Implementation of Random Image Visual Cryptography

Omkar Tiware[1], Prof. Kirti Rajadnya[2]

[1]Student in Department of IT, SSJCOE, Affiliated to University of Mumbai
[2] Associate Professor, Department of Information Technology SSJCOE, University of Mumbai

---

Abstract- *Here new encryption technique is proposed. Steganography and Visual Cryptography is used together to add multiple layers of security. Using Steganography, the secrete text message is hidden in a cover image. The stenographer image is now sliced into multiple shares using Visual Cryptography and transmitted in an open system environment.*

At the receiver end the received shares are stacked one on top of another to generate the cover image which has the message text hidden in it. This is done by Visual Cryptography. Now Steganography is used on this image to obtain the secrete text message.

***Key Words*: Visual Cryptography, Watermarking, Steganography, Shares, Encoding, Decoding.**

1. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Data encryption technique converts data into an unreadable format so as to protect the information from external intrusion. It is thus useful in ensuring the privacy and security of the information transferred or shared between the systems.

Visual cryptography (VC), proposed by Noor and Shamir, is a paradigm for cryptographic schemes that allows the decoding of concealed images without any cryptographic computation. Particularly in a k-out-of-n visual secret sharing scheme (VSS), a secret image is cryptographically encoded into n shares. Each share resembles a random binary pattern. The n shares are then photocopied onto transparencies respectively and distributed among n participants.

The secret images can be visually revealed by stacking together any k or more transparencies of the shares and no cryptographic computation is needed. However, by inspecting less than k shares, one cannot gain any information about the secret image, even if infinite computational power is available.

At this point we need to describe the term 'Steganography'. Steganography, literally means, "Covered Writing" which is derived from the Greek language. Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present"

In a digital world, Steganography and Cryptography are both intended to protect information from unwanted parties. Both Steganography and Cryptography are excellent means by which to accomplish this but neither technology alone is perfect and both can be broken. It is for this reason that most experts would suggest using both to add multiple layers of security Stenographic technologies are a very important part of the future of Internet security and privacy on open systems such as the Internet. Stenographic research is primarily driven by the lack of strength in the cryptographic systems and the desire to have complete secrecy in an open-systems environment.

2. RELATED WORKS

Jthi et al in their paper titled ―Progressive Visual Cryptography with Watermarking for meaningful shares‖ [1] discuss how progressive visual cryptography (PVC) can be utilized to recover the secret image gradually by superimposing more and more shares. If we have a few pieces of shares, we could only get an outline of the secret image. By increasing the number of the shares being stacked, the details of the hidden information can be revealed progressively. Even though no one can obtain any hidden information from a single share, this type of visual cryptography technique is insecure as the shares generated are noise like (random looking) images and have more interest of hackers as they treat them as critical information in the transmission. If the random looking shares are enveloped into some meaningful images the interest of hackers can be reduced.

Young-Chang Hou and Zen-Yu Quan in their paper titled—Progressive Visual Cryptography with Unexpanded Shares‖[2]discussed a progressive visual cryptography scheme with pixel-unexpanded shares to solve the main problems such as leak of secret information, pixel expansion, and bad quality of recovered images. Here Young and Zen's method to generate shares is used.

Soumik Das et al in their paper titled —A secure key based Digital Text Passing System through Color Image Pixels‖[3] discuss a framework for embedding text string into digital color images and the text that is embedded is perceptually invisible to Human Visual System (HVS).

Joyshree Nath et al in their paper titled —Advanced Steganography Algorithm using encrypted secret message‖[4] discuss how to embed some secret message inside any cover file in encrypted form so that no one will be able to extract actual secret message. Here they used the standard steganography method i.e. changing LSB bits of the cover file. Thus encryption method can use maximum encryption number=64 and maximum randomization number=128. The key matrix may be generated in 256! Ways. So in principle it will be difficult for anyone to decrypt the encrypted message without knowing the exact key matrix.

Yu-Chi Chen et al in their paper titled —Comment on —Cheating Prevention in Visual Cryptography‖[5] discuss how to cryptanalyze the Hu–Tzeng CPVSS scheme and show that it is not cheating immune. A visual secret-sharing scheme is said to be a cheating-prevention scheme if the probability of successful cheating is negligible. Intuitively, cheating can be prevented if participants suspect that some shares or the reconstructed images are not genuine. Based on this intuition, there are two approaches in designing CPVSS schemes. One is based on share authentication where each participant is provided with an additional share to authenticate other shares. The other is based on blind authentication where some property of the image is used to authenticate the reconstructed secret image. The goal of share authentication is to provide the participants the ability to verify the integrity of the shares before reconstructing secret images, and the goal of blind authentication is to make it harder for the cheaters to predict the structure of the shares of the other participants.

Zhi Zhou et al in their paper titled —Halftone Visual Cryptography‖[6] discuss a novel technique named halftone visual cryptography to achieve visual cryptography via half toning.

3. PROBLEM DEFINITION

In the literature review of a number of papers we have seen that various authors have encountered numerous problems such as pixel expansion, large memory requirement and the requirement of a complex system for encryption and decryption to transmit information securely over an open ended channel such as the internet. By using Visual Cryptography we reduce the computational time required by the system. A less complex system is required ,since in the decryption process the shares have to be stacked one on top of another to generate the secrete image We propose the system which uses the method of un-expandable shares. By doing so we have increased the contrast of the stenographer image. Since the pixels of the image have not been expanded we have effectively reduced the memory requirement of proposed system.

Thus we have intended to eliminate a large number of problems that other systems have encountered.

4. IMPLEMENTATION

1. Encryption Steps Using Visual Cryptography and Steganography.

Step 1 Encoding using Steganography

1. Browse through the image.
2. Get the pixel.
3. Separate the pixels in its Red, Green and Blue components.
4. Get the message character.
5. Fetch the bits of the message characters.
6. Store the message in the selected pixel component using LSB Technique.
7. Save the image in hard disk.

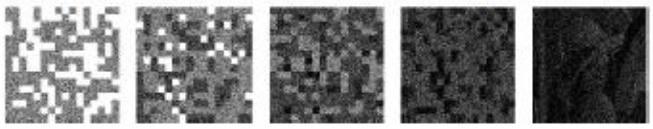
LSB is the most popular Steganography technique. It hides the secret message in the RGB image based on it its binary coding.

(a) (b) (c) (d) (e)

Fig. 2. Proposed $(2,5)$-threshold progressive VCS with $p = 0.1$. (a) shows a share; (b), (c), (d) and (e) show the resulting images obtained from stacking k shares, $k = 2, 3, 4$, and 5(all shares), respectively.

(a) (b) (c) (d) (e)

Fig. 3. Proposed $(2,5)$-threshold progressive VCS with $p = 0.5$. Figures (a)-(e) correspond to those of Fig.2.



(a) (b) (c) (d) (e)

Fig. 4. Proposed $(3,5)$-threshold block-wise progressive VCS. Figures (a)-(e) correspond to those of Fig.2.

(a) (b) (c) (d) (e)

Fig. 5. Proposed XOR-based progressive VCS with $n = 5$. Figures (a)-(e) correspond to those of Fig.2.

(a) (b) (c) (d) (e)

Fig. 6. The Hou–Quan scheme with $n = 5$. Figures (a)-(e) correspond to those of Fig.2.

Algorithm (1) Least Significant Bit Hiding Algorithm.

Inputs: RGB image, secret message.
Output: Steno image.

Begin

Scan the image row by row and encode it in binary. Encode the secret message in binary.
Check the size of the image and the size of the secret message. Start sub-iteration 1:

Choose one pixel of the image randomly
Divide the image into three parts (Red, Green and Blue parts)

Hide one bit of the secret message in each part of the pixel in the least significant bits.

Set the image with the new values and save it.

End

Step 2 Slicing the image using Visual Cryptography

The image is split into multiple shares. The shares so generated reveal no information about the original secrete image. The following steps describe how Visual Cryptography is performed on the secrete image which is to be transmitted.

1) Generate random number of sequence between width and height of the image.

2) Get the pixel color value from the nth location of the image.

3) Insert the pixel color in selected share

4) This process is repeated till all pixels of the image are inserted in the shares.

5). After Encryption the message is transmitted over the channel.

6). Decryption Steps Using Visual Cryptography and Steganography**.**

Step 3 Stacking *the* image at the receiver using Visual Cryptography.

1) After receiving the shares (slides) browse all the pixels of the shares and store it in the master slide.

2) Display the master image on the serene.

3) Repeat this process for all the shares.

Step 4 Decoding using stenography.

1) Browse the image pixel by pixel.

2) Get the image pixel.

3) Fetch the D0 th bit from the pixel component.

4) Similarly fetch the remaining bits

5) Reverse all the bits.

6) Combine all the characters in the string.

7) Return the message.

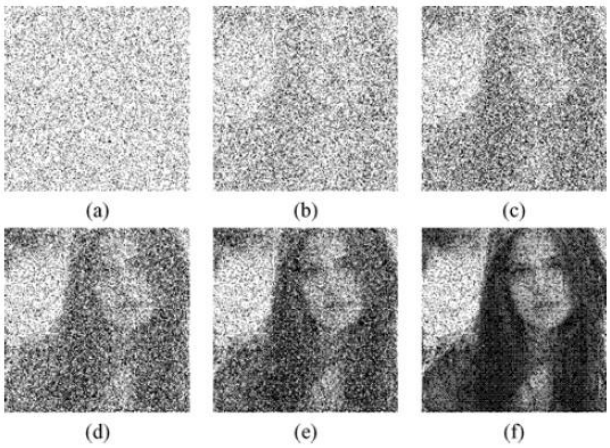


Fig. 3. *Mena* is reconstructed by stacking different numbers of shadow images. (a)–(f) Any 1–6 shadow images stacked.

5. CONCLUSIONS

Here we have proposed an enhanced encryption method which is a combination of Visual Cryptography System (VCS) and Stenography. Both these systems have their own drawbacks but when used together our system becomes more immune to unauthorized access of secrete information. In our system the contrast of the received secrete image is relatively good as no pixel expansion of the secrete image is done. We do not require a very complex system and the memory requirement of the system is small.

REFERENCES

[1] Jthi P.V. and Anitha T Nair. "Progressive Visual Cryptograpy with Watermarking for meaningful shares", IEEE, 2013.

[2] Young-Chang Hou and Zen-Yu Quan. "Progressive Visual Cryptography with Unexpanded Shares" IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 21, NO. 11, NOVEMBER 2011

[3] Soumik Das, Pradosh Bandyopadhyay, Prof. Alai Chaudhari and Dr.Monalisha Banerjee, " A secure key based Digital Text Passing System through Color Image Pixels" IEEE International Conference On Advances In Engineering, Science And Management (ICAESM-2012) March 30,31,2012

[4] Joyshree Nath and Asoke Nath "Advanced Steganography Algorithm using encrypted secret message" (IJACSA) International Journal of Advanced Computer Science and Applications ,Vol. 2, No.3, March 2011

[5] Yu-Chi Chen Gwoboa Horng, and Du-Shiau Tsai" Comment on Cheating Prevention in Visual Cryptography" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 7, JULY 2012

[6] Zhi Zhou, R. Arce, and Giovanni Di Crescenzo. "Halftone Visual Cryptography" IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 15, NO. 8, AUGUST 2006

[7] Ch.Ratna Babu, M.Sridhar and Dr. B.Raveendra Babu ."Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security", IEEE. 2013

[8] Silvana and Edlira Martiri. "Wu-Lee Stenographic Algorithm on Binary Images Processed in Parallel" International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol: 12 No: 03, June 2013

[9] Shyong Jian Shyu and Hung-Wei Jiang ,"Efficient Construction for Region Incrementing Visual Cryptography" ,IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 22, NO. 5, MAY 2012

[10] Xiang Wang, Qingqi Pei, and Hui Li . "A Lossless Tagged Visual Cryptography Scheme"
IEEE SIGNAL PROCESSING LETTERS, VOL. 21, NO. 7, JULY 2014

[11] Mamta Juneja and Parvinder Singh Sandhu, (2013) "A New Approach for Information security using an Improved Steganography Technique", Journal of Info.Pro.Systems, Vol 9, No: 3, pp.405-424.

BIOGRAPHIES:

Omkar R. Tiware is pursuing his B.E. in Information Technology from SSJCOE, University of Mumbai, India. His interested areas include Data Analytics, Business Intelligence, Data Mining and Cryptography. He also loves Digital Marketing and has lead various projects in IT Innovation.

Prof. Kirti Rajadnya is an Associate Professor at SSJCOE, Dombivli Affiliated to University of Mumbai. She has pursued her Masters in the field of Electronics from SPIT, Mumbai University and has an experience of 20 years in teaching IT and Electronics.