International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-3, March 2015

Visual Cryptography for Image Privacy

Shubhangi Kahulkar, Samiksha Patil, Prajkta Bhoir, Jayesh Kulkarni, Prof. Gayatri Naik

***Abstract*— Preserving the privacy of digital biometric data (e.g., face images) stored in a central database has become of paramount importance. This work explores the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images. In the case of faces, a privateimage is dithered into two host face images (known as sheets) that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image. A series of experiments on the confirm the following: 1) the possibility of hiding a private face image in two host face images; 2) the successful matching of face images reconstructed from the sheets; 3) the inability of sheets to reveal the identity of the private face image; 4) using different pairs of host images to encrypt different samples of the same private face; and 5) the difficulty of cross-database matching for determining identities. A similar process is used to de-identify fingerprint images and iris codes prior to storing them in a central database.**

***Index Terms*—De-identification, face, fingerprint, IrisCodes, privacy, visual cryptography.**

I. INTRODUCTION

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioural traits such as face, fingerprints, iris, etc. The working of biometric authentication system acquires raw biometric data from a subject, extracting a feature set from the data, and comparing the feature set against the templates stored in a database in order to identify the subject or to verify a claimed identity.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. The biometric data classified as physiological or behavioural. Physiological biometrics based on the physical part of the body such as fingerprint, iris, eye retina, face, palm, hand. Behavioural type is based the behaviour of human such as voice, signature and keystroke.

Cryptography is the art of sending and receiving encrypted messages that can be decrypted only by the sender or the receiver. Encryption and decryption are accomplished by using mathematical algorithms in such a way that no one but the intended recipient can decrypt and read the message.
Visual cryptography is introduced by Noar and Shamir. It is another form of cryptography in which secret communication is done in the form of images. This can be used to protect the biometric templates in which the decryption doesn't require any complex computations, it is done by human visual system. Using this visual cryptography the biometric data capture from the authorized user. These original image is divided into two shares .Each share stored in two different databases. When both images are simultaneously available then only we can get the original image. The individual share do not reveal any information about the original image.

Manuscript received March 22, 2015.

A. *Encryption*

Encryption is a mechanism that protects your valuable information, such as your documents, pictures, or online transactions, from unwanted people accessing or changing it. Encryption works by using a mathematical formula called a cipher and a key to convert readable data (plain text) into a form that others cannot understand (cipher text). The cipher is the general recipe for encryption, and your key makes your encrypted data unique. Only people with your unique key and the same cipher can unscramble it. Keys are usually a long sequence of numbers protected by common authentication mechanisms, such as passwords.

Information is also vulnerable when it's in transit. If the data is not encrypted, it can be monitored and captured online. This is why you want to ensure that any sensitive online communications, such as online banking, sending e-mails, or perhaps even accessing your Face book account, are encrypted. The most common type of online encryption is HTTPS, or connecting to secured websites. This means the traffic between your browser and the website is encrypted.
Look for **https://** in the URL or the lock icon in your browser. Many sites support this by default (such as Google Apps), and websites like Face book and Twitter give you the option in your account HTTPS.

Encryption is an important tool for protecting data, but is only effective if you have strong passwords and maintain the overall security of your computer. Your encryption is only as strong as your keys. If your key is compromised, so is your data. If you are using passwords to protect your keys, make sure you use strong passwords and protect them well. Don't lose or lose access to your keys. If you lose your encryption keys or can't access them because you've forgotten the password that protects them, you most likely cannot recover your data.

B. *Decryption*

Decryption is the process of transforming data that has been rendered unreadable through encryption back to its unencrypted form. In decryption, the system extracts and converts the garbled data and transforms it to texts and images that are easily understandable not only by the reader but also by the system. Decryption may be accomplished manually or automatically. It may also be performed with a set of keys or passwords. Break an encryption cryptanalyst can do any or all of three different things:

1 .Attempt to break a single message.

2. Attempt to recognize patterns in encrypted messages, in order to be able to break subsequent ones by applying a straightforward decryption algorithm.

3. Attempt to find general weakness in an encryption algorithm, without necessarily having intercepted any messages

C. *Problem Statements*

Explore the visual cryptography to preserve the privacy of Biometric data by decomposing original image into two images in such a way that the original image can be revealed only when both images are simultaneously available.

There are various types of attacks on Biometric Systems as follows :

a) Fake Biometric

Attack on the sensor. Sensor can be overridden by presenting fake . Like a fake finger, face mask or a copy of signature.

b) Replay Old Data

The Attack on the channel between the sensor and the feature extractor. Biometrics which was submitted can be resubmitted or replayed by bypassing the sensor. Like an old copy of fingerprint or face image.

c) Override Feature Extractor

Feature extractor can be override by attacking it and forcing it to produce feature values selected by the hacker.

d) Override Matcher

Attack on the matcher. Matcher can be overridden by attacking it and forcing it to produce high or low matching score irrespective of the input.

D. *solution*

Following approach can be used to obtain a solution for the above mentioned problem.

1) Steganography Techniques for Biometric Template Security.

2) Watermarking Techniques for Biometric Template Security.

Visual Cryptography Technique for Biometric Template Security

II. LITERATURE REVIEW

While developing our project, we have gone through lot of reviews and got various feedbacks from various ways. Some of these feedbacks and suggestions are as follows –

A. Design and develop the system for more than one user.

B. Provide an E-mail Facility to the user for handling more security consequences.

Visual cryptography Scheme

Cryptography is the art of encryption and decryption.These original images is divided into two shares.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. Short storage of secret image.

GEVCS

The extended version of visual cryptography is gray scale cryptography scheme(GEVCS) . Nakajima and Yamaguchi proposed a theoretical framework to apply extended visual cryptography on gray scale images .The gray scale cryptogaraphy is divide into 3 steps.

The first step is halftone image and partitioning the halftone image.

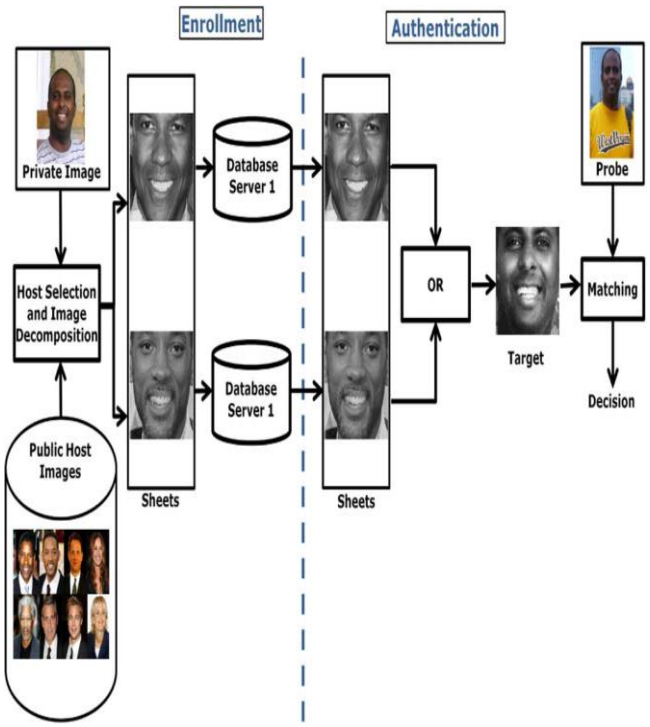
In the second step**,** the number of black pixels in each cluster from the halftone image are counted and saved in a template.

The third step starts from the first block in the top left .

The system is developed in NETBEANS and MYSQL 5.5 for use on Windows environment.

The server we used is APACHE TOMCAT for Designing and Coding and Reports. MYSQL 5.5 for Database

III. SYSTEM DESIGN



System architecture

Protecting template in the database securely is one of the challenges in any biometric system. Here visual cryptography is applied to biometric authentication system. In this system, there are two modules: Enrollment module and Authentication module.

A. *Enrollment module :*

During the enrollment process, administrator collects the template and performs image scrambling. Image scrambling is used to make images visually unrecognizable such that unauthorized users have difficulty decoding the scrambled image to access the original image. The original image can be

decomposed into blocks; each one containing a specific number of pixels. The scrambled image is then sent to a trusted party entity. Once the trusted entity receives it, the scrambled image is decomposed into two noisy images (i.e., sheets) and the original data is discarded. The decomposed components are then transmitted and stored in database servers such that the identity of the private image is not revealed.

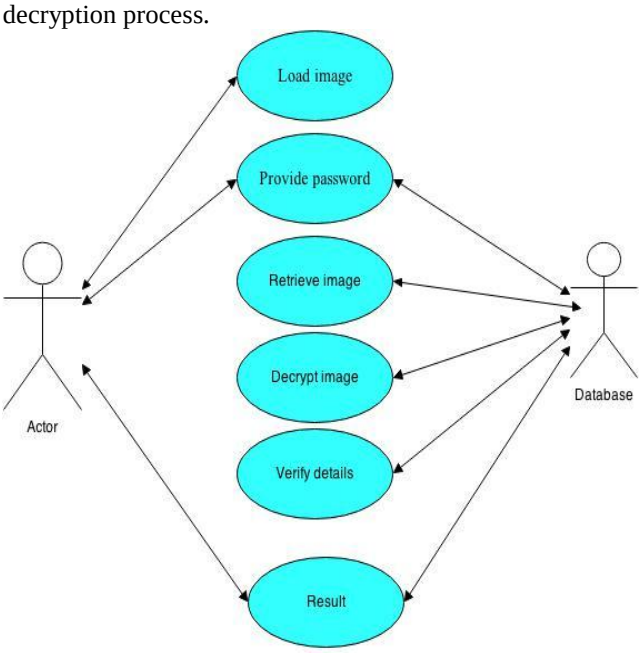
B. Authentication module :

During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the scrambled image.

IV. DESIGN

Use Case Diagram of Decryption

The use case Diagram shows all the functionalities of the decryption process.



Use Case Diagram for Decryption

V. CONCLUSION

Thus includes a methodology to protect the privacy of a face database by decomposing an input private face image into two independent sheet images such that the private face image can be reconstructed only when both sheets are simultaneously available. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance.

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.

VI. FUTURE SCOPE:

1. This project at start should aim at the security of the private face images.
2. Only qualified subset of shares can recover the secret image.
3. Any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.
4. All the shares are meaningful images.
5. The authentication must be valid for the face image registered before.
6. It can be used at all security related institutions like military, offices, confidential laboratories.

ACKNOWLEDGEMENT

We are immensely obliged to Prof. Gayatri Naik for his immense support for the project and for his guidance and supervision. It has indeed been a fulfilling experience for working out this project report. Lastly, we thank almighty & our parents, for their constant encouragement without which this project would not be possible.

.REFRENCE

[1] IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 1, MARCH 2011, Arun Ross, *Senior Member, IEEE*, and Asem Othman, *Student Member, IEEE.*

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

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

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

[5] B. Thuraisingham and W. Ford, "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.

[6] N. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3,pp. 614–634, 2001.

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

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

[9] Rahna. P. Muhammed M.Tech Student, Dept of CSE Viswajyothi College of Engineering and Technology Vazhakkulam, Muvattupuzha rahnap2000@gmail.com ACEEE Int. J. on Network Security , Vol. 02, No. 03, July 2011.

[10] C. A. Bouman: Digital Image Processing - January 13, 2014.

[11] Purdue University: Digital Image Processing Laboratories, May 11, 2011.

[12] Pratiksha P.Patil, Y.M. Patil *1(Department of Electronics, K.I.Ts College of Engineering, Kolhapur, India)(Department of Electronics, K.I.Ts College of Engineering, Kolhapur India*).

[13] Zhi Zhou, *Member, IEEE*, Gonzalo R. Arce, *Fellow, IEEE*, and Giovanni Di CrescenzoIEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006.

[14] International Journal of Computer Applications (0975 – 8887) Volume 60– No.1, December 2012.

[15] International Journal of Computer Trends and Technology- volume4Issue3- 2013.

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

[17] D. Jin, W.-Q. Yan, and M. S. Kankanhalli, "Progressive color visual cryptography," *J. Electron. Imag.* vol. 14, no. 3, p. 033019, 2005 [Online]. Available: http://link.aip.org/link/?JEI/14/033019/1 T. Cootes *et al.*, "Active appearance models," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 23, no. 6, pp. 681–685, Jun. 2001.

[18] M. B. Stegmann, "Active Appearance Models: Theory, Extensions and Cases," Master's thesis, Informatics and Mathematical Modelling, Technical University of Denmark, DTU, Kgs. Lyngby, Aug. 2, 2000 [Online]. Available: http://www.imm.dtu.dk/aam/main/

[19] F. Bookstein, "Principal warps: Thin-plate splines and the decomposition of deformations," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 11,no. 6, pp. 567–585, Jun. 1989.

[20] L. Masek and P. Kovesi, *Matlab Source Code for a Biometric Identification System Based on Iris Patterns*. Perth, Australia: Dept. of Computer Science and Software Engineering, The University of Western Australia, 2003.

[21] J. Daugman, "Demodulation by complex-valued wavelets for stochastic pattern recognition," *Int. J. Wavelets, Multiresolution Inf. Process.*, vol. 1, no. 1, pp. 1–17, 2003.

[22] M. B. Stegmann, B. K. Ersbøll, and R. Larsen, "FAME—A flexible appearance modelling environment," *IEEE Trans. Med. Imag.*, vol. 22,no. 10, pp. 1319–1331, Oct. 2003.

[23] K. Messer, J.Matas, J. Kittler, J. Luettin, and G. Maitre, "XM2VTSDB:The extended M2VTS database," in *Proc. 2nd Int. Conf. Audio and*

[24] *Video-Based Biometric Person Authentication*, 1999, pp. 965–966. Y. Chen, Y. Chan, C. Huang, M. Tsai, and Y. Chu, "A multiple-level visual secret-sharing scheme without image size expansion," *Inf. Sci.*,vol. 177, no. 21, pp. 4696–4710, 2007.