JPEG-LS Based Performance Improvement on Biometric Authentication System

Balakrishnan D.

Abstract—this paper discovers the possibility of using visual cryptography for reporting the confidentiality to biometric templates. In addition, the contribution of this paper includes a methodology to preserve 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 XOR operator is used to join the two noisy images and fully recover the original template. The proposed algorithm selects the host images that are most likely to be companionable with the secret image based on geometry and appearance. Then random permutation algorithm (RAP) is used to encrypt the each share with individual host image. In previous research, the reconstructed image quality is pitiable and pixel size of the each share is high which increase the storage requirements of the sheets. To overcome this problem, we have to propose JPEG-LS lossless compression standard refining the image quality as well as diminish the pixel size. A analogous procedure is used to de-identify fingerprint images and iris codes prior to storing them in a central database.

KeyWords -Visual Cryptography, Permutation, Face, Iris, Fingerprints, Thresholding, Privacy, and JPEG-LS Algorithm.

1. INTRODUCTION

In our daily lives, there is a frequent need in identifying people correctly and verifying their identities. To illustrate, reliable identification mechanisms are required when people boarding an aircraft, perform financial operations, desire to enter secure places etc. For higher efficiency and increased security, this identification mechanism should be automated. Obviously, high accuracy is required during the identification and this hardens the automation of identification. But once automated, it gives us the opportunity that tasks performed by computers and other devices can be widened and this results in easing our lives. It is here worth noting that, tasks performed by these devices are based on two separate mechanisms, namely authentication and authorization. Authentication is known as identity verification, whereas authorization defines particular rights of authenticated people. "Biometrics" means "life measurement" but the term is usually associated with the use of unique physiological characteristics to identify an individual. Security is the application which most people associate with biometrics. However, biometric identification eventually has a much broader relevance as computer interface becomes more natural. Knowing the person with whom you are conversing is an important part of human interaction. The method of identification based on biometric characteristics is nowadays preferred over traditional passwords and PIN based methods for various reasons like the person to be identified is required to be physically present at the time-of-identification. Biometrics utilize "something you are" to authenticate identification. This might include fingerprints, retina pattern, iris, hand geometry, vein patterns, voice, and password or signature dynamics. Biometrics can be used with a smart card to authenticate the user. The user"s biometric information is stored on a smart card, the card is placed in a reader and a biometric scanner reads the information to match it against that on the card. This is a fast, accurate and highly secure form of user authentication.

In this system, the use of visual cryptography is explored to preserve the privacy of biometric data (viz., raw images) 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. The system has two types of modules such as enrollment module and authentication module. Figs. 1.1 and 1.2 shows block diagrams of the proposed approach for biometric modalities.

During the enrollment process, the private biometric data is sent to a reliable third-party person. Once the confidential

*(**Author**)D.Balakrishnan is currently pursuing master's degree program in communication system in Anna University Chennai: Regional Center Madurai, India, PH-+918056459379. E-mail: balakrishnandr19@gmail.com*

(Guide) S.Veluchamy is currently working as an assistant professor in Anna University Chennai: Regional Center Madurai, India, PH-+919486186034. E-mail: pvs1834@gmail.com

person receives it, the biometric data is decomposed into two images and the original data is discarded.

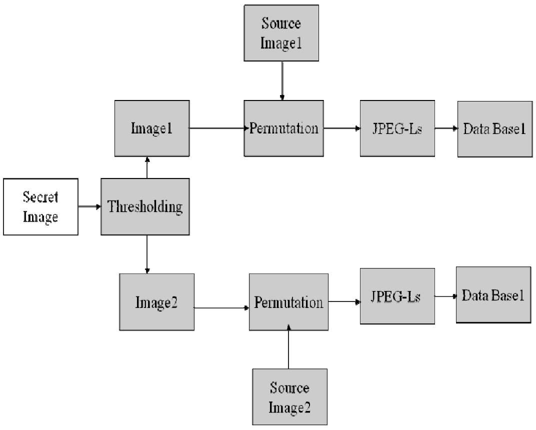

Fig 1.1Enrollment Module

The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server. The image which is to be secured, is sub divided in to 2 sub images using global thresholding process. These sub divided images are permuted using random permutation algorithm.

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 private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking, steganography or cryptosystem approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image.

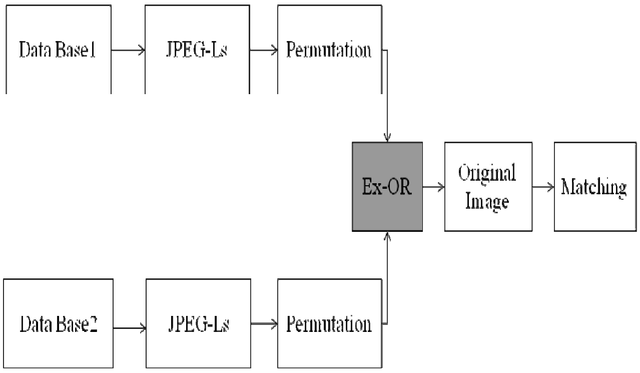

Figure 1.2 Block Diagram of Authentication Module

A system-level overview is presented with the expected conclusion that achieving good performance requires applying judicious design choices for all modules. In particular, both the biometric tasks of identification and verification are applicable in the considered framework. Identification is needed to perform one-to-many searches, while verification is required to perform one-to-one matches. It is important to note that the function of the key binding block is to implement verification, comparing a query sample against the sample(s) of the claimed identity in the database. Clearly, the key binding module depends on other preceding blocks for achieving good performance.

In the case of faces, the performance of the proposed technique was tested on two different databases: the IMM and XM2VTS databases. These databases were used since the facial landmarks of individual images were annotated and available online. These annotations were necessary for the AAM scheme.

2. VISUAL CRYPTOGRAPHY

One of the best known techniques to protect data such as biometric templates is cryptography. It 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.

Naor and Shamir introduced the visual cryptography scheme (VCS) as a simple and secure way to allow the secret sharing of images without any cryptographic computations. VCS is a cryptographic technique that allows for the encryption of visual information such that decryption can be performed using the human visual system. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear.

3. JPEG-LS ALGORITHM

JPEG-LS is a lossless/near-lossless compression standard for continuous-tone images. Its official designation is ISO-14495-1/ITU-T.87. It is a simple and efficient baseline algorithm which consists of two independent and distinct stages called modeling and encoding. JPEG-LS were developed with the aim of providing a low-complexity lossless and near-lossless image compression standard that could offer better compression efficiency than lossless JPEG. It was developed because at the time, the Huffman coding-based JPEG lossless standard and other standards were limited in their compression performance. The decorrelation cannot be achieved by first order entropy of the prediction residuals employed by the interior standards.

JPEG-LS, on the other hand can obtain better decorrelation and these standard was finalized in 1999. JPEG-LS have excellent coding and computational efficiency, and it outperforms JPEG2000 and many other image compression methods. JPEG-LS mainly consist of context modeling, pixel prediction, and prediction error encoding.

In the run mode of JPEG-LS, a run length coding scheme with low computational cost is used to encode constant regions when a zero prediction error occurs. A small compression gain with respect to the static JPEG-LS coding, applied on a frame by frame basis, is obtained at the price of significant increase of computational complexity, delay time, and memory cost.

4. RANDOM PERMUTATION ALGORITHM

A random permutation is a random ordering of a set of objects, that is, a permutation-valued random variable. The use of random permutations is often fundamental to fields that use randomized algorithms such as coding theory, cryptography, and simulation.

b. Permutation Algorithm

$$C^0 = \begin{bmatrix} 1 & 1 & \cdots & \cdots & 1 \\ 0 & 0 & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & 0 \end{bmatrix}_{n\times n} \qquad C^1 = \begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & 0 & \ddots & \vdots & \vdots \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}_{n\times n}$$

```
Step 1: Generate the sharing matrices Co and C1.
Step 2: For each pixel p(i,j), $1\le i \le W$, $1 \le j \le H$.
Step 3: Randomly choose a value l, range from 1to n.
Step 4: For m=1, 2… and n
        1. If the pixel p(i,j) – o(white), the pixel Value
        $S^m(i,j)$ = Co(l,m).
        2. If the pixel p(i,j) – o(black), the pixel Value
        $S^m(i,j) = C_1(l,m)$.
```

5. EXPERIMENTAL RESULTS

In this chapter, the description of proposed system simulation is discussed. The simulation is carried out by using MATLAB simulation software.

a. ORIGINAL IMAGE

Figure shows the simulation result of image which is to be secured by using visual cryptography.

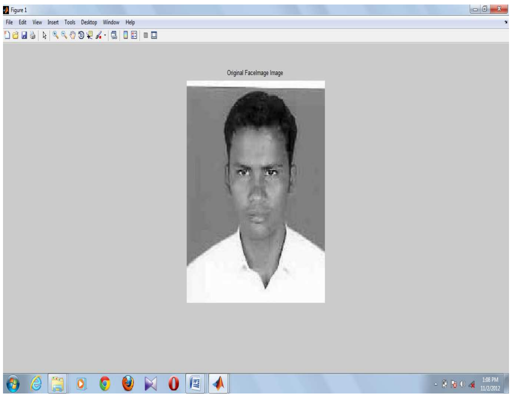

Figure a.1 Original Image

b. RESULT OF HOST IMAGE

The host images that are most likely to be compatible with the secret image based on geometry and appearance (i.e. the aspect ratio between both host and secret image should be matched).

- Secret image of size is M*N.
- Host image of size is P*Q.
- The condition for host image and secret image aspect ratio.

P/Q=M/N

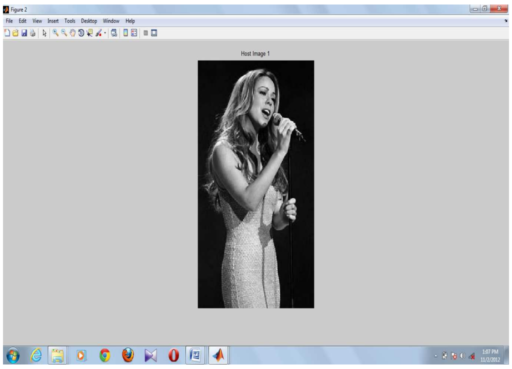

Figure b.1(a) Result of Host Image 1

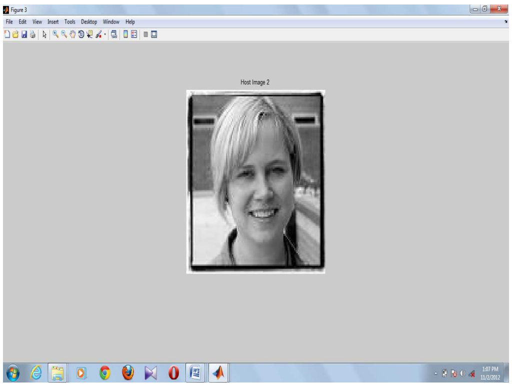

Figure b.2(b) Result of Host Image 2

c. RESULT OF SEGMENTED IMAGE AND ENCRYPTED IMAGE

The image which is to be secured is first dithered in to foreground and background using global threshold process. The foreground part is embedded or hidden into first source image using low parameter quantization table and background part is embedded in to second source image using high parameter quantization table. The foreground and background slices are encrypted using JPEG LS compression algorithm.

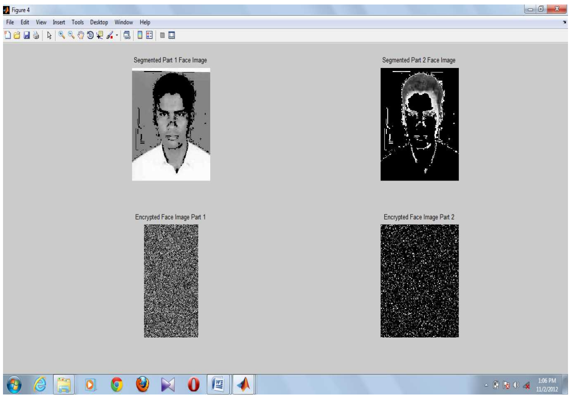
Figure 4
File Edit View Insert Tools Desktop Window Help
Segmented Part 1 Face Image
Segmented Part 2 Face Image
Encrypted Face Image Part 1
Encrypted Face Image Part 2

Figure c.1 Result of Segmented and Encrypted Image

d. ENCRYPTION KEY

The image which is to be secured, is sub divided in to 2 sub images using global thresholding process. These sub divided images are permuted using random permutation algorithm. The permuted pixels are stored as .mat file for further compression based encryption. Then the .mat file is used as key for encryption and decryption of image.

e. RESULT OF DECRYPTED IMAGE

Decryption is reverse operation of encryption. For secret decryption, must know the key is used to encrypt the data. For public key decryption, must know either public key or private key. The figure shows the simulation result of decrypted image which is to be used for authentication process. Here .mat file is used as key to decrypt the encrypted image.

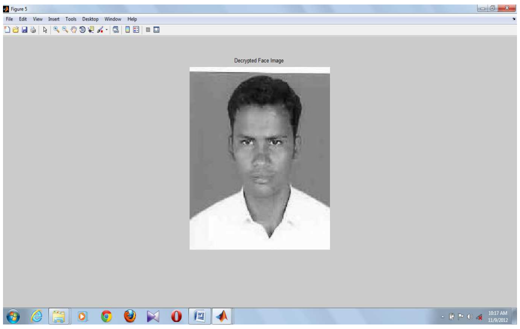

Figure e.1 Result of Decrypted Image

f. PERFORMANCE ANALYSIS

The performance system can be analyzed by evaluating the parameters such as PSNR, Error rate and time for both encryption and decryption of image. Also find out the compression ratio of image and compare with exist methods. The PSNR is most commonly used as a measure of quality of reconstruction of lossy compression codec's. The signal in this case is original data, and noise is the error introduced by compression. The equation of PSNR

$$PSNR_t = 10\log_{10}\frac{255^2}{\frac{1}{w\times h}\sum_{j=0}^{h-1}\sum_{i=0}^{w-1}(f_t(i,j)-\hat{f}_t(i,j))^2}$$

Mean square error is a risk function corresponding to the expected value of the squared error loss and which measures the average of the squares of the errors. MSE The performance of the biometric system is described in the table f.1.

Table f.1 Performance analysis

Image Type	Encryption Time (Min)	Decryption Time (Min)	PSNR	MSE
Facial Image 1	0.186332	0.29233333	90	2
Facial Image 2	0.083714	0.185015	62.1269	139.256
Finger Image 1	0.146163	0.178997	26	49.12
Finger Image 2	0.176163	0.223451	31.342	43.7294

g. PERFORMANCE COMPARISION

For comparison, we have included the performance of a state- of- the-art lossless encoder JPEG-LS with lossy encoder JPEG image compression. The performance parameters PSNR, MSE and compression ratio of JPEG-LS are to be compared with JPEG compression standard and is to be noted in table g.1

Table g.1 Methodology comparison

Methodology	Image Type	PSNR	MSE	Compression Ratio
JPEG Compression	Facial	44.1	155.6732	72%
JPEG-LS Compression	Facial	90	2	25%

The performance of the proposed method was compared with those of existing method. The performance of both proposed technique and existing technique is shown in table 3. The measuring parameters are elapsed time for both encryption and decryption, error rate of recovered image should be discussed in table g.2.

Table g.2 Performance Comparison

Content	Image Type	Encryption Time (Sec)	Decryption Time (Sec)	Error Rate
Existing Method	**Facial**	22.0751	33.9654	65%
Proposed Method	**Facial**	18.6332	29.233333	2%

6. CONCLUSION AND FUTURE WORK

This paper discovers the possibility of using visual cryptography for reporting the privacy to biometric templates. In addition, the influence of this paper includes a methodology to preserve 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 XOR operator is used to superimpose the two noisy images and fully recover the original template. The proposed algorithm selects the host images that are most likely to be compatible with the secret image based on geometry and appearance. VCS is then used to encrypt the private image in the selected host images. It is observed that the reconstructed images are similar to the original private image. Finally, experimental 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 M can lead to an increase in the storage requirements for the sheets. In order to overcome this problem and also improve the quality of a recovery image, we have to apply lossless compression standard JPEG-LS compression algorithm. In future work, the elapsed time of the image should be further reduced in order to improve the performance of the system and also performing the matching process to find out the EER value of image. Applying the same kind of scenario for the video based biometrics and also verifying the authentication by this above scenario for both still image and video based biometrics.

7. ACKNOWLEDGMENT

I thank Mr. S.Veluchamy, Asst. Professor of ECE in Anna University, Regional Centre-Madurai for his support in guidance and also thank our staffs and Students for their timely help. And the author would like to thank the anonymous reviewers for providing constructive comments and suggestions that have contributed to the improvement in the quality and presentation of this paper.

REFERENCES

[1]. Arun Ross (2011), Senior Member, IEEE, and Asem Othman, Student Member, IEEE,“Visual Cryptography for Biometric Privacy”,IEEE Transactions On Information Forensics And Security, Vol. 6, No. 1.

[2]. Dong.J and Tan.T (2008), “Effects of watermarking on iris recognition performance, “in Proc. 10th Int. Conf. Control, Automation, Robotics and Vision.

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

[4]. Jain.A and Uludag.U (2003), “Hiding biometric data,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 25.

[5]. Lin.T, Horng.S, Lee.K, Chiu.P, Kao.T (2010) , “A novel visual secret sharing scheme for multiple secrets without pixel expansion,” Expert Systems With Applications, vol. 37,no. 12, pp. 7858–7869

[6]. Ratha.N, Connell.J, and Bolle.R (2001), “Enhancing security and privacy in biometrics-based authentication systems,” IBM Syst. J., vol. 40.

[7]. Rao.Y, Sukonkina.Y Bhagwati,C (2008), “Fingerprint based authentication application using visual cryptography methods (improved id card),” in Proc. IEEE Region 10 Conf., Nov, pp.1–5.

[8]. Ross.A and Othman.A (2010), “Visual cryptography for face privacy,”in Proc. SPIE Biometric Technology for Human Identification VII, Orlando,FL, vol. 7667.