Stegnography Using Visual Cryptography, RSA and DWT

Madhuri Ghuge[1], **Prof.Kanchan Doke**[2]
[1,2]Computer Engineering Department
[1,2]Bharati Vidyapeeth's college of Engineering, Navi Mumbai,India

Abstract— Visual cryptography (VC) schemes encrypt a secret image into two or more cover images, called shares. The secret image can be reconstructed by stacking the shares together. Encoding data based on binary encoding methods and visual cryptography schemes is used to share pixels of a covert data to form two shadow matrices. Then, the two shadow matrices are encoded into a host image to form an overt image. The overt image contains matrix in encrypted form that is derived from two shadow matrices using RSA algorithm. Encrypted matrices are embedded in host image. This method makes use of binary encoding, visual cryptography, cryptography and Haar transform for hiding data into image.

Key words: Shares, Overt image, Shadow images, PCA, VC

I. Introduction

Recent advancements in Internet technologies have enabled information sharing and have brought the world closer. At the same time security concerns have grown proportionally. This has led to organizations, institutions and individuals spending exorbitant amounts of money to secure their data. Naor and Shamir proposed a "(k,n)-threshold visual secret sharing scheme" in the year 1994 [7], which is now commonly referred to as Visual Cryptography(VC). The major feature of their scheme is that the secret image can be decrypted simply by the human visual system. Thus no knowledge of cryptography is required when a user uses a system employing visual cryptography. Each share looks like a collection of random pixels and appears meaningless by itself. The generated shares alone do not reveal the security level of the secret image is enhanced. Information encryption techniques are usually used to hide confidential data or images. There are two main types of information encryption techniques [10]. The first type uses optical methods to encode and decode information. The second type uses digital methods to encode and decode information. Because both encoding and decoding procedures are executed with light, decoded information usually contains noises for the optical type of encryption techniques. As both encoding and decoding procedures are executed with calculations, decoded information can contain few or no noises for the digital type of information encryption techniques. VC can be used in many applications, which include information hiding, transmitting financial documents (VCRYPT), banking applications , remote electronic voting applications for authentication and validation. More recent applications are in the field of biometrics such as face privacy, iris authentication and fingerprint scanning.

II. Literature survey

A. Visual cryptography by Naor and Shamir

Visual cryptography (VC) is one of the most important aspects of information security. The theory of visual cryptography scheme was introduced by Naor and Shamir in 1994 [7]. It encrypts a secret image by sharing matrices onto transparencies and giving them to *n* shadow matrices. The secret image can be recovered by viewing the overlapped transparencies. Each shadow matrix is usually a random looking picture that appears distinctly different from an innocent looking meaningful share image.

B. Visual cryptography by Kafri and Karen

Kafri and Keren visual cryptography generates shares first by Visual Cryptography VC (2, 2) scheme. Then both shares were embedded into the cover images with the help of watermarking. For reveal of secret image, the extraction process was used to extract the shares from the embedded images. At last both shares were overlapped and revealed the secret image. Two cover images have been used to hide the shares which require extra memory space. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality. But still there is noise and distortion in recovered image

C. Visual cryptography by Anto and Monoth

The (k,n) visual cryptography needs 'k' shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography [9] eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced. The visual quality obtained by the new method is significantly better than that attained by extended VC or any other available VC method known to date.

D. Extenden visual cryptography for color image

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Savita Patil1, Jyoti Rao proposed Extended visual cryptography for natural images constructs meaningful binary images as shares [3]. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, their paper establishes the extended visual cryptography scheme suitable for natural images.TABLE 1 shows comparison of VC schemes studied in lirature survey.

VC scheme	Pixel expansion	Quality of decoded data	security	Suspicion of data hiding
Basic VC	required	poor	less	yes
Watermarking VC	required	poor	less	yes
Random grid VC	not required	poor	less	yes

Extended VC	not required	poor	high	yes
Halftone VC	required	good	less	yes

Table 1: Comparison Of Various Vc Schemes

There are methods for visual cryptography where the decoding processes are computation-free. But the decoded covert data comparing with the original covert data has distortion and noise. Loss or theft of shares is a major security issue.There is a possibility of retrieval if hackers are able to collect all the shares. There is less focus on good quality of reconstructed image &security with minimum pixel expansion.

III. METHODOLOGY OF THE PROPOSED SCHEME

The proposed scheme generates the VC shares using basic Visual Cryptography model and then encrypt both shares using RSA algorithm of Public Key Cryptography so that the secret shares will be more secure and shares are protected from the malicious adversaries who may alter the bit sequences to create the fake shares. During the decryption phase, secret shares are extracted by RSA decryption algorithm & stacked to reveal the secret image. Figure. 3.1shows complete scheme.

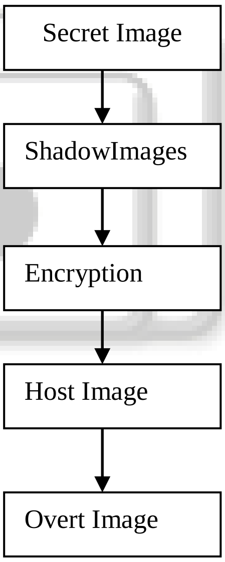

Fig. 1: Flow from Host to Overt image

A. *Visual cryptography for shares*

Let C be a r X c covert data to be encoded and let D1 and D2 be two rp X cq shadow matrices formed from the VC scheme of C by using a p X q sharing matrix S. The constructing processes [1] for deriving D1 and D2 from C are shown below. First, map the pixels of C to form a pixel string A with rc elements according to a specified order. Then, take every pixel in A to form the elements of E1 and E2 in sequence by the sharing-matrix dimension codes p and q until all pixels in A have been shared in two p X rcq shadow matrices E1 and E2. Then, transform the pixels of E1 and E2 into two rp X cq shadow matrices D1 and D2 according to a specified order respectively.

When the sharing-matrix dimension codes p and q are all equal to 1, the size of each shadow matrix is the same as the size of the covert data without any expansion. For the case, the algorithm for image encryption is used. The steps of the algorithm are shown below.

- Step 1: Generate a random matrix E1 which has the same size with A.
- Step 2: Fetch a not-yet-process pixel A(i,j) from A according to the specified order.
- Step 3: Examine the value A(i,j), and then proceed with one of the following substeps:
- Step 3.1 If A(i,j) is 0, then E2(i,j)= E1(i,j).
- Step 3.2 If A(i,j) is 1, then E2(i,j)=1- E1(i,j).
- Step 4: Repeat steps 2 and 3 until all pixels in A are processed.

B. *Algorithm*

- Step 1: Apply Haar transform on the image.
  Haar transform divides the image into four regions LL, HH, HL, LH.
- Step 2: Divide LL and HH into blocks.
  Divide LL and HH in 32x32 blocks each. Process each Block separately by selecting six continuous bocks.
- Step 3: Apply PCA to LL and HH.
  Covariance matrix is computed using PCA. Then the eigenvalues and corresponding eigenvectors of covariance Matrix are solved and obtain the projection matrix. Finally, the samples are projected on the projection matrix
- Step 7: Encrypt the imagesD1 and D2.
  Image is encrypted using RSA algorithm
- Step 4: Choose two multiplying factors.
  Two multiplying factors are chosen to add encrypted
  shadow images D1 andD2 in LL and HH blocks of
  host image to get new LL1 and HH1.
- Step 5: Apply Inverse PCA.
  Inverse PCA is applied to obtain LL and HH for reconstruction of host image
- Step 6: Apply Inverse DWT.
  IDWT is applied to obtain combined blocks LL1, HH1, LH, and HL

C. *Performance Metrics*

The following objective metrics can be used for comparison between the original secret image and the reconstructed secret image:

- Mean Square Error (MSE): It measures the average of the square of the error. The error is the amount by which the pixel value of original image differs from the pixel value of decrypted image.

$$\mathrm{MSE} = \frac{\sum_{i=0}^{M}\sum_{j=0}^{N}(x(i,j)-y(i,j))}{MN} \qquad (1.1)$$

Where x(i,j) represents the original image, y(i,j) is the decrypted image and (i,j) represent the pixel positions of the MxN image. Here, M and N are the height and width of image respectively.

- Peak signal to noise ratio (PSNR): It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is usually expressed in terms of the logarithmic decibel. PSNR is given by

$$\mathrm{PSNR} = 10\log\frac{255\mathrm{X}255}{\mathrm{MSE}} \qquad (1.2)$$

IV. Experimental results

Proposed scheme has been implemented in MATLAB 7.6. To run this scheme minimum hardware configuration is required with no extra specifications. The experiments have been run in Windows 7 on a HP laptop with Intel i5 2.4 GHz processor.To test the performance of this scheme number of experiments has been conducted with varying image sizes, types & keys but every time secret image is retrieved with good visual quality. Results of some experiments are shown in Figure.4.1, Figure.4.2 & Figure.4.3.

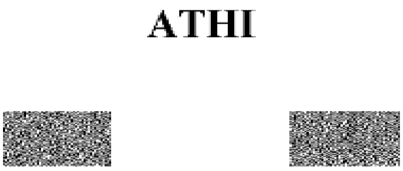

Fig. 2

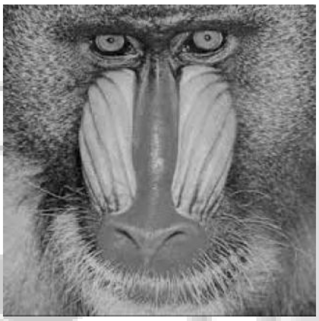

Fig. 3

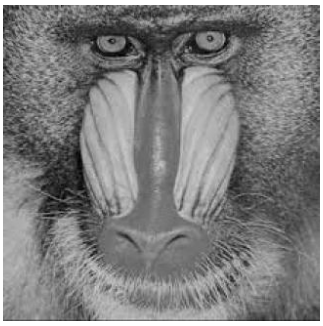

Fig. 4

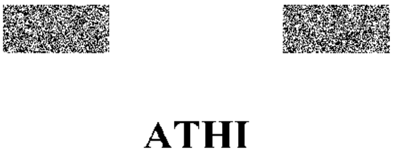

Fig. 5

Fig. 2 shows the secret image is divided into two unreadable shares. Fig. 3 shows original host image for embedding of seret image.Fig. 4 shows overt image after embedding secret image.The Fig. 5 shows the decoded secret data after stacking of the shares.The mse value is 0.429 and PSNR value is 51.8. The difference between original host image and overt image is difficult to detect.

V. Conclusion and future scope

The proposed method encrypts covert data by combining the binary encoding method, visual cryptography scheme, HAAR ransform and RSA algorithm to derive an overt image from host image. The proposed method enhances security level as shares are encrypted before embedding into host image. It reduces suspicion of data hiding as it reduces difference between host image and overt image .The proposed method reduces distortion in decoded data. It does not require pixel expansion.

It has been observed that there are many possible enhancements and extensions exist as the visual quality & size of revealed image.

The major areas of future scope are:

We can work for colour secret image in place of binary image and then generate the shares using Visual Cryptography.Compression of encrypted shares to reduce bandwidth Requirement. We can try for increase in size of input secret image.

References

[1] Kuang Tsan Lin (Author),” Based on Binary Encoding Methods and Visual Cryptography Schemes to Hide Data”, 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing ,VOL. 11, ISSUE 5, AUGUST 2012

[2] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE,” Color Extended Visual Cryptography Using Error Diffusion”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011

[3] Savita Patil1, Jyoti Rao2,” Extended Visual Cryptography for Color Shares using Random Number Generators”, International Journal of Advanced Research in Computer and Communication Engineering VOL. 1, ISSUE 6, AUGUST 2012

[4] Ching-Nung Yang, Senior Member, IEEE, Hsiang-Wen Shih, Chih-Cheng Wu, and Lein Harn,” k Out of n Region Incrementing Scheme in Visual Cryptography”, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 22, NO. 5, MAY 2012

[5] Chandramathi S., Ramesh Kumar R., Suresh R. and Harish S., “An Overview of Visual Cryptography,” IJCI’10, VOL. 1, ISSUE 1, PP. 32-37, 2010.

[6] C. Sasivarnan, A. Jagan, Jaspreet Kaur, Divya Jyoti, and Dr. D.S. Rao, “Image Quality

Assessment In Spaatial Domain," IJCST, VOL. 2, ISSUE 3, SEPTEMBER 2011.

[7] M. Naor and A. Shamir, "Visual cryptography," EUROCRYPT'94-Lecture Notes in computer Science, vol. 950, 1995, pp. 1-12,doi:10.1007/BFb0053419.

[8] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, vol. 12, Jun. 1987, pp. 377-379,doi:10.1364/OL.12.000377.

[9] T. Monoth and B. Anto P, "Tamperproof transmission of fingerprints using visual cryptography schemes," Procedia Computer Science, vol.2, Dec. 2010, pp. 143-148, doi:10.1016/j.procs. 2010.11.018.

[10] K. T. Lin, "Digital information encrypted in an image using binary encoding," Optics Communications, vol. 281, Jul. 2008, pp. 3447-3453, doi:10.1016/j.optcom.2008.03.010

[11] Z. Wang and G. R. Arce, "Halftone visual cryptography via error diffusion," IEEE Trans. In Forensics Security, vol. 4, no. 3, pp. 383-396, Sep. 2009.