TWO LEVEL DATA SECURITY SYSTM USING IMAGE SLICER WITH STEGANOGRAPHY

Prof. Shirish V. Pattalwar[1]
Associate Professor, Dept. of Comp. Science & Engg.
Prof. Ram Meghe Institute of Tech. and Research
Badnera, Amravati, India
shirishpattalwar@rediffmail.com

Mohan Kumar[2]
M.E. (Final Yr.), Dept. of Elect. & Telecom. Engg.
Prof. Ram Meghe Institute of Tech. and Research
Badnera, Amravati, India
mohankumarji@yahoo.com

***Abstract*— The main purpose of a security system is to transfer data securely in an open system environment. There are various ways of doing this. Sometimes multiple methods are used simultaneously to add multiple levels of security for data transfer. Cryptography and Steganography are the basic methods used in a security system. Cryptography is the science of encrypting data in such a way that nobody can understand the encrypted message, whereas in Steganography the existence of data is conceived, means its presence cannot be noticed. The information to be hidden is embedded into the cover object which can be text, image, audio or video so that the appearance of cover object doesn't vary even after the information is hidden. This paper presents a two level data security system using Visual Cryptography and Steganography.**

Keywords*— *Visual Cryptography, Steganography, Shares.

I. INTRODUCTION

Visual Cryptography is the secrete image sharing scheme used to protect against unauthorized data access and secure dissemination of sensitive information. Visual Cryptography is the technique that encrypts a secret document or image by breaking it into shares. The secret image can be reconstructed by stacking the shares together, with no complex cryptographic calculations.

Steganography methods can be classified mainly into six categories as shown in Figure 1, although in some cases exact classification is not possible.

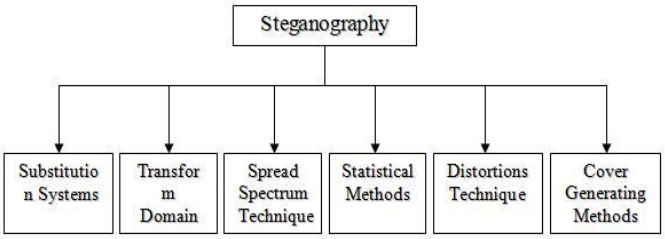

Figure 1. Different Steganography Methods

With the boost of computer power, the internet and with the development of Digital Signal Processing (DSP), Information Theory and Coding Theory, Steganography and Visual Cryptography went "Digital". In the realm of this digital world Steganography and Visual Cryptography has created an atmosphere of corporate vigilance that has spawned various interesting applications of the science.

II. CURRENT SYSTEMS AND THEIR DRAWBACKS

In this highly digitalized world, the Internet serves as an important role for data transmission and sharing. However, since it is a worldwide and publicized medium, some confidential data might be stolen, copied, modified, or destroyed by an unintended observer. Therefore, security problems become an essential issue. Encryption is a well-known procedure for secured data transmission. Frequently used encryption methods include RSA, DES (Data encryption standard). Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. These unnatural messages usually attract some unintended observers' attention. This is the reason a new security approach arises.

In the literature review of a number of papers it has been seen that various authors have encountered numerous problems to transmit information securely over an open ended channel such as the internet.

By using Visual Cryptography, decryption time required by the system can be reduced. Here 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. A system which uses the method of undependable shares has been proposed. The contrast of the received image and hence image quality will thus improve. The system will also require less memory.

When shares are transmitted over a channel there is a possibility that hackers may try to decode the image. This is because the shares generate suspicion in the mind of hackers.

To overcome this Steganography technique is used. In Steganography, the text message is hidden in a cover image. By doing so another layer of security has been added in the system. In Steganography secret message is the text data that the sender wishes to remain confidential. This text data is represented by a stream of bits. The cover or host is the medium in which the message is embedded and serves to hide the presence of the message. The cover-image with the secret data embedded is called the "Stego-Image". The Stego-Image should resemble the cover image under casual inspection and analysis. There are two things that need to be considered while designing the steganographic system: (a) Invisibility: Human

eyes cannot distinguish the difference between original and stego image. (b) Capacity: The more data an image can carry better it is. However large embedded data may degrade image quality significantly.
Thus, in the proposed system a number of problems such as only one layer of security, bad image quality, image having low contrast, non graphic user interface, slow systems, capability of handling only monochrome images, static systems, pixel expansion, large memory and a complex systems have been eliminated.

III. IMPLEMENTATION

A. *Encryption Steps Using Visual Cryptography and Stegnography as shown in Figure 2.*

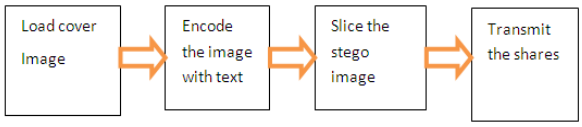

Figure 2. Block diagram of embedding process

1) *Encoding using Stegnography.*

Least Significant Bit Hiding Algorithm which is used for encoding is as follows:

Inputs: RGB image and secret text message.
Output: Stego image.

a) Scan the image row by row and encode it in binary.
b) encode the secret message in binary.
c) check the size of the image and the size of the secret message.
d) choose one pixel of the image randomly
e) divide the image into three parts (Red, Green and Blue parts)
f) hide one bit of the secret message in each part of the pixel in the least significant bits.
g) set the image with the new values and save it.

2) Slicing the image using Visual Cryptography

Algorithm for slicing process is as follows:

Input: Stego image, patch size and number of slides.
Output: Meaningless shares of stego image.
a) Get stego image
b) Get patch size and get total slides
c) Generate all statistics like,
Cols = width / patch size
Rows = height / patch size
Total patches = rows * cols
Patches per slide = total patches / slides
d) Generate blank slide images and store in slide array
e) Generate XY coordinates of all patches and store in patch XY array.
f) Generates patch IDX array for shuffling.
g) Shuffle the array.
h) Take one patch at a time.
h.1. Fetch the coordinate of x,y of current patch
h.2. Copy all the pixels of current patch to the selected slide
i) Go to next slide
j) Update panel
k) Save slides.

B. *Decryption Steps Using Visual Cryptography and Steganography as shown in Figure 3.*

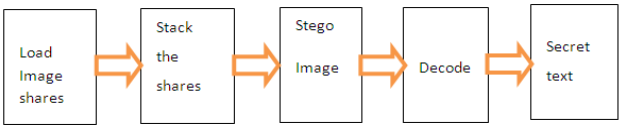

Figure 3. Block diagram of extraction process.

1) *Stacking of shares using Visual Cryptography*

Algorithm for Stacking the slide images is as follows:
Input: All meaningless shares of the stego image.
Output: final image same as stego image.
a) Open all side images
b) Take one slide at a time.
b.1. XOR all the pixel of current slide and stacked slide
c) Update panel
d) Save image.

2) *Decoding using Steganography.*

Algorithm to extract the text message is as follows:

a) Browse the image pixel by pixel.
b) Get the image pixel.
c) Fetch the D0 th bit from the pixel component.
d) Similarly fetch the remaining bits
e) Reverse all the bits.
f) Combine all the characters in the string.
g) Return the message.

IV. RESULT

Now we discuss and compare the various parameters obtained. Different parameters obtained when the Patch size is varied but the number of slides are kept constant in the Slicing process as shown in Table 1.

Table 1. Different parameters obtained when the Patch size is varied but the number of slides are kept constant in the Slicing process.

Serial Number	Patch Size	Number of Slides	Number of Columns	Number of Rows	Total number of Patches	Patches/ slide
1	10	6	102	76	7752	1292
2	25	6	40	30	1200	200
3	50	6	20	15	300	50
4	100	6	10	7	70	11

We can see in the Table 1. that when we keep the number of slides constant but vary the patch size, the value of the other parameters vary.

Table 2. Different parameters obtained when the patch size is kept constant but the number of slides are changed in the Slicing process.

Serial Number	Patch Size	Number of Slides	Number of Columns	Number of Rows	Total number of Patches	Patches/ slide
1	25	2	40	30	1200	600
2	25	4	40	30	1200	300
3	25	5	40	30	1200	240
4	25	6	40	30	1200	200

We can see in Table 2. that when we keep the patch size constant, the number of columns, number of rows and the total number of patches does not change even if we change the number of slides.

Table 3. Different parameters obtained when the Information Size is changed in the Encoding process.

Serial Number	Information Size	Number of Image Pixels	Total LSB	Maximum Characters
1	10	786432	2359296	294912
2	11	786432	2359296	294912
3	4159	786432	2359296	294912

We can see in Table 3. that when the size of the text information is increased, the other parameters namely, number of image pixels, total LSB and maximum characters does not change.

I have tested my proposed framework on a large number of colour images with different size of text. The images ensure the persistency of their quality.

V. CONCLUSION

This system is designed after reviewing the work carried out by various authors on Visual Cryptography and Steganography. Many designers faced with numerous hurdles while designing their systems. PSNR values obtained by them also varied.

The proposed system uses Visual Cryptography and Steganography. I have taken eleven case studies. In these case studies, I have changed the size of the patches, number of slides and the size of the text message. In all these cases I was able to receive the text message faithfully. Thus we can say that although Visual Cryptography and Steganography processes may generate some noise, our system is able to circumvent this drawback. This system works very well for short text messages.

In this dissertation advance study includes complete analysis of Visual Cryptograph and Steganography methods with development of efficient algorithms to reduce the computational cost, add two layers of security and to make the system dynamic. The proposed algorithms are capable of handling Color images and are able to obtain much improved results as compared with other methods. C# .Net has been used to enhance the execution speed.

In the testing environment 11 case studies have been undertaken. The proposed system demonstrated specificity and accuracy of 100%. All the text messages that were sent, was received at the receiver faithfully.

1) Advantages

a) Here color image is used as the cover image. This makes the encryption process more sophisticated and immune to external attacks.

b) The Visual Cryptography process is more dynamic because there are two input fields. The two inputs, which the user is asked for, are: 1) the number of slides and 2) the patch size.

2) Disadvantages

The major drawback of this work is that it can handle only short text data. This is because large text data get distorted after Visual Cryptography.

3) Applications

a) Military Applications
b) Secrete communications

Even though some progress has been achieved, some challenges and directions are still remaining for future research.

VI. FUTURE SCOPE

Visual Cryptography technique is used to protect image-based secret information. In this scheme we have proposed a technique called random sequence to divide an image into n number of shares. The shares are sent through different communication channels from sender to receiver so that the probability of getting sufficient shares by the intruder minimizes.

But the distorted shares may arise suspicion to the hackers mind that some secret information is passed. The original image can be encrypted using a key to provide more security to this scheme. The key may be a text or a small image.

Steganography though is still a fairly new idea. There are constant advancements in the computer field, suggesting advancements in the field of Steganography as well. It is likely that there will soon be more efficient and more advanced techniques for Steganalysis. A hopeful advancement is the improved sensitivity to small messages. Knowing how difficult it is to detect the presence of a fairly large text file within an image, imagine how difficult it is to detect even one or two sentences embedded in an image! It is like finding a microscopic needle in the ultimate haystack. What is scary is that such a small file of only one or two sentences may be all that is needed to commence a terrorist attack. In the future, it is hoped that the technique of steganalysis will advance such that it will become much easier to detect even small messages within an image.

1) Legitimate use of Steganographic techniques

Steganographic techniques have obvious uses, some legitimate, some less so, and some are likely illegal. The business case for protection of property, real and intellectual is

strong. Individuals or organizations may decide to place personal/private/sensitive information in steganographic carriers. With advances in Steganography, it is possible that this medium could serve as a relatively secure storage/transmission method.

2) Illegal use of Steganographic techniques

Other uses for Steganography range from the trivial to the abhorrent. A report on High Technology crime lists eight common types of computer crime:

a) Criminal communication
b) Fraud
c) Hacking
d) Electronic payment
e) Gambling and pornography
f) Harassment
g) Intellectual property offenses
h) Viruses

In examining this list, one can identify several of these areas where Steganography could be used, especially considering the broad term "criminal communications". If one includes steganographic techniques other than computer related, the potential grows even more.

In terms of computer security, there are some areas to be aware of. One area that has potential far ranging implications is "A protocol that uses Steganography to circumvent network level censorship".

Finally, computer warfare should be addressed. The Steganography tools are not conducive to be sole attack weapons. However, the tools combined with other applications could be used to automatically extract the hidden information with minimal user intervention.

References

[1] Jthi P.V. and Anitha T Nair. "Progresive Visual Cryptography 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, Proj Alai Chaudhari and Dr.Monalisha Banerjee, " A secure key based Digital Text Passing System through Colour 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, andDu-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 Steganographic 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.
[12] P.Thiyagarajan, V.Natarajan, G.Aghila, V.Pranna Venkatesan, R.Anitha, (2013) "Pattern Based 3D Image Steganography", 3D Research center, Kwangwoon University and Springer 2013, 3DR Express., pp.1-8.
[13] Shamim Ahmed Laskar and Kattamanchi Hamachandran (2013) "Steganography Based On Random Pixel Selection For Efficient Data Hiding", International Journal of Computer Engineering and Technology, Vol.4,Issue 2.pp 31-44.
[14] S.Shanmuga Priya,K.Mahesh and Dr.K.Kuppusamy, (2012) "Efficient Steganography Method To Implement Selected Least Significant Bits In Spatial Domain", International Journal Of Engineering Research And Applications. Vol2 Issue 3.pp 2632-2637.