A REVIEW ON TWO-LEVEL SECRET MESSAGE ENCLOSURE TECHNIQUE BASED ON IMAGE PROCESSING

Hima.S.Rao[1], Dr. Shilpa Mehta[2]
[2]Professor
Department of ECE, REVA ITM, Bangalore, India

Abstract: This paper combines the features of both steganography and visual cryptography. Though, a number of algorithms have been proposed in the fields of steganography and visual cryptography with the goals of improving security, reliability, and efficiency; because there will be always new kinds of attacks and drawbacks in the field of information hiding. Visual cryptography has the demerit of revealing the occurrence of the hidden data whereas Steganography hides the occurrence of hidden data. So we make use of the advantage of both to overcome their drawbacks. Here, we perform multiple layers of encryption by hiding the hidden data. Hiding, here refers to encrypting the information using visual cryptography and then hide the share/s into images or audio files using steganography. The proposed system is preferred as it can be of less draw backs and can resist towards upcoming attacks.

Keywords: Stenography, Visual Cryptography, Share, Discrete Cosine Transform (DCT).

I. INTRODUCTION

At present scenario, every people use computer networks to share resource and to exchange information. Here for exchange of information they are communicate with each other. The most important factor has been the security of information. There are mainly two type of technique is used to provide security to the information: Cryptography and Steganography, Cryptography is a technique for securing the secrecy of communication. Many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Sometimes it is not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. Steganography is the technique used for implementing this. Steganography is the art and science of invisible communication of messages in such a way that no one can seen the existing of message except sender and receiver and the goal of Steganography is to hide the very presence of communication. This is done by hiding information in other information, i.e. hiding the existence of the communicated information.

II. INTRODUCTION TO STEGANOGRAPHY

The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and Steganography. The World Wars had accelerated the development of Steganography by introducing a new carrier – the electromagnetic waves. Presently, the most popular carriers include digital images, audio and video files and communication protocols. Steganography derives from the Greek word, "Steganos", meaning covered or secret, and "graphy" means writing or drawing. On the simplest level, Steganography is hidden writing, Today, Steganography is most often associated with data hidden with other data in an electronic file. This is usually done by replacing that least important or most redundant bits of data in the original file.

The information to be hided is called the secret message and the medium in which the information is hided is called the cover document. The cover document containing hidden message is called stego-document. The algorithms employed for hiding the message in the cover medium at the sender end and extracting the hidden message from the stego-document at the receiver end is called stego system.

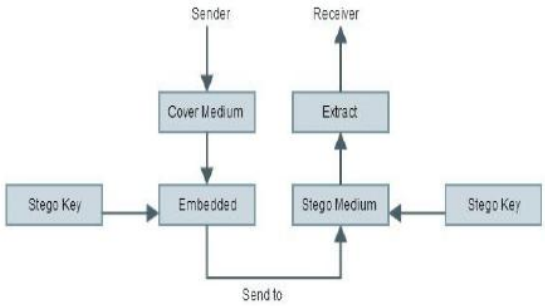


Fig 1: Block Diagram of Steganography Mechanism [6]

Here a secret data is being embedded inside a cover image. So it produces the stego image. A key is also needed in the embedding process. The proper stego key is used by the sender for the embedding procedure. The same key is used by the recipient to extract the stego cover image in order to view the secret data. The stego image should look almost identical to the cover image.

Various application of Steganography Steganography is applicable to the following areas.

1) Confidential communication and secret data storing
2) Protection of data alteration
3) Access control system for digital content distribution
4) Media Database systems

A. Steganography Methods

There are only three ways to hide a digital message in a digital cover: injection, substitution, and generation of new files.

- Injection: Data injection embeds the secret message directly in the host medium. The problem with this kind of embedding is that it usually makes the host file larger, and therefore the alteration is easier to detect.

- Substitution: Normal data is replaced or substituted with the secret data. This usually results in very little size change for the host file. However, depending on the type of host file and the amount of hidden data, the substitution method can degrade the quality of the original host file.
- Generation of New Files: A cover is generated for the sole purpose of concealing a secret message. A sender creates a picture of something innocent that can be passed to receiver; the innocent picture is the cover that provides the mechanism for conveying the message.

III. INTRODUCTION TO CRYPTOGRAPHY

It is about protecting the content of messages. Here we use the new type of cryptography technique- VISUAl CRYPTOGRAPHY.

A. visual cryptography

It is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer. One of the best-known techniques has been credited to MoniNaor and Adi Shamir, who developed it in 1994. 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. Using a similar idea, transparencies can be used to implement a one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text.

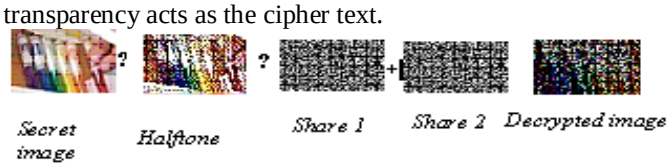


Fig 2: Encryption Using Visual Cryptography

B. How Visual Cryptography Works

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts. If a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel. We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlayed. These pixels have a state that is opposite to the same pixel in layer1. If both images are overlayed, the areas with identical states will look gray, and the areas with opposite states will be black. The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels. If the pixel states of layer 1 are truly (crypto secure) random, both empty and information of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory. If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as the two layers don't fall together in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

Most of the existing secret sharing schemes are generalized within the so-called {k,n}-threshold framework that confidentially divides the content of a secret message into n shares in the way that requires the presence of at least k, for $k \leq n$, shares for the secret message reconstruction, Thus, the framework can use any of $n!/(k!(n-k)!)$ possible combinations of k shares to recover the secret message, whereas the use of $k-1$ or less shares should not reveal the secret message.

IV. LITERATURE SURVEY

[1] “Information Hiding Techniques for Steganography and Digital Watermarking”

Steganography, a means by which two or more parties may communicate using "invisible" or "subliminal" communication, and watermarking, a means of hiding copyright data in images, are becoming necessary components of commercial multimedia applications that are subject to illegal use. This new book is the first comprehensive survey of steganography and watermarking and their application to modern communications and multimedia.

[2] “Computer Graphics, Principles and Practice, Reading”

All code has been converted into C, and changes through the ninth printing of the second edition have been incorporated. The book's many outstanding features continue to ensure its

position as the standard computer graphics text and reference. By uniquely combining current concepts and practical applications in computer graphics, four well-known authors provide here the most comprehensive, authoritative, and up-to-date coverage of the field. The important algorithms in 2D and 3D graphics are detailed for easy implementation, including a close look at the more subtle special cases. There is also a thorough presentation of the mathematical principles of geometric transformations and viewing. In this book, the authors explore multiple perspectives on computer graphics: the user's, the application programmer's, the package implementor's, and the hardware designer's. For example, the issues of user-centered design are expertly addressed in three chapters on interaction techniques, dialogue design, and user interface software. Hardware concerns are examined in a chapter, contributed by Steven Molnar and Henry Fuchs, on advanced architectures for real-time, high performance graphics.

[3] "Software Engineering a Practitioner's Approach",

A Practitioner's Approach has been designed to consolidate and restructure the content introduced over the past two editions of the book. The chapter structure will return to a more linear presentation of software engineering topics with a direct emphasis on the major activities that are part of a generic software process. Content will focus on widely used software engineering methods and will de-emphasize or completely eliminate discussion of secondary methods, tools and techniques. The intent is to provide a more targeted, prescriptive, and focused approach, while attempting to maintain SEPA's reputation as a comprehensive guide to software engineering.

[5] "Digital Image processing"

Digital image processing is the use of computer algorithms to perform image processing on digital images. As a subcategory or field of digital signal processing, digital image processing has many advantages over analog image processing. It allows a much wider range of algorithms to be applied to the input data and can avoid problems such as the build-up of noise and signal distortion during processing. Since images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

[7] "Embedding Robust Labels into Images for Copyright Protection"

This paper describes a set of novel steganographic methods to secretly embed robust labels into image data for identifying image copyright holder and original distributor in digital networked environment. The embedded label is undetectable, unremovable and unalterable. Furthermore it can survive processing which does not seriously reduce the quality of the image, such as lossy image compression, low pass filtering and image format conversions.

V. V.PROBLEM DEFINATION

As, mentioned both steganography and cryptography have pros and corns. Whenever they are using independently we could only have single level of security. That can easily be broken by eavesdroppers. If we could combine the features of both together then we would have two levels of security. That is, in a simple way we can say hiding hidden data, which ensure multi-level of security. So as we suggest blending of both steganography and visual cryptography. The steganography technique used here is DISCRET COSINE TRANSFORM TECHNIQUE [DCT] in literature survey, the most reliable type of steganography technique and the new type of cryptography technique which is VISUAL CRYPTOGRAPHY.

VI. METHODOLOGY USED FOR THE PROPOSED SYSTEM

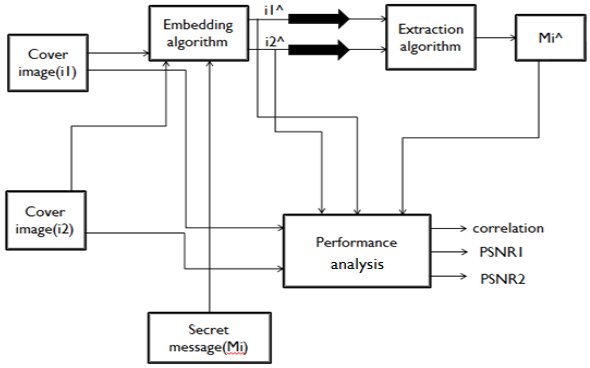


Fig 3: Encryption Using Visual Cryptograph

In our proposed method we use two cover images.

Algorithms

Hiding Process

Input: Cover image, secret image, secret key

Output: embedded images

- Choose Information to be encrypted, say Mi.
- Using the aforementioned algorithm of visual cryptography, divide the content of the message (Mi) into n shares (here we get first level of hiding).
- Each share will be treated as information.
- Shares can be treated as a single image or different.
- If shares are treating as a single image we can hide it together inside a single Image. Else we need different images to different shares.
- Select an appropriate image or images so that the shares of the original message can be embedded in to a single image or each share in different images.
- Instead of sending the n shares immediately it will be embedded into an image or images using any of the steganography technique. (Here we get second level of hiding).
- If we are using different images to store different shares it will be much secure and very difficult to find out the information by the intruders. But need different Images.
- Use DCT-Steg encoding process to encrypt the shares[which comprises the secret data]
- Retrieving Process

Input: Secret key

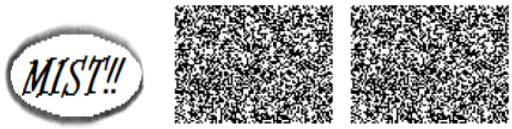
Output: secret image

- Use DCT- Steg decoding process to decrypt the shares from images
- After decoding the message from the cover medium [Here image/images] we will get the n shares of the message. They are in encrypted form. That is encrypted by visual cryptography.
- These n shares can then be decrypted by human visual system, without the aid of computers. We need no computing mechanism to decrypt the message encrypted by visual cryptography. What we only need is to super impose all the n shares on one another so that we will get the original message.

VII. PROPOSED EXPERIMENT AND RESULTS

A. Level 1 hiding using visual cryptography

Figure 4



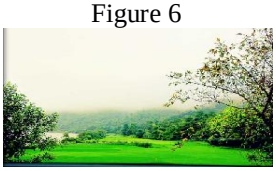
Secret Data Share 1 Share 2

B. Level 2 hiding using steganography

Figure 5

Share 1 Embedded Image

Figure 6



Share 2 Embedded Image

C. Extracted shares from images

Figure 7

Extracted Share 1 Extracted Share 2

D. Super imposing Share1 and Share2 to form the original secret data

Figure 8

The secret information

VIII. CONCLUSION

This project implemented the steganography, visual cryptography and the combination of both in such a way that no one can see that message except the sender and receiver. We introduced about new cover object which is cover images and also presented efficient algorithm for embedding data into this cover images and extracting data from same cover images. It can be implemented bit wise so speed will be faster compare to character wise. It will be implemented on binary file so any file can be encrypted. So we can say that it is the efficient method for Steganography.

IX. FUTURE ENHANCEMENTS

The proposed system is aimed to simplify the complex and redundant process with the flexibility of a simple process. The proposed system is being developed as an attempt to overcome the difficulties of the existing system.

X. ACKNOWLEDGMENT

With the cooperation of my guide, I am highly indebted to Professor. Dr. Shilp Mehta for his valuable guidance and supervision regarding my topic as well as for providing necessary information regarding research work.

REFERENCES

[1] Stefan Katzenbeisser,Fabien A. P. Petitcolas "Information Hiding Techniques for Steganography and Digital Watermarking ".ARTECH HOUSE, INC. 685 Canton Street Norwood.
[2] Foley, J., et al., Computer Graphics, Principles and Practice, Reading, MA: Addison Wesley, 1990
[3] Roger S. Pressman, "Software Engineering a Practitioner's Approach", fifth edition, McGraw-Hill.
[4] William Stalling, "Cryptography and Network Security-Principles and Practices", fourth edition, Pearson Prentice Hall pf India P.Ltd.
[5] Pratt, W. K., Digital Image Processing, New York: Wiley, 1991.
[6] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001 Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999
[7] Jian Zhao, Eckhard Koch: Embedding Robust Labels into Images for Copyright Protection. KnowRight 1995: 242-251

