International Journal of Information and Communication Technology Research

http://www.esjournals.org

Analysis & Design of Visual Cryptography Using Moving Image

[1]Gajanand Sharma, [2]Amit Gupta, [3]Dinesh Goyal
[1]SBCET. RTU
[2]SBCET, Jaipur
[3]Suresh Gyan Vihar University

ABSTRACT

Cryptography, Steganography, Watermarking and many other techniques have evolved over a period of time, at the same time attacks on them have also increased as the data is in nuclear form (even though encoded), in these techniques. In last decade Visual Cryptography has evolved as an entity which divides the data into different shares and then embedding is done. This technique increases the overhead of multiple security and multiple output cover objects. In this paper we true to reduce this over head up to some extent by using GIF as cover image and reduce communication overhead.

Keywords: *GIF, Visual Cryptography, LSB.*

1. INTRODUCTION

As the rise of the web one amongst the foremost vital factors of knowledge technology and communication has been the safety of knowledge. Cryptography was created as ways for ensuring the secrecy of message and varied completely different ways are developed encode and decipher knowledge s o as to keep the message secret.

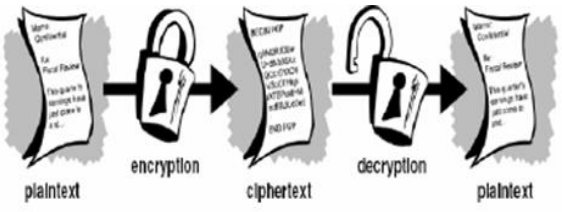


Fig 1 shows the operating of cryptography

2. VISUAL CRYPTOGRAPHY

Visual cryptography is a cryptographic process which enables visual information (pictures, text, etc.) to be protected in such a way that the decryption could be done by individuals (without computers). The first visual cryptographic process was manufactured by Moni Naor and Adi Shamir in 1994[12]. It involved breaking up the picture in to n shares so that only somebody with all n shares could decrypt the picture by overlaying all the shares around each other. Practically, that can be achieved by printing each reveal on another visibility and then placing every one of the transparencies on top of each other. Inside their technique n-1 shares shows no information about the first image.

Simple visual cryptography is based on breaking of pixels in to some subscription pixels or we are able to state expansion of pixels. In this kind of scenario first strategy reveals that all pixel are divided in to two subscription pixels. Let N reveals dark pixel and T reveals Clear (White) pixel. Each reveal will be studied in to different transparencies. When we position both transparencies on top of one another we get following combinations, for dark pixel BT+TB=BB or TB+BT=BB and for bright pixel BT+BT=BT or TB+TB=TB. Equally second strategy is to be provided where each pixel is divided in to four subscription pixels. We are able to obtain 4C2 =6 different instances with this approach.

2.1 Working of Visual Cryptography

Visual cryptography method permits the visual information to be encrypted in such a way that their decryption can be performed by human visual system. This approach used to encrypt a image into shares such that stacking a adequate quantity of shares shows the secret images. In visual cryptography there are different approach like sub pixel, mistake diffusion, Boolean function and so forth.

Visual Cryptography offers information safety using easy algorithm. This approach permits visual information to be encrypted with a couple cryptographic schemes and their decryption can be performed by the human visual systems without any complex cryptographic algorithms. It encrypts the secret image into shares and the stacking of adequate quantity of shares shows the initial image. Shares are usually displayed in transparencies.

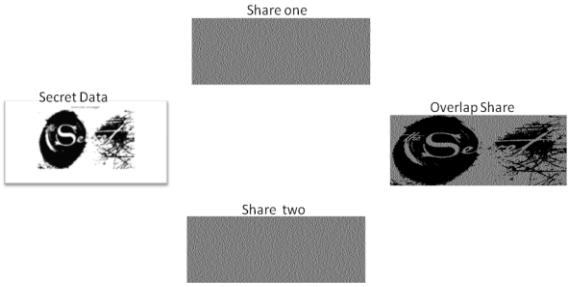


Figure 2 Working of Visual Cryptography

Visual cryptography was first introduced by Naor and Shamir in 1994. In their paper, they deal with the idea of visual cryptography for threshold structures. They assume that the image is composed of black and white pixels, and each pixel is encrypted separately. Each pixel of the image appears in the *n* shares distributed to the participants. It is divided into m subpixels, either black or white, which are sufficiently small and close that the eye averages them to some shade of grey. We can represent this with an $n \times m$ matrix: $S[i, j] = 1$ if and only if the j sub pixels in the ith share is black. When the shares are combined, the perceived grey level is proportional to the number of ones in the boolean OR of the *m*-vectors representing the shares of each participant. The black and white areas of the image are determined by a rule of contrast based on three variables: a threshold value, a relative difference, and the number of subpixels (referred to as the pixel expansion).

The Color Visual Cryptography is a visual sharing process, wherever the original color picture is converted in to three color components red, natural and blue. These three components become halftone images and when overlapping these gives, three color components, which show meaningful visual information.

A visual cryptography scheme may then be built by finding gives in the next fashion: - If the pixel of the original binary picture is bright, randomly pick exactly the same structure 0 down our pixels for both shares. It's substantial to select the designs randomly to be able to produce the structure random. If the pixel of the original picture is dark, select a complementary set of designs, i.e., the designs from exactly the same column.

3. LSB – LEAST SUBSTANTIAL BIT HIDING (IMAGE HIDING)

This approach is probably the best means of hiding information in a graphic and however it is remarkably effective. It operates using the least substantial pieces of every pixel in one single picture to hide the absolute most substantial components of another.

So in a JPEG picture as an example, the following measures would have to be used:

1. First stock up both the sponsor picture and the picture we need to hide.
2. Next chose the number of pieces we wish to hide the trick picture in. The more pieces used in the sponsor picture, the more it deteriorates. Increasing the number of pieces applied however demonstrably features a valuable reaction on the trick picture raising its clarity.
3. We now have to produce a new picture by mixing the pixels from equally images. If we decide for example, to use 4 pieces to hide the trick picture, you will have four pieces remaining for the sponsor image. (PGM - one byte per pixel, JPEG - one byte each for red, green, orange and one byte for leader route in some picture types)

Host Pixel: 10110001
Secret Pixel: 00111111
New Image Pixel: **10110011**

To get the original image back we just need to know how many bits were used to store the secret image. We then scan through the host image, pick out the least significant bits according the number used and then use them to create a new image with one change - the bits extracted now become the most significant bits.

Host Pixel: 10110011
Bits used: 4
New Image: **00110000**

This method works well when both the host and secret images are given equal priority. When one has significantly more room than another, quality is sacrificed. All we need to do is change how the least significant bits are filled in the host image. However this technique makes it very easy to find and remove the hidden data.

4. PROPOSED SECURE DATA SPLITTING AND EMBEDDING ALGORITHMS

Least-significant-bit (LSB) substitution is a technique used to embed secret data in least significant bits of pixels in a host image. The LSB approaches typically achieve high capacity. A simple LSB substitution, which hides secret data directly into LSBs, is easily implemented but will result in bad quality of the Embed-image. In order to reduce the degradation of the host image after embedding, We have proposed an LSB substitution method.

In proposed method we split the secure data into two-three shares by applying Visual Cryptography and then use two-three different frames of a moving image (gif) for embedding secret data in it. I have used the last three bits (LSB) of cover image to insert this share.

The information hiding includes both information embedding algorithms and information extraction algorithms. Embedding is an information hiding process, while extraction is the restoration process of secret information. Therefore extraction operation is the inverse operation of embedding operation.

The following algorithms are used for visual cryptography. Proposed watermarking scheme is defined as 7-tuple (S, S1, S2, C1, C2, E1 and E2):

1. **'S' denotes the Secret image (which has to be protected).**
2. **'S1' and 'S2'denotes the two different Secret shares of Secret Data.**
3. **'C1' and 'C2'denotes the two frames of moving image for watermarking.**
4. **'E1' and 'E2' denotes the two embedded frames generated from Embedding Algorithm.**

Split Secure Data Algorithm:

Step 1: Read Input Secure Data 'S' and Convert it into 256*256
Step 2: Convert Secure Data 'S' RGB into Binary Image.
Step 3: Initialize Two different Shares with Pixel values Zero
Step 4: Find Pixel value one in S and Store required values in Share 'S1'.
Step 5: Find Pixel value zero in S and Store required values in Share 'S2'.
Step 6: Overlap S1 and S2 (For checking Visual Cryptography).

Embedding Algorithm:

Step 1: Read Two frames of cover image 'C1' and 'C2' and Convert into Gray.
Step 2: Check That Shares 'S1' and 'S2' are not large for Cover frames 'C1'and 'C2'.
Step 3: Embed 'S1' into last three LSB of 'C1' and Generate E1.

```
        Set kk=1
        For ii: 1 to height of C1
        For jj: 1 to weight of C1
        If kk<= size of S1
                sum=0;
                sum=sum+4*s1_vector(kk)
                kk=kk+1
        End
        If kk<=size of S1
                sum=sum+2*S1_vector(kk)
                kk=kk+1
        End
        if kk<=size of S1
                sum=sum+1*S1_vector(kk)
                kk=kk+1
        end
        if C1(ii,jj)+sum<255
                E1(ii,jj)=C1(ii,jj)+sum
        Else
                C1=C1(ii,jj)-sum
        End
Else
        ii=Height of C1
        jj=Weight of C1
End
End
```

Step 4: Repeat Step 3 for 'S2' and 'C2' Generate E2
Step 5: Calculate Difference between Embedded frames 'E1', 'E2' and frames 'C1' 'C2'.
Step 6: Calculate PSNR for E1 and E2.
Step 7: END

4.1 Computing Peak Single to Noise Ratio (PSNR) and MSE

The ratio between the maximum possible power of the signal and the power of corrupting noise that affects the reliability of watermark illustration is known as phase peak signal-to-noise ratio (PSNR). It is represented in terms of logarithmic decibel scale due to wide range of signals.

For measuring performance of algorithm we need to check The Peak Single to Noise Ratio (PSNR). PSNR is a common measure of the quality of Embedded Image.

Calculating PSNR using following formula:

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right)db \quad (4.1)$$

The mean square error (MSE) of two images of N x N pixels is defined as:

$$MSE = \frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left(p_{ij} - p'_{ij}\right)^2 \quad (4.2)$$

Where P_{ij} is the original cover image value and p'_{ij} is the embedded image pixel value. The higher the pixel value the better the quality of the reconstructed image.

5. SIMULATION AND RESULTS

For calculation of Peak Signal to Noise Ratio (PSNR) and MSE for the analysis and simulation algorithms, we have used MATLAB software.

The information hiding includes both information embedding algorithms and information extraction algorithms. Embedding is an information hiding process, while extraction is the restoration process of secret information. Therefore extraction operation is the inverse operation of embedding operation. As the better performance of the proposed visual cryptography scheme, we use the Secret Data as shown in Figure 1(a) and in figure 1(b) shows the binary image of this secret data.

Digital images are mainly of two types:-

- 24 bit images, and
- 8 bit images.

In 24 bit images we can embed three bits of information in each pixel, one in each LSB position of the three eight bit values. Increasing or decreasing the value of pixel by changing the LSB, does not change the appearance of the image. Therefore the resultant stego image looks similar to the cover image}

Digital image is most popular of medium to transfer information among audio, video and other media. In the process of information hiding message from sender is hidden into a host medium, which is only known by the recipient. In case of image hiding system, the image in which secret message is embedded is known as host image (cover image) and the resultant image is known as stego-image in which message is embedded.

In a data hiding procedure, the host image must not be degraded too much, otherwise the quality of the embedded image or stego-image will not be acceptable, and the embedded data easily detected. A simple LSB substitution, which hides secret data into LSBs directly, is easy implemented but will result in a low quality stego-image. In order to achieve a good quality stego-image, we have used a substitution matrix to transform the secret data values prior to embedding into the cover image. For a 3-bit LSB substitution we have used a substitution matrix to overcome a long running time of the exhaustive search.

5.1 Secret Image

Figure 1 (a) Original Secret Data and (b) its binary equal Secret Data

Visual Cryptography technique has been proposed using LSB method. Using visual cryptography we split secret image into two different shares S1 and S2 .For checking visual cryptography we overlap two shares and we have found original secret image.

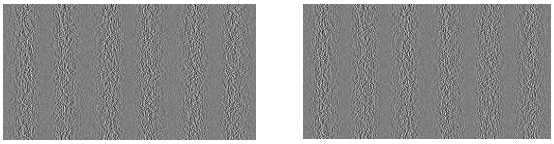


Figure 2 Two share of secret Data (a) First Share and (b) Second Share

Figure 3 Overlap of shares to check the visual cryptography

We use the last three LSB's of the cover images to insert the share of this secret data. Figure 2 shows the two separate shares of secret data which used in our dissertation work. For our dissertation work we have used three gif images (moving image) for analysis:

Secure Gif Image with Frames

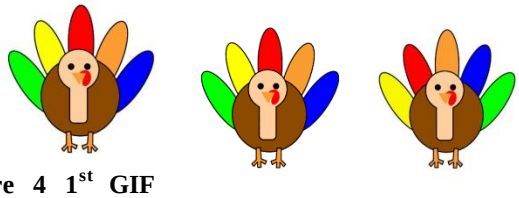


Figure 4 1st GIF image and its Frames (Bird)

Figure 5 1st GIF image and its Frames (boys)

Figure 6 3rd GIF image and its Frames (shoot)

5.2 Embedding Process:

We embedded the share one in to 1st frame moving image and share2 in to 2nd frames of moving image after embedding we find two different watermarked image. The process for implementing the visual cryptography is shown in figure 7. The figure shows the processes for secret data hiding on the cover object. First the secret data is split into two different parts called shares and then these shares embedded on two frames of moving images know as cover object then we create moving image back and we transmit this cover object to communication channel.

International Journal of Information and Communication Technology Research

http://www.esjournals.org

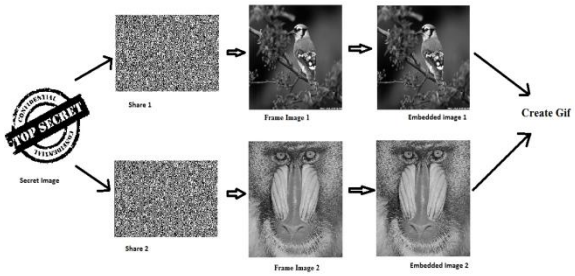


Figure 7 "EMBEDDING PROCESS"

Human eye cannot easily find this share in cover object. At the recipient side we apply the extraction process which is shown in figure 8. We easily find the secret data using overlapping these shares.

5.3 Extraction Process

In extraction process we first create two frames of a moving embedded cover image then we apply extraction algorithm to extract the shares. We get two shares share1 and share 2 using extraction process then overlapping two shares we get the original secret image.

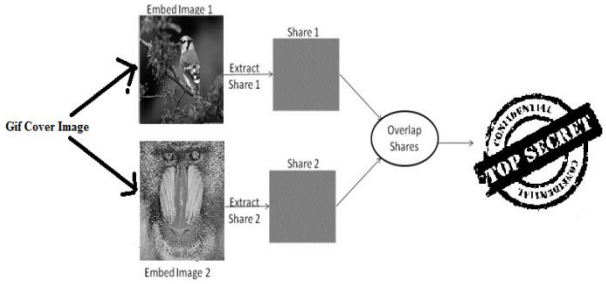


Figure 8 "Extraction Process"

From figure 7 and 8 shows the embedded images Original cover Image is almost same. Human eyes can almost not figure out the differences between these images. So the proposed visual cryptography schema is good to transfer the secret data over communication channel.

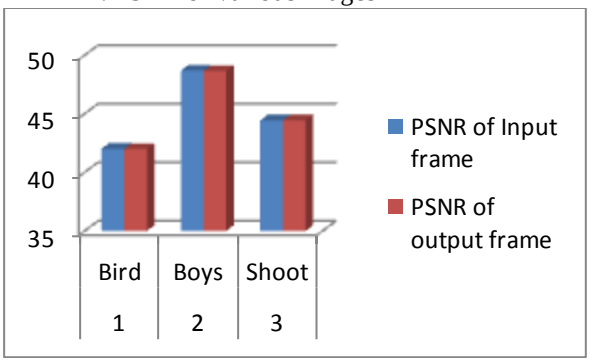
5.4 Result

We have applied two moving cover images for proposed scheme and find results for both of them. We have showed both results in form of table.

Following table shows the result of LSB method.

S. No.	Name of Cover Image	PSNR of Input frame	PSNR of output frame
1	Bird	42.02	41.99
2.	Boys	48.68	48.64
3.	Shoot	44.43	44.43

TABLE 1. PSNR of various images



When PSNR is higher than 30, recomposed image has a very good quality and the eye could hardly tell the difference between the original and the recomposed image. We got resultant PSNR is greater than 40db which shows our proposed scheme is good and it provides robustness also.

6. CONCLUSIONS

From the results it can be inferred that the new algorithm has merits in terms of configuration requirement, optimal running time, ease of use and a better PSNR value & reduced communication overhead. This type of information hiding and retrieval system can be easily implemented on a MAT Lab platform, providing less running time and ease of use. It also has benefit of using only one cover image (moving) as it can have multiple frames.

The robustness of LSB algorithm can be greatly increased by improving the watermark discovery or by expanding m sequence into two dimensions the security of algorithm can also be enhanced using encryption algorithms.

- This algorithm provides increased security by providing two levels of security. The information is protected in two phases; the first phase is to keep intruders out, if intruder break-in then second phase hides the data in such a way that is not recognizable by intruders.
- By using cryptography or steganography, it overcomes the limitation of single level hiding.
- As visual cryptography requires no computation time to decrypt information, adding a second level does not increase computation time in LSB algorithm.
- To differentiate between cover and stego images, LSB algorithm uses only the least significant bit planes are considered, this provides efficient way of comparison which is absent other algorithms.
- The benefit of using moving cover image is to ensure sending data only once and probability of hacking is less.

6.1 Scope for future development

Watermarking algorithms have wide area of application which is provided as follows. Future works will provide highest level of security and better performance.

- Pictorial database
- Photo image
- Video
- Audio
- Email server message

REFERENCES

[1]. M. L. Miller, I. J. Cox, and J. A. Bloom, "Informed embedding: exploiting image, Digital watermarking, Morgan Kaufmann Publishers Inc., San Francisco, CA, 2001.

[2]. Jitao Jiang, Xueqiu Zhou and Xiaohong Liu, "An improved algorithm based on LSB in digital image hidden", Journal of Shandong University of Technology (Science and Technology), vol. 20(3), 2006, pp. 66-68, ISSN: 1672-6197.0.2006-03-018.

[3]. Juan Zhou, Shijie Jia, "Design and Implementation of Image Hiding System Based on LSB", Computer Technology and Development, vol. 17 (05), 2007, pp. 114-116, doi: cnki: ISSN: 1673-629X.0.2007-05-034.

[4]. Gil-Je Lee, Eun-Jun Yoon, Kee Weng Yoo "A new LSB based Digital Watermarking Scheme with Random Mapping" in 2008 International Symposium on Ubiquitous Multimedia Computing.

[5]. Jianwei Zhang, Xinxin Fang, Junhong Yan, "Implement Of Digital Image Watermarking LSB", Control & Automation, vol. 22(10), 2006, pp. 228-229, doi: cnki:ISSN:1008-0570.0.2006-10-083.

[6]. Qian-lan Deng Jia-jun Lin, "A Steganalysis of LSB based on Statistics", Modern Computer, No.1, 2006, pp. 46-48, doi: cnki: ISSN: 1007-1423.0.2006-01-010.

[7]. Jian-quan Xie, Chun-hua Yang. "Adaptive hiding method of large capacity information", Journal of computer applications, vol. 27(5), 2007, pp.1035-1037, doi: CNKI: ISSN: 1001-9081.0.2007-05-001.

[8]. Hongwei Lu, Baoping Wan, "Information Hiding Algorithm Using BMP Image", Journal of Wuhan University of Technology, vol.28(6), 2006, pp. 96-98, doi: cnki: ISSN: 1671-4431.0.2006-06-027.

[9]. P. Geum-Dal,; Y. Eun-Jun,; Y. Kee-Weng , (2008) "A New Copyright Protection Scheme with Visual Cryptography", Second International Conference on Future Generation Communication and Networking Symposia. pp. 60-63.

[10]. J.J. Eggers, J.K. Su and B. Girod, "A Blind Watermarking Scheme Based on Structured Codebooks," IEE Colloquium: secure image and image authentication, London, UK, April 2000

[11]. A Westfield, A. Pfitzmann. "Attacks on steganographic systems". In Proceedings of 3rd. International Workshop Computer Science (IH '99) Germany, 1999.