel on the right-bottom position was moved to the left-top position, and vice versa

F.Comparing the biometrical data:

The Biometric data which is saved before was secured with the above visual cryptography scheme. To compare the another biometric data with the saved biometric data a separate module is generated in that we can compare the biometric data. When the new biometric data is given as the input the module searches for the matching biometric data and displays the result as to which biometric data is matched with the input biometric data.

VI.CONCLUSION

Various types of approaches developed by researches to secure the biometric data and template in database. In this paper, three new security related performance criteria which are to be satisfied by non expansible visual cryptography scheme. In addition, a modified VC technique called Pair-Wise Visual Cryptography (PWVC) technique is applied in order to have no pixel expansion while creating the shares.

The simulation done by using MATLAB, in the result,the proposed scheme has good robustness to a range of image processing attacks. When compared with the popular DWT and VC-based copyright protection schemes in the literature, the advantages of the proposed scheme are as follows: First, the proposed scheme meets all the security requirements of VC and hence offers better security; second, the scheme requires less memory space to store private shares, thereby reducing the overhead on CA.

ACKNOWLEDGMENTS

The authors are grateful to Dr.S.Karthik**,** Professor & Dean**,** Prof.T.Kalaikumaran**,** HoD, Department of Computer Science and Engineering, for their valuable suggestion and guidance.

REFERENCES

[1] Agrawal .N and Savvides.M, “Biometric data hiding: A 3 factor authentication approach to verify identity with a single image using steganography, encryption and matching,” in Proc. Computer Vision and Pattern Recognition Workshop, 2009, vol. 0, pp. 85–92..

[2] Ateniese.G, Blundo.C, Santis.A, and Stinson.D, “Extended capabilities for visual cryptography,” Theor. Comput. Sci., vol. 250, no. 1–2, pp. 143–161, 2001.

[3] Bitouk.D, Kumar.N, Dhillon.S, Belhumeur.B, and Nayar.S.K, “Face swapping: Automatically replacing faces in photographs,” ACMTrans. Graph., vol. 27, no. 3, pp. 1–8, 2008.

[4] Chen.Y, Chan.Y, Huang.C, Tsai.M, and Chu.Y, “A multiple-level visual secret-sharing scheme without image

size expansion," Inf. Sci.,vol. 177, no. 21, pp. 4696–4710, 2007.

[5] Cootes.T et al., "Active appearance models," IEEE Trans. Pattern Anal. Mach. Intell., vol. 23, no. 6, pp. 681–685, Jun. 2001.

[6] Davida G.I, Frankel.Y, and Matt.B.J, "On enabling secure applications through off-line biometric identification," in Proc. IEEE Symp. Security and Privacy, 1998, pp. 148–157.

[7] Dong.J and Tan.T, "Effects of watermarking on iris recognition performance," in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision, 2008 (ICARCV 2008), 2008, pp. 1156–1161.

[8] Feng.Y, Yuen.P, and Jain.A, "A hybrid approach for face template protection," in Proc. SPIE Conf. Biometric Technology for Human Identification, Orlando, FL, 2008, vol. 6944.

[9] Gross.R, Sweeney.L, De la Torre.F, and Baker.S, "Model-based face de-identification," in IEEE Workshop on Privacy Research in Vision, Los Alamitos, CA, 2006.

[10] Jain.A and Uludag.U, "Hiding biometric data," IEEE Trans. Pattern Anal. Mach. Intell., vol. 25, no. 11, pp. 1494–1498, Nov. 2003.

[11] Jain.A, Nandakumar.K, and Nagar.A, "Biometric template security," EURASIP J. Advances Signal Process., pp. 1–17, 2008.

[12] Maltoni.D, Maio.D, Jain .A, and Prabhakar .S, Handbook of Fingerprint Recognition. Secaucus, NJ: Springer-Verlag New York, Inc., 2003.

[13] Moskovich.B and Osadchy.M, "Illumination invariant representation for privacy preserving face identification," in Proc. IEEE Computer Society and IEEE Biometrics Council Workshop on Biometrics, San Francisco, CA, Jun. 2010, pp. 154–161.

[14] Naor .M and Shamir .A, "Visual cryptography," in Proc. EUROCRYPT, 1994, pp. 1–12.

[15] Nakajima. M and Yamaguchi.Y, "Extended visual cryptography fornatural images," J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.

[16] Prabhakar.S, Pankanti.S, and Jain.A, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42,Mar./Apr. 2003.

[17] Pravin M Sonare,Shubhangi Sapkal, "Stegano-CryptoSystem for Enhancing Biometric-feature security with RSA", Int. Conf.Information and Network Technology IPCSIT Vol.4 2011.

[18] Revenkar.P, Anjum.A, and Gandhare.W, "Secure iris authentication using visual cryptography," Int. J. Comput. Sci. (IJCSIS), vol. 7, no. 3, pp. 217–221, Mar. 2010.

[19] Soutar.C, Roberge.D, Stoianov.A, Gilroy.R, and Kumar .B, "Biometric encryption," in ICSA Guide to Cryptography. New York: Mc-Graw-Hill, 1999.

[20] Thuraisingham.B and Ford.W, "Security constraint processing in a multilevel secure distributed database management system," IEEE Trans. Knowl. Data Eng., vol. 7, no. 2, pp. 274–293, Apr. 1995.

[21] A. Ross and A. A. Othman, "Visual cryptography for Biometric privacy,"in IEEE transaction on information Forensics and security,vol.6,No.1,March 2011.