www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 5 May 2017, Page No. 21523-21527
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i5.55

Secure Data Transfer: Based on Steganography and Visual Cryptography

Rini K[1], *D.Rajapriya*[2]
[1]ME CSE Student, Anna University, RVS Technical Campus,
Coimbatore, Tamil Nadu, India
inoarini@gmail.com
[2]Professor, Computer Science & Engineering Department, RVS Technical Campus,
Coimbatore, Tamil Nadu, India

Abstract: ***Secure data transfer is one of the most important concern with the internet users who are transmitting highly secures information through internet. We have various technologies available to overcome this issue and the main includes the steganographic and visual cryptographic techniques. Using steganography, messages senders can hide their secure data in image, audio or video files. Images are widely used because of its availability as well as there are millions of images are transmitted through internet in each fractions of second, which makes them an excellent cover for secure messages. Steganography got a challenger in the form of steganalysis who can recreate the secure data from the message using various steganalysis techniques. Visual cryptography is another important method which provides 2 way authentication, where the user the needs to get all the shares of the image to complete the required action. In this paper, we have presented a system which uses both the concepts of steganography and visual cryptography to securely transfer data. The secured message is hidden in the image using the steganographic LSB and then the images are partitioned into shares and send separately to the receiver. The receiver needs all the shares to recover the image with hidden message and then the message to be decoded from the image.***

Keywords: Steganography, LSB, Visual Cryptography, One-pad encryption

1. Introduction

In today's technology era, information sharing and secure data transfer has increased with a whooping count. In parallel, the threat of intruders to who uncover the secured data without authorizations also increased. In turn, the need for a secured data transfer becomes inevitable. We have many strong technologies available to secure the data transferred using steganography and visual cryptography. Steganography hides the message in a cover image called stego-image. On the other hand, visual cryptography coverts the image into an unreadable cipher. Both the techniques provide some level of security and individually both have its own drawbacks too. So neither of them alone is secure enough to share information over a communication which is vulnerable to security attacks.

The main objective of the project is to design a secure data transmission system which combines the use of both steganography and visual cryptography with the goals of improving security, reliability, and efficiency for secret message. In this method, two level of security is provided which means first layer of security is accomplished by embedding secret data inside the image using steganographic scheme and second layer of security is accomplished by splitting an input image into two shares, the key and the cipher, using Visual Cryptography scheme.

2. Literature Survey

2.1 Steganography

Steganography is the art of hiding information in a cover medium. The cover medium could be of any kind of digital media like audio, video, images etc. Images are widely used due to its availability and excess use of the same in the internet. Steganography refers to covered writing. The procedure for steganographic technique can be explained as follows:

Cover-Medium + Hidden Data + Steg-key = Stego-Medium

Steganography is mainly used to prevent the detection of secured information from unintended parties. The main aim of steganography is to embed the message into the digital media in such a way that it cannot be destroyed easily. Concealing messages using steganographic methods are been used for a very long period of time. As time goes, techniques are developed by the hackers to extract the message from the stego-medium. The major challenges of effective steganography are:

1. Security of the hidden secured data
2. Embedding capacity the cover medium

The major threat to secure data transmission using steganalysis is the steganalytic attacks. Steganalysis is the art and science of detecting messages hidden using steganography. The goal of steganalysis is to identify suspected packages, determine whether or not they have a payload encoded into them, and, if possible, recover that payload. Different ways of steganalytic attacks are –

1. Visual attacks: The method of detecting the hidden data or the presence of information by visual inspection. This is done either by naked eye or by a computer. The attack is based on guessing the embedded layer of an image, say a bit plane and then visually inspecting that layer to look for any unusual modifications in that layer
2. Statistical attacks: This methods uses first or higher order statistics of the image to reveal tiny alterations in the statistical behaviour caused by steganographic embedding and hence can successfully detect even small amounts of embedding with very high accuracy

A Steganographic Framework:

In gene In general there is no need of using any key for secret communication is "pure" steganography. But now these days there are other variations on these techniques where some of the techniques implement a key. The digital and modern steganography could be implemented on any kind of digital media like text files, image, audio or video.

The working mechanism of any steganographic system can be studies as shown in Figure 1. For a steganographic algorithm having a stego-key, given any cover image the embedding process generates a stego image. The extraction process takes the stego image and using the shared key applies the inverse algorithm to extract hidden image. In the process of image steganography the secret information could be embedded into cover image by using some algorithm. The combined data which holds the secret information called stego image, transfer to the communication channel whereas this stego image transmitted to the receiver and receiver extract the secret information from the stego image.

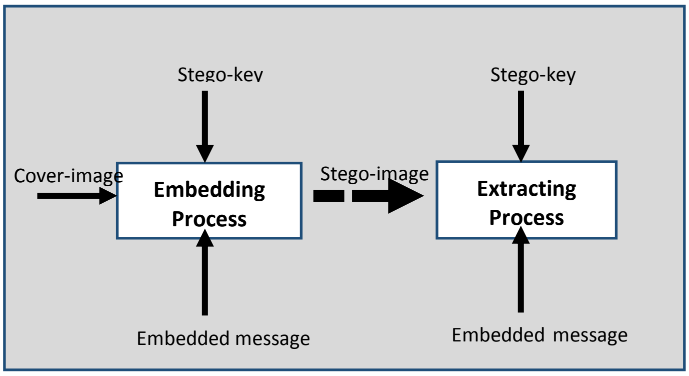


Figure 1: Generalized steganographic framework

2.2 Visual Cryptography

Visual Cryptography is an encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994. Visual Cryptography uses two transparent images. One image contains random pixels and the other image contains the secret information. It is not possible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation we can observe that the two layers sliding over each other until they are correctly aligned and the hidden information appears to the receiver.

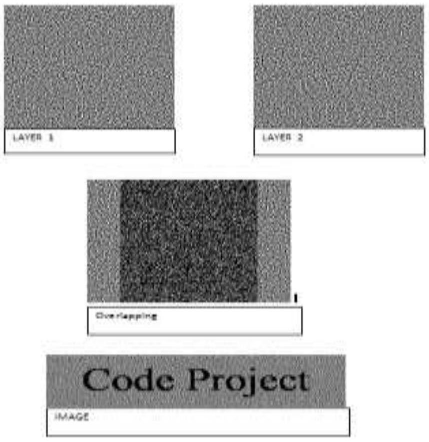


Figure 2: Visual Cryptography

Visual Cryptography Working:

In visual cryptography concept, each pixel of the images is divided into smaller blocks. There are always the equal number of white (transparent) and black blocks. If a pixel is divided into two parts, then one to be white block and the other one a black block. If the pixel is divided into four equal parts, then there are two white and two black blocks. Below figure shows that a pixel is divided into four parts and as shown it 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 overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

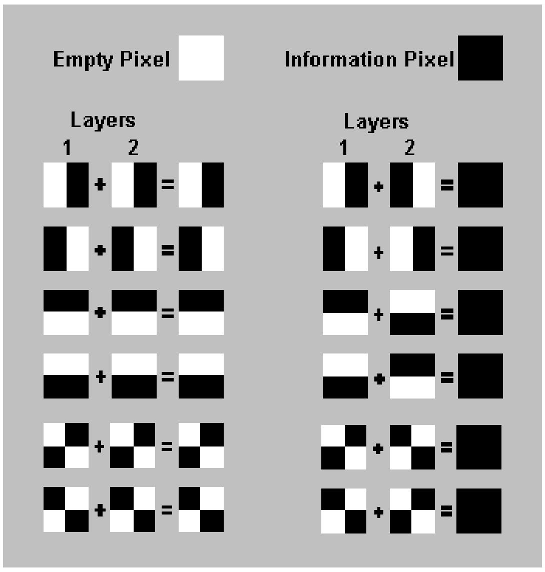


Figure 3: Pixel Partition

Now the two layers are created. 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 overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gravy, 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

DOI: 10.18535/ijecs/v6i5.55

blocks. However, we can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter how the pixel is divided, it can be divided horizontally or vertically. There are many different pixel systems, like pixels with better contrast, pixels with higher resolution or even with color pixels. If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels 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 it 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. On using Visual Cryptography for secure communications, the sender will distribute one or more random layers, say layer 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 both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

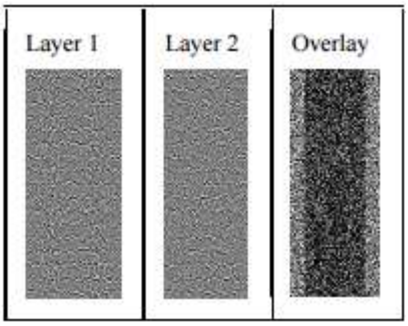


Figure 4: Layers Overlay

One time pad encryption

The mechanism of the one-time pad is very simple: XOR every plaintext bit with the corresponding random key bit to yield a cipher text bit: c = p k. To decrypt, XOR the cipher text with the key once more: d = c k. The two keys will cancel out and you’ll get the plaintext. d = c k = p (k k) = p 0 = p.

The one time pad is the only demonstrably secure cipher, in the sense that even an infinite amount of cipher text will not leak any bits of information to the attacker about the plaintext (except the length). This is because, given a cipher text, you can choose any plaintext you want and there will always exist a key that generates that cipher text from that plaintext

Simple Algorithm XOR

There is a simple algorithm for visual cryptography that creates 2 encrypted images from an original unencrypted image. The algorithm is as follows:

1. Create an image of random pixels the same size and shape as the original image.

   {random1}

2. Create a second image whose pixels are the exclusive-or (XOR) of the first image and the original image.

   {random2=random1 XOR original}

3. The two apparently random images can now be combined with XOR to recreate the image.

   {random1 XOR random2 = random1 XOR (random1 XOR original) = original}

The process performed has the following steps:

1. Convert the source image to pure black and white, without any gravy-scale.
2. Generate a random key of black and white pixels, of exactly the same size as the original image.
3. Based on the pixels in the original and key images, create a cipher image.
4. Expand the cipher and key images to 4 times the size (each pixel becomes a 2x2 grid of pixels).
5. Compare each 2x2 grid of pixels in the expanded key and expanded cipher images, based on the comparison, create either a black or white pixel in the decrypted image.
6. The resulting decrypted image should be an exact copy of the original black and white image.

3. Implementation

The Secure data hiding system requires any type of image file and the information or message that is to be hidden. Two main modules of the system are – encryption and decryption. Encryption happens on the sender side and decryption done at the receiver side. The proposed system works in the following phases.

SENDER SIDE:

- Encryption Phase – The data to be encrypted is first read from the user through the keyboard and the secret message is encoded into the least significant bits of the image to create stego image.
- Pixel Modification Phase – Coverts the stego-image to pure black and white without any grey scale. Then a random key of black and white pixels of exactly the same size as the original image created. Based on the pixels in original and key images, a cipher image is created. This key image and cipher image is transmitted to the receiver.

RECEIVER SIDE:

- Overlapping Phase – Receiver needs to upload the two shares of the image. The stego-image is recreated at the receiver side using the key image and the cipher image.
- Decryption phase – The data hidden in the stego-image is extracted and displayed to the user.

Secure Data Hiding system requires any type of image file and the information or message that is to be hidden. User needs to run the application. The user has two options – encrypt and decrypt. If user select encrypt, application displays the screen Create Encrypted Images to select image file or information file. Application also gives the option to save the modified image file. Click on Encrypt to create the random key image and a cipher image created using the original image and random key image. If user select decrypt, application gives the screen to upload the two images shares – Key image and

Cipher image. After uploading click on Decrypt button to extract the original image or the message.

Encryption Process: The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (8st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step we go to upper layer image quality decreases and image retouching transpires. This module requires any type of image and message and gives the only one image file in destination. The stego-image created is treated with a random generated key image of black and white pixels to create a cipher image.

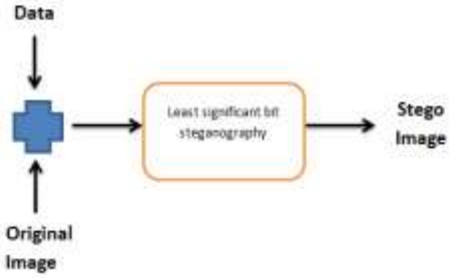


Figure 5: Encoding the text into the image

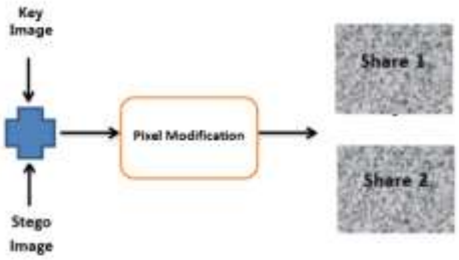


Figure 6: Creating Shares of Stego-image

Decryption Process: The decrypt module is used to get the hidden information in an image file. It take the two shares generated from the encryption phase as input, and overlays these two shares to generate stego-image. The stego-image generated in the above process is then decode to retrieve the message stored in the least significant bits. The reverse of the LSB encoding is performed here.

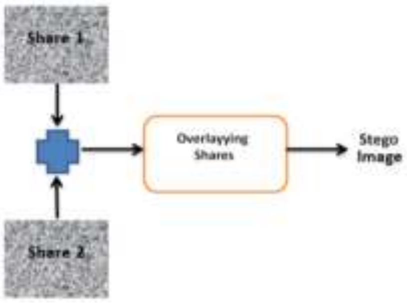


Figure 7: Overlaying Shares

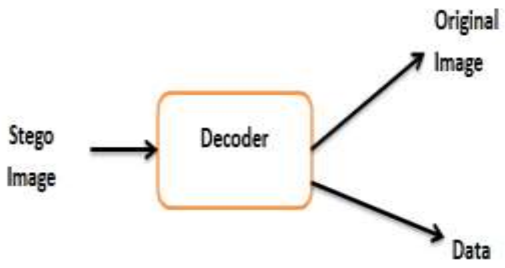


Figure 8: Decoding the message

4. Experimental Results

The secured message "Secure message transaction" to hidden in an images and then the shares of the image are created in the sender side. The image used for hiding the text is as below,

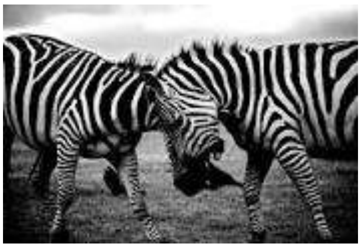


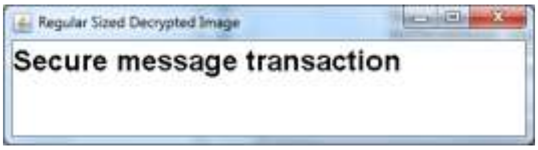
Figure 9: Cover image

Using secure data hiding system, the message gets encoded in the cover image and creates a stego-image. Which in turn is taken through visual cryptographic techniques to generate two shares – Key Image and Cipher Image as in the below figures,

Figure 10: Key Image

Figure 11: Cipher Image

In the receiver side, the system is used to recover the message. Here the user needs to upload both the shares of the stego-image created during the encryption. Application overlays both the shares to generate the stego image and extract the original message from the stego-image.


Regular Sized Decrypted Image

Secure message transaction

Figure 12: Decrypted Image

DOI: 10.18535/ijecs/v6i5.55

5. Conclusion and 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 Steganography application which are vulnerable to RS attacks. The software provided can be used with any type of image formats to hiding secret messages inside them. The master work of this application is in supporting any type of pictures without need to convert to bitmap, and lower limitation on file size to hide, because of using maximum memory space in pictures to hide the file. Application of visual cryptographic techniques to the stego image created enhance the protection level of the secret message. It provides two levels of security to the information being transmitted. That is the intruders cannot easily break the system. Even if they realize the existence of a secret data they cannot easily recognize the data, since data is hidden in two ways. This system overcomes the demerits of using single level of hiding and that too it requires

The technique of steganography using visual cryptography in images has its scope on transmission of data in highly secured manner through audio streams and video streams. This is accomplished by encoding the audio data using steganography and cryptography technique in the audio streams and adopting the same technique to send the data in audio format, text format or image format in video streams. The technique in audio streams and images is best utilized in sending the data in video streams

References

[1] Secure Information Hiding System Using LSB with Sequence Mapping Technique – A. Vasavi, K. Muralidhar Reddy, Y. Madhusudhana Reddy, J. Leela Mahendra Kumar

[2] International Journal on Recent and Innovation Trends in Computing and Communication

[3] N. F. Johnson, and S. Jajodia, “Steganography: Seeing the Unseen”, IEEE Computer, Feb. 1998

[4] Natarajan Meghanathan and Lopamudra Nayak,Steganalysis Algorithms for Detecting the Hidden Information in Image, Audio and Video Cover Media, Jackson State University, 1400 Lynch St., Jackson, USA

[5] Eric Cole, Hiding in Plain Text, Wiley Publishing,Inc. :2003

[6] V. K. Pachghare, Cryptography and Information Security, Prentice-hall Of India Pvt Ltd

[7] Luis von Ahn and Nicholas, Steganography, Carnegie Mellon University, Pittsburgh, USA

[8] Archana B.Dhole and Prof. Nitin J. Janwe. ”An Implementation of Algorithms in Visual Cryptography in Images”. International Journal of Scientific and Research Publications, Volume 3, Issue 3, March 2013 1 ISSN 2250-3153.

[9] Kulvinder Kaur and Vineeta Khemchandani. ”Securing Visual Cryptographic Shares using Public Key Encryption”.2013 3rd IEEE International Advance Computing Conference (IACC).

[10] A. Parakh and S.kak.”A Recursive Threshold Visual Cryptography Scheme”. Department of Computer Science, Oklahoma State University Stillwater, OK 74078.

[11] D. Jena and S. Jena. ”A Novel Visual Cryptography Scheme”. 978- 07695-3516-6/08 2008 IEEE DOI 10.1109/ICACC.2009.109.

[12] P. S. Revenkar, Anisa Anjum and W. Z. Gandhare. ”Survey of Visual Cryptographic Schemes”. International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.

[13] Ujjwal Chakraborty et al.”Design and Implementation of a (2, 2) and a (2,3) Visual Cryptographic Scheme” .International Conference [ACCTA-2010], Vol.1 Issue 2, 3, 4, PP 128-134.

Author Profile

Rini Kallivalappil received the B.Tech. degree in Computer Science & Engineering from Calicut University in 2006 and pursuing M.E. degree in Computer Science & Engineering from RVS Technical Campus, Coimbatore in 2017. She also had an IT experience of 7+ years in a reputed software company.