International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 8, November 2014, PP 40-44
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Data Security Using Visual Cryptography and Bit Plane Complexity Segmentation

Prashant Lahane[1], Yashashri Kumbhar[2], Suraj Patil[3], Swati More[4], Meenali Barse[5]

Department of CSE, MITCOE, Pune, India

Abstract: *The Internet information communication is used in many applications which are in a secret format. This is used in bank transfers, email communications, and credit card purchases on large number of daily email. But Internet is not a secure medium in reality. We are going to suggest Visual Cryptography approach which will provide us privacy protection while sharing secret financial documents over the Internet. These documents are represented in a bit map format file, and extend it into two or more encoded file shares which can be transferred to the receiver in a cover image using Bit Plane Complexity Segmentation technology through electronic mail or electronic file transfer process.*

The Bit Plane Complexity Segmentation allows hiding large secret information into cover image. This cover images are chosen for analysis and according to the threshold value it will increase the complexity of each segment to verify the changes occurred in the original image. therefore, the final image can be obtained only when the number of shares are combined together at receiving side. Thus a combined use of VC and BPCS technology provides data security to all forms of documents during transfer over internet.

Keywords: *Visual Cryptography, Steganography, vessel image, Bit Plane Complexity Segmentation, Information Hiding, Complexity.*

1. INTRODUCTION

In today's world, Internet communication has become an important part. The information send over internet is in numeric form. Applications of this are bank, credit cards, emails, business in which secret communication is required. People assume that internet communication is safe because it is small packet of data sent over internet. But in outside world there are many hackers who can hack the data easily.

Encryption is one part of data security which is used to encrypt data and encryption program are readily available. Encrypted message can be easily identified by hacker. So furthermore using new technologies it is possible to send information or data without noticing that secrete data has been sent. Visual Cryptography (VC) is technique used to hide the data in shares.

Steganography is another approach to data security. The term steganography has come from Greek word means, "Covered Writing". In steganography, data is hidden inside a vessel that appears like containing something. A variety of vessels are possible, such as digital images, sound clips, and even executable files. So that intermediate persons cannot see the message. A Stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data. LSB is one of the techniques of steganography in which information is stored at LSB position. So anyone can detect data easily. Capacity of data vessel is nearly 5-10%.

So we have invented a new technique Bit Plane Complexity Segmentation (BPCS) which is used to hide secret information in a colour image. This is not based on a programming technique, but is based on the property of human vision system.50% data of original image can be stored in vessel. This could open new applications for steganography leading to a more secure Internet communication age.

2. RELATED WORK

Shailender Gupta,Ankur Goyal, proposed information hiding using Least Significant Bit Steganography and Cryptography[1]. Shreelekshmi , Wilscy and C E Veni Madhavan, October 2010 proposed improving the Reliability Of Detection Of LSB Replacement Steganography[3]. Whereas, K. Devi Lavanya, Nittala. Raviteja, Katta. Mangarao, proposed a Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast scheme [4].

The above schemes results we cannot remove the graying effects of the images. The LSB technique can hide only 10-20% of data in the cover image. Noar and Shamir introduced VC where pixel expansion was used [2]. Moni Naor and Adi Sharma proposed new cryptographic scheme which can decode concealed images without any cryptographic computations[2]. But all above schemes supports only less number of image hiding, which results to image distortion and is unaddressed.

3. PROPOSED SCHEME

3.1. Visual Cryptography

In 1994, Naor and Shamir presented a new cryptographic paradigm based at the pixel level. Theytermed this *visual cryptography* and introduced it as a method for encrypting such things as handwritten notes, pictures, graphical images, as well as typed text stored as a graphic image. The performance of visual cryptography scheme depends on pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images (either binary or colour) and number of secret images(either single or multiple) encrypted by the scheme.

Visual cryptography is used to hide the information and divide the image into two parts and these two parts are called as shares that is share1 and share 2.

Black and white image: each pixel divided in 4 sub-pixels

- *White pixel:* shared into two identical sub-pixel layouts
- *Black pixel:* shared into two complementary sub-pixel layouts

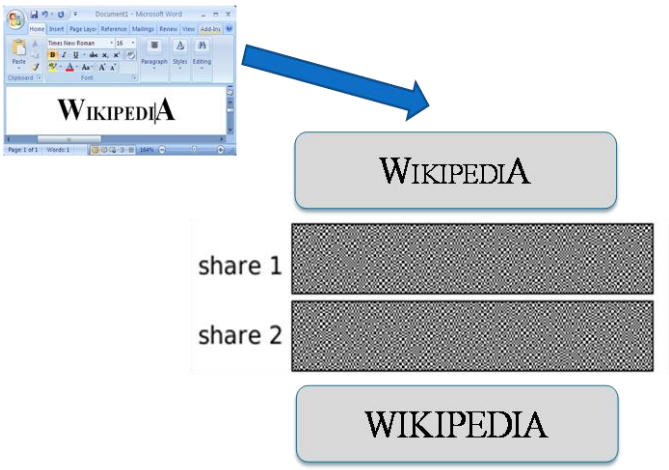

Fig1.1. *Visual Cryptography*

Perfect Security

- Layout was randomly chosen
- Each pixel has 2 black and 2 white sub-pixels

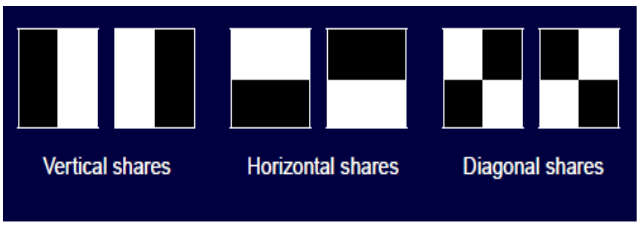

Fig1.2. *Pixel Expansion*

3.2. BPCS

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason, to overcome the short comings of traditional steganography techniques such as Least Significant Bit (LSB) technique, Transform embedding technique, Perceptual masking technique. Previously steganography techniques have limited information-hiding capacity.50–60% Data can be hidden after implementation of this

paper. This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. BPCS steganography makes use of important characteristic that of human vision. In BPCS, the vessel image is divided into informative region and noise-like region and the secret data is hidden in noise blocks of vessel image without degrading image quality. In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits. But in BPCS technique, data is hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region.

3.3. System Model

Architecture

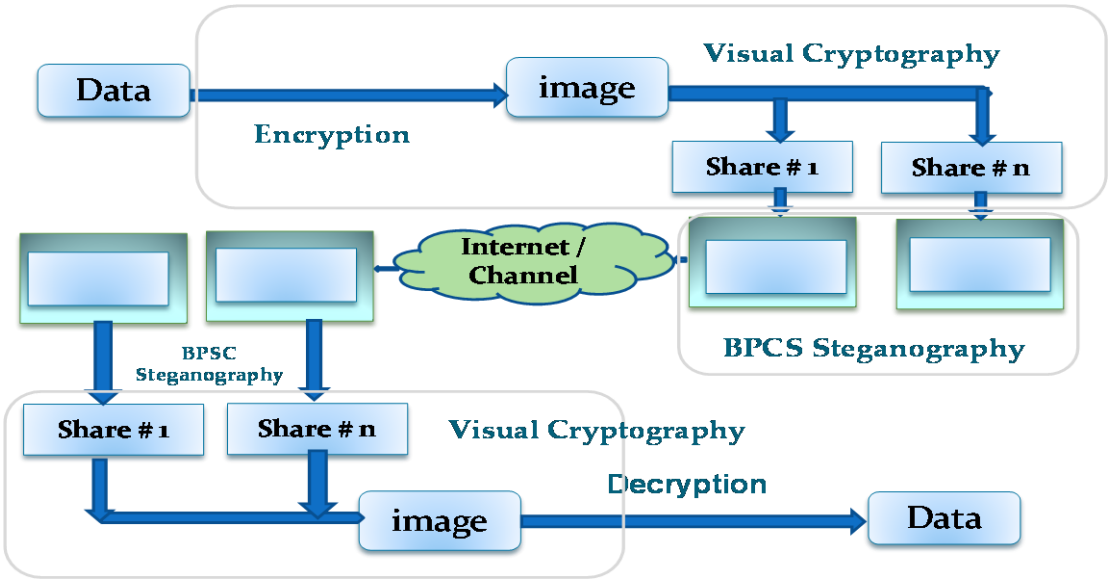

Fig1.3. *Architecture of VC and BPCS*

In this technique we are using BMP image format to hide the information because BMP image can store a large amount of data. By using visual cryptography we make two shares of image in which we hide the data. Again by applying BPCS on individual shares, make bit planes of shares. According to bits positions we store bits in corresponding planes. Make segments means divide plane in equal numbers of blocks. We calculate complexity of each segment. According to complexity values we store our data in respective segments by considering threshold value. Threshold value is needed when most important data is to be sent so we can store data in segments those are having high complexity value that is high complexity value proportional to high security. Send these shares over internet, at receiver side exactly opposite operations are done to retrieve data.

3.4. Calculating the Complexity

Here using BPCS technology we use 24-bit colour image. The image is of 54 byte header format which is divided number of bit planes. Bit plane is a collection of bits of particular position of particular colour. For example, consider bit plane 0 of red colour and divide the pixel into RGB format which are of 8-bit. We make segments of each bit plane 0 and then divide the segment and calculate the complexity of segment.

Complexity of Segment= Number of bit change/number of bits in the block.

3.5. Proposed Algorithms for VC and BPCS

3.5.1. Algorithm for Share Generation:

1. Start

2. Read Number of pixels in Secret image

3. Calculate the size of share using No. of Pixels X 4 for each share.

4. While end of Secret image

{

Read one pixel from Secret image

If (Secret Pixel= =1) then

{

Share1= [0 , 0 , 1, 1];

Share2= [0 , 0 , 1, 1];

}

Else

{

Share1=[1 ,1 , 0, 0];

Share2=[0 ,0 , 1, 1];

}

}

5. Generate images share 1 and share 2 .

6. Stop

3.5.2. Algorithm for Share Overlapping

1 .Start

2. Read Number of pixels in Share 1 image and Share 2 image.

3. Calculate the size of Secret using No. of Pixels / 4

4. while end of shares

{

Read 4 pixel from share1 and share2

If (Share1= = [0 ,0 , 1, 1] XOR Share2= =[0 ,0 , 1, 1]) then SecretPixel=1;

Else

SecretPixel=0;

}

5. Generate Secret Image.

6. Stop

3.5.3. Algorithm for Share Hiding Using BPCS Steganography (BPCS Encoder)

1. Start

2. Number of pixels in Cover Image.

3. Read the share

4. while end of shares length

{

CreateBitPlane();

Segmentation();

{

CalculateComplexityOf8X8Block using

Complexity=Total No. of changes in the Black and white Border / blocksize;

If (Complexity> thresholdValue)

Hide data into of segments;

Else

go for next segment of current bit plane;

}

}

5. Generate Stego Image.

6. Stop.

4. CONCLUSION

In this way we conclude that, we can hide the image data in the cover image and can sent to the receiver side in secret format using complexity algorithm and also increase the image capacity. This helps to develop new applications which will be secured for internet communication.

RESULTS

By increasing the threshold value we can increase the security of data. We can also decrease the image distortion and graying effects.

REFERENCES

[1] Information Hiding Using Least Significant Bit Steganography and Cryptography, Shailender Gupta,Ankur Goyal, June 2012

[2] Department of Applied Math and Computer Science, Weizmann Institute, Rehovot, 76100, Israel. e-mail: {naor,shamir}@wisdom.weizmann.ac.il.

[3] IMPROVING THE RELIABILITY OF DETECTION OF LSBREPLACEMENT STEGANOGRAPHY Shreelekshmi , Wilscy and C E Veni Madhavan, October 2010.

[4] A Secure and Lossless Adaptive Image Steganography with Mod-4 LSB Replacement Methods Using Image Contrast, K. Devi Lavanya, Nittala. Raviteja, Katta. Mangarao, January 2014.