MULTI LAYER INFORMATION HIDING -A BLEND OF STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

[1]JITHESH K , [2]Dr. A V SENTHIL KUMAR .

[1]Asstt Prof., Department of Computer Science, Mahatma Gandhi College, Iritty, Kerala, India-670703
[2]Lecturer, Department of Computer Science, Hindustan College of Science & Commerce, Coimbatore-641006, Tamil Nadu.

ABSTRACT

This study combines the notion of both steganography [1] and visual cryptography [2]. Recently, a number of innovative 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 threats in the field of information hiding. Actually Steganography and visual cryptography are two sides of a coin. Visual cryptography has the problem of revealing the existence of the hidden data where as Steganography hides the existence of hidden data. Here this study is to suggest multiple layers of encryption by hiding the hidden data. Hiding the hidden data means, first encrypting the information using visual cryptography and then hide the share/s[3] into images or audio files using steganography. The proposed system can be less of draw backs and can resist towards attacks.

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

1. INTRODUCTION TO STEGANOGRAPHY

An important sub division of information hiding is steganography [1]**.** While cryptography [4] is about protecting the content of messages, steganography is about concealing their very existence. This modern adaptation of *steganographia* (Trithemius, 1462–1516), assumed from Greek, literally means "covered writing" and is usually interpreted to mean hiding information in other information.

1.1 Steganography Methods[1]

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.

1.2 Techniques of Steganography

In all methods of steganography, something is done to conceal a message; naturally, these actions or techniques can be separated and analyzed to learn what is happening during the whole process. The six categories of steganography are:

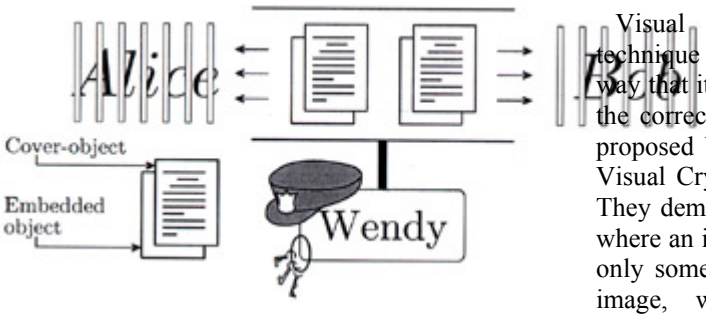
1. Substitution system techniques
2. Transform domain techniques
3. Spread spectrum techniques

4. Statistical method techniques
5. Distortion techniques
6. Cover generation techniques

1.3 Principles of Steganography

The "classic" model for invisible communication was first proposed by Simmons as the "prisoners' problem"[1]. Alice and Bob are arrested for some crime and are thrown in two different cells. They want to develop an escape plan, but unfortunately all communications between each other are arbitrated by a warden named Wendy. She will not let them communicate through encryption and if she notices any suspicious communication, she will place them in solitary confinement and thus suppress the exchange of all messages. So both parties must communicate invisibly in order not to arouse Wendy's suspicion; they have to set up a subliminal channel. A practical way to do so is to hide meaningful information in some harmless message: Bob could, for instance, create a picture of a blue cow lying on a green meadow and send this piece of modern art to Alice. Wendy has no idea that the colors of the objects in the picture transmit information.

Figure-1



The prisoners' problem, illustrated.

Unfortunately there are other problems which may hinder the escape of Alice and Bob. Wendy may alter the message Bob has sent to Alice. For example, she could change the color of Bob's cow to red, and so destroy the information; she then acts as an active warden. Even worse, if she acts in a malicious way, she could forge messages and send a message to one of the prisoners through the subliminal channel while pretending to be the other. The above model is generally applicable to many situations in which invisible communication—steganography—takes place. Alice and Bob represent two communication parties, wanting to exchange secret information invisibly. The warden Wendy represents an eavesdropper who is able to read and probably alter messages sent between the communication partners cryptographic techniques try to conceal the contents of a message, steganography goes yet a bit further: it tries to hide the fact that a communication even exists. Two people can communicate covertly by exchanging unclassified messages containing confidential information. Both parties have to take the presence of a passive, active or even malicious attacker into account.

2. VISUAL CRYPTOGRAPHY [9][10]

There are many powerful secret-sharing schemes that enable you to encode a document or file so that nobody can decipher the real contents of the encoded document without access to the encrypted shares and a computer to perform the calculations necessary to decrypt the secret document. Visual Cryptography is a secret-sharing method that encrypts a secret image into several shares but requires neither computer nor calculations to decrypt the secret image. Instead, the secret image is reconstructed visually: simply by overlaying the encrypted shares the secret image becomes clearly visible.

Visual Cryptography is a special 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 Moni Naor and Adi Shamir in 1994. Visual Cryptography uses two transparent images. 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. One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Both transparent images and layers are required to reveal the information.

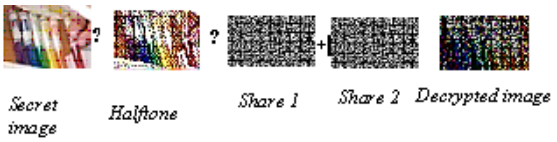
The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a One-time Pad system and will offer unbreakable encryption. In the overlay animation you can observe the two

layers sliding over each other until they are correctly aligned and the hidden information appears.Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

Visual cryptography is a popular solution for image encryption. Using secret sharing concepts, the encryption procedure encrypts a secret image into the so-called shares which are noise-like secure images which can be transmitted or distributed over an unreliable communication channel. Using the properties of the human visual system to force the recognition of a secret message from overlapping shares, the secret image is decrypted without additional computations and any knowledge of cryptography. Visual cryptographic solutions operate on binary or binarized inputs. Therefore, natural (continuous-tone) images must be first converted into halftone images by using the density of the net dots to simulate the original gray or color levels in the target binary representation. Then, the halftone version of the input image is used instead of the original secret image to produce the shares. The decrypted image is obtained by stacking the shares together. Because binary data can be displayed either as frosted or transparent when printed on transparencies or viewed on the screen, overlapping shares that contain seemingly random information can reveal the secret image without additional computations or any knowledge of cryptographic keys. However, due to the nature of the algorithm, the decrypted image is darker, contains a number of visual impairments, and most of visual cryptography solutions increase the spatial resolution of the secret image. In addition, the requirement for inputs of the binary or dithered nature only limits the applicability of visual cryptography.

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.

Figure-2



Encryption using visual cryptography

2.1 How Visual Cryptography Works

Each pixel [5] 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 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 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.

3. METHODOLOGY USED FOR THE PROPOSED SYSTEM

For this study the existing methods are analyzed. A few techniques are there to implement both steganography and visual cryptography. Among them an optimal one can be find out by analyzing and verifying the existing tools, which are implemented using the known techniques. Each one has got there own pros and corns. Using the existing methods of both steganography and visual cryptography a novel algorithm is suggested in this paper. That is, as aforementioned, combining both steganography and visual cryptography. It can be made better match for sending hidden information.

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 [9] 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] [8] [14], the most reliable type of steganography technique and the new type of cryptography technique which is VISUAL CRYPTOGRAPHY. The main advantage of DCT is, it is very robust. Similarly, the merit in the case of visual cryptography is, we need no computation to decrypt the encrypted data. It can be well perceived through human visual system (HVS). What we need is only the required number of shares of the original information which is divided into number of shares when encrypted.

Previously the methodology used for encrypting information is either cryptography or steganography. But here we used both. The algorithm is as follows. First the information which is going to be transmitted is encrypted using visual cryptography. So there we achieve first level of security. Then this crypt is embedded into natural or artificial image/images, which is steganography. That gives second level of security.

4. STEGANOGRAPHY ALGORITHMS

A number of steganographic algorithms are available but only one of them adopted in this study are explained in detail below

4.1 Steganography in the DCT Domain [1]

One popular method of encoding secret information in the frequency domain is modulating the relative size of two (or more) DCT coefficients within one image block. We will describe a system which uses digital images as covers and which is similar to a technique proposed by Zhao and Koch.[10]

Algorithm 1. DCT-Steg encoding process

for $i = 1, \ldots, \ell(M)$ **do**
choose one cover-block b_i
$B_i = D\ \{b_i\}$
if $m_i = 0$ **then**
if $B_i(u1, v1) > B_i(u2, v2)$ **then**
swap $B_i(u1, v1)$ and $B_i(u2, v2)$
end if
else
if $B_i(u1, v1) < B_i(u2, v2)$ **then**
swap $B_i(u1, v1)$ and $B_i(u2, v2)$
end if
end if
adjust both values so that $|B_i(u1, v1) - B_i(u2, v2)| > x$
$b'_i = D^{-1}\{B_i\}$
end for
create stego-image out of all b'_i

During the encoding process, the sender splits the cover-image in 8x8 pixel blocks; each block encodes exactly one secret message bit. The

embedding process starts with selecting a pseudorandom block b_i which will be used to code the ith message bit. Let $B_i = D\{b_i\}$ be the DCT-transformed image block.

Before the communication starts, both sender and receiver have to agree on the location of two DCT coefficients, which will be used in the embedding process; let us denote these two indices by (u_1, v_1) and (u_2, v_2). The two coefficients should correspond to cosine functions with middle frequencies; this ensures that the information is stored in significant parts of the signal (hence the embedded information will not be completely damaged by JPEG compression). Furthermore, we can assume that the embedding process will not degenerate the cover heavily, because it is widely believed that DCT coefficients of middle frequencies have similar magnitudes. Since the constructed system should be robust against JPEG compression, we choose the DCT coefficients in such a way that the quantization values associated with them in the JPEG compression algorithm are equal.

One block encodes a "1," if $B_i(u_1, v_1) > B_i(u_2, u^2)$, otherwise a "0." In the encoding step, the two coefficients are swapped if their relative size does not match with the bit to be encoded. Since the JPEG compression can (in the quantization step) affect the relative sizes of the coefficients, the algorithm ensures that $|B_i(u_1,v_1) - B_i(u_2,v_2)| > x$ for some $x > 0$, by adding random values to both coefficients. The higher x is, the more robust the algorithm will be against JPEG compression, however, at the expense of image quality. The sender then performs an inverse DCT to map the coefficients back into the space domain. To decode the picture, all available blocks are DCT-transformed. By comparing the two coefficients of every block, the information can be restored. Embedding and extraction algorithms are outlined later .

Algorithm 2. DCT-Steg decoding process

for $i = 1, \ldots, \ell(M)$ **do**
get cover-block b_i associated with bit i
$B_i = D\{b_i\}$
if $B_i(u1, v1) \leq B_i(u2, v2)$ then
$m_i = 0$
else
$m_i = 1$
end if
end for

If the constant x and the location of the used DCT coefficients are chosen properly, the embedding process will not degenerate the cover visibly. We call expect this method to be robust against JPEG compression, since in the quantization process both coefficients are divided by the same quantization values. Their relative size will therefore only be affected in the rounding step.

Perhaps the most important drawback of the system presented above is the fact that Algorithm 1 does not discard image blocks where the desired relation of the DCT coefficients cannot be enforced without severely damaging the image data contained in this specific block.

Zhao and Koch proposed a similar system which does not suffer from this drawback. They operate on quantized DCT coefficients and use the relations of three coefficients in a block to store the information. The sender DCT transforms the image block b_i and performs a quantization step to get B^Q_i. One block encodes a "1," if $B^Q_i(u1, v1) > B^Q_i(u3, v3) + D$ and $B^Q_i(u2, v2) > B^Q_i(u3, v3) + D$. On the other hand, a "0" is encoded, if $B^Q_i(u1, v1) + D < B^Q_i(u3, v3)$ and $B^Q_i(u2, v2) + D < B^Q_i(u3, v3)$. The parameter D accounts for the minimum distance between two coefficients for representing an embedded bit; normally $D = 1$. The higher D is, the more robust the method will be against image processing techniques. Again, the three selected coefficients should be situated in the middle of the spectrum.

In the encoding step, the relations between these three coefficients are changed so that they represent one bit of the secret information. If the modifications required to code one secret bit are too large, then the block is not used for information transfer and marked as "invalid." This is the case, if the difference between the largest and the smallest coefficient is greater than some constant value MD. The higher MD is, the more blocks can be used for communication. In order to allow a correct decoding, the quantized DCT coefficients of an invalid block are changed so that they fulfill one of the two conditions

$B^Q_i(u_1,v_1) <= B^Q_i(u_3,v_3) <= B^Q_i(u_2,v_2)$
$B^Q_i(u_2,v_2) <= B^Q_i(u_3,v_3) <= B^Q_i(u_1,v_1)$

Afterwards the block is dequantized and the inverse DCT is applied.

The receiver can restore the information by applying DCT and quantizing the block. If the three selected coefficients fulfill one of the conditions, the block is ignored. Otherwise the encoded information can be restored by comparing $B^{Q}_{i}(u1, v1)$, $B^{Q}_{i}(u2, v2)$, and $B^{Q}_{i}(u3, v3)$. The authors claim that this embedding method is robust against JPEG compression (with quality factors as low as 50%), since all changes are made after the "lossy" quantization step.

5. VISUALCRYPTOGRAPHY ALGORITHMS

5.1 Construction Algorithm for a *(2, 2)*-Threshold Scheme

General Requirement

- Construct two 2*x*2 basis matrices as:

$$S^0 = \begin{matrix} 1\ 0 \\ 0\ 1 \end{matrix}, \qquad S^1 = \begin{matrix} 1\ 0 \\ 1\ 0 \end{matrix}$$

- Using the permutated basis matrices, each pixel from the secret image will be encoded into two subpixels on each participant's share. A black pixel on the secret image will be encoded on the i^{th} participant's share as the i^{th} row of matrix S^1, where a 1 represents a black subpixel and a 0 represents a white subpixel. Similarly, a white pixel on the secret image will be encoded on the i^{th} participant's share as the i^{th} row of matrix S^0.
- Before encoding each pixel from the secret image onto each share, randomly permute the columns of the basis matrices S^0 and S^1.
- This VCS (Visual Cryptography Scheme) divides each pixel in the secret image into m=2 subpixels.
- It has a contrast of $\alpha(m)\cdot m$=1 and a relative contrast of $\alpha(m)$=1/2.

5.3 Construction Algorithm for a *(k, n)*-Threshold Scheme

General Requirement

- Let $n_0 = k \cdot \left\lceil \frac{n}{k} \right\rceil$.
- Construct a **initial matrix** IM on ground set A = {1,2,…,k} such that the columns of IM are all of the distinct n-tuples that contain each element of A exactly n_0/k times.
- Construct a (k, k)-threshold VCS with basis matrices T^0 and T^1.
- Build basis matrices R^0 and R^1 by replacing each element i ($1 \le i \le k$) in IM with the i^{th} row of T^0 and T^1, respectively.
- Build basis matrices S^0 and S^1 by restricting R^0 and R^1, respectively, to their first n rows.
- This construction generates a VCS with relative contrast $\alpha(m) = (n_0/k)^k/(2^{k-1}(n_0 \text{ nCr } k)$.

6. ALGORITHM FOR THE PROPOSED SYSTEM

6.1 Encoding Process

- 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]

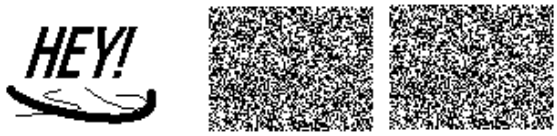
6.2 Decoding Process

- 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.

7. EXPERIMENTAL RESULT

7.1 Level 1 hiding using Visual Cryptography

Figure 3



Secret Data share 1 share 2

7.2 Level 2 Hiding using steganography

Figure-4

Share 1Embedded Image

Figure-5

Share 2 Embedded Image

7.3 Extracted Shares from Images

Figure-6

7.4 Super Imposing Share1 and Share2 to Form the Original Secret Data

The secret Information

8. CONCLUSION AND FURTHER DEVELOPMENT

This project implemented the steganography, visual cryptography and the combination of both. This project allows the authorized users to work. The algorithm developed can be used depending on the situation and application.

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.

The following are the merits of the proposed system.

- ❖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. That is either using cryptography or steganography.
- ❖And one more thing to add is it requires only the computation time of single level hiding, because visual cryptography requires no computation to decrypt the information.

The implemented algorithm can be used in the following areas

- ❖ In military and navy to make their communication secure
- ❖ In payment gate way.
- ❖ In medical production system for secret products
- ❖ In business dealing and settlement contracts
- ❖ In electronic mail communication

9. SCOPE FOR FURTHER DEVELOPMENT

The proposed algorithm can be implemented in the following area of applications.

- ❖ Pictorial database
- ❖ Photo image
- ❖ Video image
- ❖ Audios
- ❖ Email server message

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]. C.C. Chang, M.H. Lin, and Y.C. Hu, "A fast and secure image hiding scheme based on LSB substitution," International J. of Pattern Recognition and Artificial Intelligence, vol.16, no.4, pp.399–416, 2002.

[7].c _ British Computer Society 2003 Hiding Information in Image Mosaics CARLO BLUNDO AND CLEMENTE GALDI1 Department of Information and Applications, Cryptography and Network Security Group, University of the Salerno, 84081 Baronissi (SA), Italy

[8].A Public-key image steganography using discrete cosine transform and quadtree partition vector quantization coding.

a.Opt. Eng., Vol. 42, 2886 (2003).

[9].Evaluation of image based steganography methods using visual inspection and automated detection techniques Karen Bailey & Kevin Curran Published online: 1 June 2006 # Springer Science + Business Media, LLC 2006.

[10]. Tanaka, K., Y. Nakamura, and K. Matsui, Embedding Secret Information Into a Dithered Multilevel Image, in Proceedings of the 1990 IEEE Military Communications Conference, 1990, pp. 216–220.

[11]. Jian Zhao, Eckhard Koch: Embedding Robust Labels into Images for Copyright Protection. KnowRight 1995: 242-251

[12]. www.slideshare.net

[13]. www.leemon.com

[14]. www.google.com

[15]. www.ccse.kfupm.edu.sa