International Engineering Journal For Research & Development
Vol.3
Issue 2

High Security Encryption Using AES & Visual Cryptography

Rajkamal Gupta[1], Ankit Sanghavi[2]
[1]Assistant Professor, [2]Assistant Professor
Department of Computer Engineering, ARMIET,SHAHAPUR
THANE-421 601, Maharashtra, India.
[1]rajkamal.gupta@armiet.com,[2]ankit.sanghavi@armiet.com

Abstract— ***Nowadays, many researchers proposed algorithms based on the combination of steganography and visual cryptography method with the aim of high secure secrecy, reliability, accuracy and efficiency for the secret message. Steganography means hides secret data inside another medium and visual cryptography provide high security with less computation when comparative with other methods. The main objective of the proposed work is to develop a novel scheme for shares generation and hides the data in a carrier for secure secret data transmission. In this paper, two level of security is provided which means first layer of security is accomplished by splitting an input image into two shares using VC scheme and second layer of security is accomplished by embedding secret data inside the shares means bits of the secret data is hidden behind the shares bits and so information cannot be revealed with single share. The experimental result shows the feasibility of the novel scheme which is highly secure and reliable. This novel method can be deployed in forensic department or transmits confidential message from sender to receiver that is to be safe and so intruders can't reveal that secret information.***

Keywords: Steganography, Visual Cryptography(VC), shares, Security, Image.

INTRODUCTION

Steganography defines hiding secret information within a carrier file in undetectable form. It is derives from the two Greek words steganos means covered and graphy means writing [1]. If medium hides the secret then it is known as cover medium such as text, image, audio and video file. Image steganography hides secret data within an image is known as stego-image. Steganography has four characteristics such that
secrecy, imperceptibility, capacity, accurate and reliable
Visual Cryptography is a novel method first proposed by Naor and Shamir [3] and in this method, secret images are decomposed into n shares and information can't be visible with an individual shares. Thus, when all the shares are stacked together, information is revealed about the secret image. This scheme can be applicable to information hiding, visual authentication, identification, etc. Extended VC method is introduced by [4] that means shares have secret but these share meaningful. Visual cryptography method is only applied to black, white pixels until 1997. Christo Ananth et al. [6] proposed a system which contributes the complex parallelism mechanism to protect the information by using Advanced Encryption Standard (AES) Technique. AES is an encryption algorithm which uses 128 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder.

The VC scheme is proposed by [7] for gray level images which is based on halftone technique & color decomposition method. The use of steganography in combination visual cryptography is a sturdy model and adds a lot of challenges to identifying such hidden and encrypted data. The rest of the paper is organized as follows: In section 2, some of the related works are discussed. In section 3, novel share creation scheme is implemented along with steganography and algorithm is proposed. In section 3, experiments are carried out and results produced. In section 4, conclusion of the proposed work is given.

RELATED WORK

Ravindra Gupta et al. [8] have proposed novel method in which secure the data hiding using the combination of visual cryptography and steganography in computer forensics. This method use steganographic technique using genetic algorithm and VC using pseudo random number. The Main objective of this method is to highly prevent from RS attack and also it is optimal for both grayscale and color images.

The method proposed by M. Wherate et al. 1) for provide two layer of security by using of VC and steganography. In this method, original image is divided into two shares and here DCT technique is used for

2) steganography where secret shares are covered using stego image. This method can be applicable to online voting, military, navy and etc.

Aishwarya Nandakumar et al. [10] have introduced method based on visual cryptography and steganography is used. Original data is embed Matrix Embedding using Hamming Codes and shares are generated using Random Grids Method. For restore the stego image, stack two shares and from reconstructed stego image, data is extracted using extraction algorithm.

Gokul.M et al. [11] have proposed method that hides the message behind the image using VC and SLSB encryption techniques. In this method, original data is written in an image and share generation algorithm is applied on this image to get two shares. Share images with cover image are given to LSB method. To extract the data from steganographed image, apply the reverse process of encryption.

The novel approach is proposed by Megha Goel et al. [12] for data hiding in which steganography and extended VC is used. In this novel method, hiding data in color image and shares are generated using Visual Information Pixel which is used to maintain possession of place of pixels having visual information of original images and error diffusion technique which is used to produce share of good quality.

Deepa Priya V et al. [13] use Rotation Based Visual Cryptography and LSB based Steganography for transmit secret data with securely. By use of rotation VC, secret data is hiding in two image shares and by use of PVD is termed as Pixel Value Differencing method; secret image shares are hide in the cover image. Merits of this novel method that provides high level of security when PVD is used and also use of rotation operation, secret data is embed into two shares.

PROPOSED SYSTEM:

In steganography based VC, we have proposed a novel scheme for share creation and secret data is hidden behind every shares instead of whole image. In this proposed method, first part is based on secret image decomposition using visual cryptography and second part is based on secret data is embedded inside the shares. At sender side, image (cover image) is read as an input and transform into gray scale image then break into 2 shares using novel scheme. In this scheme, shares are generated by dividing every pixel by two and 2 shares are created. For example, pixel value 14 is read from image and this value is dividing by 2, then creates two shares i.e. share1 hold first 7 and share2 hold another 7. Now, input secret data and it is converted into ASCII values and again coding into binary representation. These binary digits are dividing into two halves. First 4bits is hidden behind the first 4bits of the share2 and last 4bits is hidden behind the last 4bits of the share1.

Example, let take secret data bits 01010111, share1 00000011 and share2 00000011. First 4 bits of secret data is 0101 hidden behind the first 4bits of share2 0000 then, last 4 bits of secret data is 0111 hidden behind the last 4bits of share1 0011.

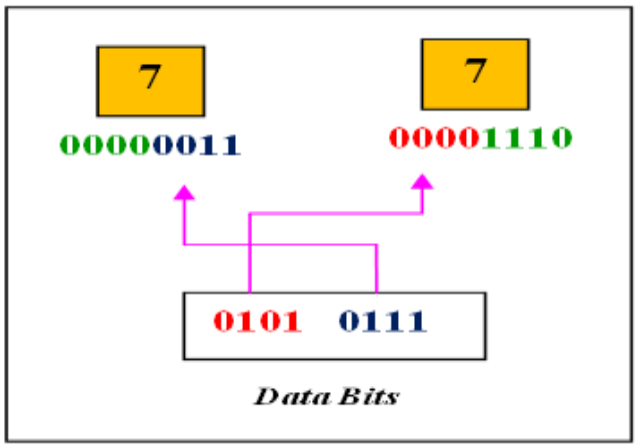

Fig. 1 Example of Data bits embedded

After hidden the data inside the shares and send it to the destination point over the communication channel. At receiver side, if encrypted shares are decrypted then original shares are reconstructed and stacked together to get the secret data what is hidden it. The entire process of proposed method is depicted in the Figure 2.

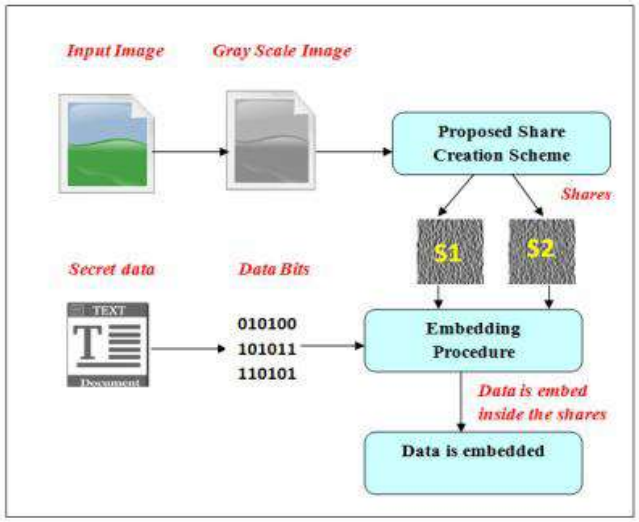

Fig. 2 Process of Proposed System

The algorithm for proposed methodology is as follows

Step 1: Read Cover image as an input image.
Step 2: Transform into gray scale image.
Step 3: Novel share creation scheme is applied in which each pixels are dividing by 2 and by using this values, generate two shares.
Step 4: Repeat step 3 till all the pixels in the gray scale image is decomposed, so resulting in two shares to transmit secret data.
Step 4: Then, secret data is given as an input then this data is convert into ASCII and also represent in binary code.
Step 5: Now, we embedded secret data bits inside the bits of the pixels of the shares by using of fore mentioned embedding procedure.
Step 6: To extract the data, shares are stacked together and receiver get the original data what is embedded.

RESULT AND DISCUSSION:

A. Performance Evaluation

1) Peak Signal to Noise Ratio:

The peak signal to noise ratio is defined as the ratio between the maximum possible power of the signal and the power of corrupted noise.

$$PSNR = 20 * \log_{10}(255/\sqrt{MSE})$$

Where, MSE is the mean square error value of the image. High PSNR (Peak Signal to Noise Ratio) indicate a lower variation between the original (without noise) and reconstructed image. The major benefit of this measure is simplicity of computation, but it does not reflect perceptual quality of the image [15].

3) Mean Square Error : The Mean Square Error is the average square of the error in particular images and the following equation is

$$MSE = \frac{1}{W * L}\left(\sum_{p=1}^{p}\sum_{q=1}^{q}(OI_{pq} - EI_{pq})^2\right)$$

Where, W is the width of the original image, L is the length of the original image, p and q is the row and column value of the pixel, OI is the original image pixel and EI is the decrypted image pixel value. Following table shows the MSE & PSNR for the share1 & share 2.

Cover Image	Size	Share 1	Share 2
Cameraman	256x256	65.6274	64.57894
Pirate	300x256	66.0808	66.2378
Lena	400x400	69.4901	68.9902
Monalisa	512x512	71.6319	71.2479

B. Experimental results

In order to test the proposed methods a test bed of 1000 images was created. The databases used are the UCID dataset and test images [14] widely used in experiments etc. Initially we have taken a 256×256 grayscale image as original image. Table 2 shows the creation two shares using proposed share creation scheme. The sizes of the shares are same as that of the original image. Above table shows the results of Embedding and extracting secret data in the shares using proposed visual cryptography and steganography.

TABLE II
EXPERIMENTAL RESULTS OF THE PROPOSED METHOD

Original Image	*Shares*	*Sample Secret Data*	*Embedded shares*
	 	*Visual cryptography (VC) is the concept of dividing a secret image into „n" shares and revealing secret image by stacking a qualified subset of „n" shares. The scheme is perfectly secure and very easy to implement. Visual cryptography takes the input as one secret image and creates the shares (more than one encrypted images) by the process of encryption, later decryption is done by human visual system.*	 

CONCLUSION

The proposed data hiding technique gives two level of security which means first level is achieved by using of simple share creation scheme and second level is achieved by embedding data inside the shares. Imposters can easily to broken the system whenever single level of security is provided. If steganography is combined with VC yields work well with high level of security. VC has no computation time to decrypting data and also beaten the inauspiciousness of one level hiding which is either cryptography or steganography. In the proposed method, the combination of VC and steganography not only improved security but also yields reliability and efficiency.

REFERENCES

[1] Cole, Eric, and Ronald D. Krutz. Hiding in plain sight: Steganography and the art of covert communication. John Wiley & Sons, Inc., 2003.

[2] Suneetha, B., CH HIMA BINDU, and S. SARATH CHANDRA. "Secured data transmission based video steganography." IEEE International Journal of Mechanical and Production Engineering (IJMPE) ISSN No.: 2315 4489.

[3] Naor, Moni, and Adi Shamir. "Visual cryptography." Advances in Cryptology—EUROCRYPT'94. Springer Berlin/Heidelberg, 1995.

[4] Ateniese, Giuseppe, et al. "Extended capabilities for visual cryptography." Theoretical Computer Science 250.1 (2001): 143-161.

[5] Verheul, Eric R., and Henk CA Van Tilborg. "Constructions and properties of k out of n visual secret sharing schemes." Designs, Codes and Cryptography 11.2 (1997): 179-196.

[6] Christo Ananth, H.Anusuya Baby, "High Efficient Complex Parallelism for Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 01-07.

[7] Hou, Young-Chang. "Visual cryptography for color images." Pattern Recognition 36.7 (2003): 1619-1629.

[8] Gupta, Ravindra, Akanksha Jain, and Gajendra Singh. "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics." International Journal of Computer Science and Information Technologies 3.3 (2012): 4366-4370.

[9] M. Wherate, Dr. S. Sherekar, Dr. V. M. Thakre, "Two Layer Security Using Visual Cryptography and Steganography", International Journal of Advanced Research in Computer Science and Software Engineering 5 (4), April- 2015, pp. 92-95.

[10] Nandakumar, Aishwarya, et al. "A Secure Data Hiding Scheme Based on Combined Steganography and Visual CryptographyMethods." Advances in Computing and Communications. Springer Berlin Heidelberg, 2011. 498-505.

[11] Gokul, M., et al. "Hybrid Steganography using Visual Cryptography and LSB Encryption Method." International Journal of Computer Applications 59.14 (2012).

[12] Goel, Megha, and M. Chaudhari. "Secured Data Hiding By Using Extended Visual Cryptography."

[13] Deepa Priya V, Dr. Sundaram M, "Secret Data Transfer using Rotation Based Visual Cryptography and LSB based Steganography", International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Special Issue 6, May 2015.

[14] Schaefer, Gerald, and Michal Stich. "UCID: an uncompressed color image database." In Electronic Imaging 2004, pp.472-480. International Society for Optics and Photonics, 2003.

[15] K.Shankar and P.Eswaran. "An Efficient Image Encryption Technique Based on Optimized Key Generation in ECC Using Genetic Algorithm", Advances in Intelligent Systems and Computing, Springer, Vol. 394, pp.705-714, 2016.