Open access Journal International Journal of Emerging Trends in Science and Technology

Visual Secret Sharing (VSS) of Digital Images by Diverse Media using Stegnography

Authors

Pooja Ambekar, Yogita Bade, Payal Beura, Prof. S.M. Rajbhoj

Department of ENTC, Bharti Vidyapeeth College of Engineering for Women, Pune

Email: *Poojaambekar11@gmail.com,yogitabade6321@gmail.com,payalbeura@ymail.com*

Abstract

Visual cryptography (VC) is a technique that encrypts secret image in meaningful images. The meaningful images can be photos or hand-painted pictures in digital form or in printed form. N such shares can be used. VC is used to securely transmit secret images in non-computer aided environment. The shares can appear as noise-like pixels it will arouse suspicion and increase interception risk during transmission of the shares. Hence, VC schemes suffer from a transmission risk problem for the secret image. We also propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. Cryptography hides the contents of the message from an attacker, but not the existence of the message.To addresses this problem; we proposed Steganography that hides the very existence of the message in the communicating data. To hide noise like shares generated as a result of encryption, carrier image is used to reduce transmission risk; this technique used is called 'Steganography'. In addition to this Alpha channel watermarking is used in case where hackers hack the image and try to destroy the image. In alpha channel water marking the average value of RGB of meaningful shares is stored in alpha channel. Such that receiver is able to make it out the integrity of received image by comparing original image with alpha channel embedded image.

Index Terms—*Visual cryptography, steganography, shares, transmission risk.*

INTRODUCTION

Visual Secret Sharing (VSS) is a technique in which any no. of meaningful shares and one secret image are encrypted. This scheme enables us to securely transmit secret image to the intended receiver. In this process of encryption noise like share is generated which may arouse suspicion and increase interception risk during transmission. To solve this problem the proposed method uses the technique called steganography. To check the integrity at receiver end the process carried out is alpha channel water marking, which calculates the rgb value of the meaningful shares at transmitter and stores its value in alpha channel. At receivers side again the rgb value of the received meaningful shares is calculated and compared with received rgb value from transmitter side. A match in both the rgb values of receiver and transmitter indicates image as reached safely to the intended receiver.

RELATED WORK

As fig 6 shows. The first step is to acquire Meaningful images. It can be color or gray images. These can also be bookmark, web images etc. The next step is grayscaling. In photography and computing, a grayscale or grayscale digital image is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as

black-and-white, are composed exclusively of shades of grey, varying from black at the weakest intensity to white at the strongest.

RGB To Greyscale Conversion:

Fig 1. Rgb to grayscale conversion.

RGB to grayscale,grayscale to thresholding conversion:

Fig 2. Rgb to gray scale to binary conversion of meaningful image.

The meaningful images taken in step 1 are subjected to grayscaling, thresholding.

Then password is generated

On the basis of no. of white and black pixel generated during thresholding of each images. To calculate the password

Password= (No of black pixels+no. of white pixels) and this is shown in fig 3.

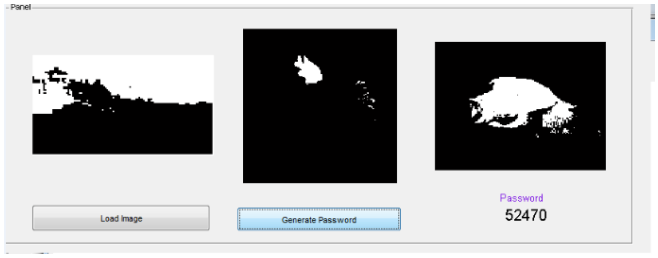

Fig 3.**generation of password.**

Pixel swapping of secret image is done using chaos sequence (password). Because of the distortions introduced into the acquire digital images different distortions are caused by each the encryption process and the decryption process. Since the acquired digital images in the encryption and decryption phases are not the same. These distortions result in noise that appears in the recovered images. When a large amount of noise clusters together, the image is severely disrupted, which may makes it impossible for the naked eye to identify it. The pixels-swapping process is used to cope with this problem. Noise also is distributed in the recovered image rather than clustered together. If the noise is distributed uniformly, the human visual system has a higher probability of recognizing the recovered image.

250	200	200	200
185	200	200	160
185	60	90	185
110	80	120	190

1	1	1	1
0	1	1	0
1	0	0	0
0	0	0	1

0	1	1	0
0	0	0	1
1	1	1	0
1	0	0	1

Fig:4 Original image pixels

b.Pixel value after Thresholding

c. Pixel values after swapping

the password that is generated in previous step which is as shown in fig 3 is used to pixel swapt or encrypt the secret image and it is shown in fig 5

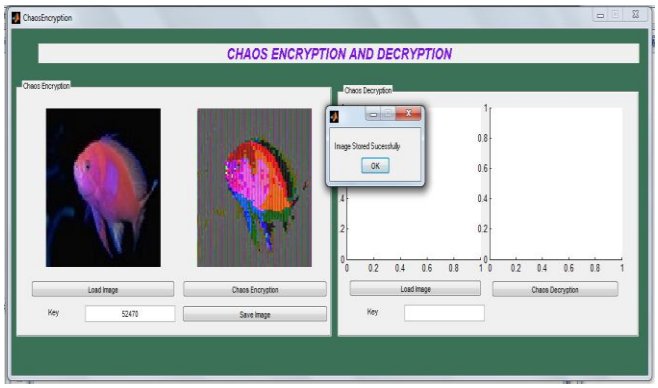

Fig.5 chaos encryption.

steganography is a process of hiding the data within a data. Carrier image is used to hide the noisy image. To hide the noise like share to reduce the transmission risk problem for the share a "Steganography" technique is used.

For stegnanography 3 bit LSB algorithm is used.

In the case of 24 bit color image each pixel is composed of RGB values and each of these colors requires 8-bit for its representation. [R (8 bits), G (8 bits) , B (8 bits)]. If we read color image in Matlab and display its first pixel, we get-:

>> a = imread('coverimage.jpg')

>> a (1,1,1) = 220

>> a (1,1,2) = 198

>> a (1,1,3) = 135

Here last term (1, 2 and 3) represent RGB component of pixels (1,1)
For ex. The image of RGB first pixel can be represent as
[11011**100** 11000**110** 10000**111**]
For embedding secret image whose first pixel is [11001001] firstly we have to replace last 3 LSB of each of RGB component and then embedding first 3 MSB of first pixel of secret image to R component, then next 3 MSB of first pixel of secret image to G component and lastly another next 3MSB of first pixel of secret image to B component. In this way we get stego image whose first pixel is:
[11011**110** 11000**010** 100000**010**].
In this method 9 bits of secret image get hide by replacing only 3 bits of RGB component so stego-image is visually indistinguishable from the original cover-image in the case of 24 bit.

An alpha channel is a special type of channel used in graphics software for saving selections. An alpha channel, representing transparency information on a per-pixel basis, can be included in grayscale and true color PNG images. Alpha channels can be included with images that have either 8 or 16 bits per sample, but not with images that have fewer than 8 bits per sample. The alpha sample for each pixel is stored immediately following the grayscale or RGB samples of the pixel. Alpha channel watermarking is used in case where hackers hack the image and try to destroy the image. The average value of RGB of meaningful shares is stored in alpha channel.
Decryption: At receivers end receiver is able to make it out by comparing original image with alpha channel embedded image the integrity of the transmitted images.

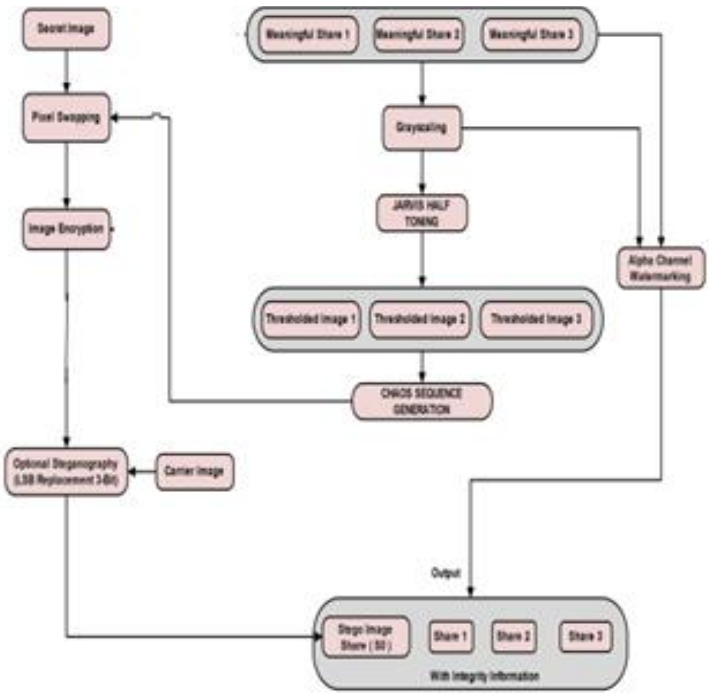

Fig 6 block diagram.

THE PROPOSED ALGORITHM

- ***Encryption algorithm:***

A. *Take meaningful images:*

The first step is to take meaningful share images. It can be gray or colour photographs of scenery, bookmarks, hand-painted pictures, web images. The images are subjected to grayscale conversion process.

B. *Algorithm for grayscale conversion:*

- Traverse through entire input image array.
- Read individual pixel color value (24-bit).
- Split the color value into individual R, G and B 8- bit values.
- Calculate the grayscale component (8-bit) for given R, G and B pixels using a conversion formula.
- Compose a 24-bit pixel value from 8-bit grayscale value.
- Store the new value at same location in output

Detail explaination of above algorithm:

i. Traverse Through Entire Image:

```
for(y=0; y<height ;y++) {
for(x=0; x<width ;x++) {
pix = input[y][x];
```

ii. Extract 8-bit R, G and B values from24-bit Color Value:

```
b = pix & 0xff;
g = (pix >> 8) & 0xff;
r = (pix >> 16) & 0xff;
```

iii. To separate blue we can use the logical AND operator to mask or filter the blue component from the rest. Since AND'ing with 1 makes no difference where as AND'ing with 0 will force the bit to 0.

a. For Green we shall first right shift the pixel value by 8 bits so that green component is now at LSB position And then repeat the masking process.

b. Similarly we shall right shift by 16 bits so that red component will be at the LSB position and then do the masking

iv. Calculate grayscale component

```
gs = (r + g + b) / 3;
```

Here average of all three colors is calculated and saved in output image.

C. *Algorithm for thresholding:*

- Traverse through entire input image array.
- Read individual pixel color value (24-bit) and convert it into grayscale.
- Calculate the binary output pixel value (black or white) based on current threshold.
- Store the new value at same location in output image.

D. *Chaos sequence generation*:

The meaningful images taken in step 1 are subjected to grayscaling, thresholding.

Then password is generated

On the basis of no. of white and black pixel generated during thresholding of each images. To calculate the password

Password= (No of black pixels+no. of white pixels)

i. Take a secrete image

ii. Enter the password

Password is used to pixel swap the image.

E. *LSB replacement/stegnography:*

- take pixel swapped image .
- take carrier image to hide pixel swapped image.
- enter key randomly to replace data in carrier image with pixel swapped image.
- display stego image.

F. *Alpha channel watermarking:*

Alpha channel watermarking is used in case where hackers hack the image and try to destroy the image. The average value of RGB of meaningful shares is stored in alpha channel. Such that receiver is able to make it out by comparing original image with alpha channel embedded image.

- ***Decryption process:***

1.reverse of encryption process is carried out to receive the secret image at receiver side back.

REFERENCES

1. M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.
2. R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia,"Incrementing visual cryptography using random grids," Opt. Commun.,vol. 283, no. 21, pp. 4242–4249, Nov. 2010. 98 IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 1, JANUARY 2014
3. P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992–1001, Sep. 2011
4. K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," IEEE Trans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.

5. G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, “Extended capabilities for visual cryptography,” Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.
6. N. Yang and T. S. Chen, “Extended visual secret sharing schemes: Improving the shadow image quality,” Int. J. Pattern Recognit. Artif. Intell., vol. 21, no. 5, pp. 879–898, Aug. 2007.
7. K. H. Lee and P. L. Chiu, “An extended visual cryptography algorithm for general access structures,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.
8. Z. Zhou, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography,” IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
9. Z. Wang, G. R. Arce, and G. D. Crescenzo, “Halftone visual cryptography via error diffusion,” IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.
10. I. Kang, G. R. Arce, and H. K. Lee, “Color extended visual cryptography using error diffusion,” IEEE Trans. Image Process., vol. 20, no. 1, pp. 132–145, Jan. 2011.