www.ijecs.in
*International Journal Of Engineering And Computer Science ISSN:2319-7242*
*Volume 4 Issue 5 May 2015, Page No. 11997-11999*

# Visual Cryptography and BPCS Steganography for Data Shielding

***Prashant Lahane, Yashashri Kumbhar, Suraj Patil, Swati More, Meenali Barse***

Pune University,Department of Computer Engineering, MITCOE, Pune, India

**Abstract:Internet communication has become the essential part of the infrastructure of today's world. The information communicated in various forms and this information is used in many applications which are in a secrete format. Security is one of the most important factors for transferring different types of important documents. Internet is one of the most important media which is used to transfer documents. This is used in bank transfers, email communications, credit card purchases on large number of daily email and military application. But in reality the internet is not a secure form. So we are suggesting VC that is visual cryptography method which is simple, fast and provide security while sharing secretes documents over the internet. These documents are presented 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 BPCS that is Bit Plane Complexity Segmentation technology through electronic mail. The Bit Plane Complexity Segmentation allows hiding large secret information into cover image. This cover images are selected 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. And data will be stored at higher complexity. Steganography is technique of data hiding. Steganography is a technique in which secret data is hidden into vessel image. All other techniques have limited data hiding Capacity and other technique can hide up to 15% of data amount of vessel image. But hiding capacity of steganographic technique is up to 50 –60%. This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. Therefore, the final image can be obtained only when the number of shares is 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:** *VC (Visual Cryptography), Steganography, vessel image, BPCS (Bit Plane Complexity Segmentation), SI (Secrete Image), Information Hiding, Encryption, Decryption, Complexity, Bit plane, Segmentation*

## 1.Introduction

With the rapid improvement of network technology, multimedia information is transmittedOver the Internet easily. Various private data such as military maps and commercial identifications are transmitted over the Internet. Internet is used to transfer the documents. So security is one of the most important forms for transferring different kinds of data. But in reality internet is not secure medium because one can easily hack private information in document.

Due to security problems of secret images, various image secret sharing methods have been developed. Visual cryptography is introduced by first in 1994 Noar and Shamir. Visual Cryptography is a special encryption technique to provide security with images. In this technique Secret Image is expanded in to shares using pixel expansion method. So by overlapping shares original secret image can be retrieved. Visual cryptography scheme eliminates complex computation problem in decryption process. Therefore visual cryptography especially useful for the low computation load requirement.Steganography is another method to data security. The word steganography has come from Greek word means, "Covered Writing". Steganography is technique of data hiding. Steganography is a technique in which secret data is hidden into vessel image. The hiding capacity of steganographic technique is up to 50 – 60%. 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 invented new technique and this technique is called Bit Plane Complexity Segmentation (BPCS) Steganography which is used to hide secret information in a color image. It will store large information in the image. The data is stored in highly complexed regions or segments. Hence due to this maximum data storage, it is feasible for information security. for this BPCS BMP image format is feasible.Therefore, the final image can be obtained only when the number of shares is 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.

## 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. 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 .

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. Main drawback of LSB technique is hacker can hack the data easily.So 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 into image distortion.

## 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 significant or not significant, type of secret images (either binary or color) 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 similar sub-pixel layouts

*Black pixel:* shared into two corresponding sub-pixel layouts.

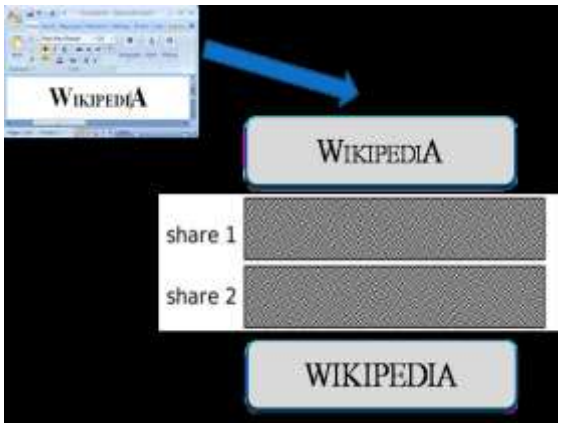


***Fig1.1. Visual Cryptography***

*Perfect Security*

-Layout was randomly chosen

-Each pixel has two black and two white sub-pixels

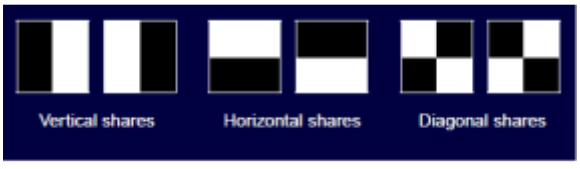


***Fig1.1. Visual Cryptography***

• If the pixel is black

• If the pixel is white

So like this there are 16 possible combinations of pixel expansion for each white and black and algorithm will choose any random one to expand the pixel.

### 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 technique makes use of important characteristic that of human vision. In BPCS technique, the vessel image is divided into instructive 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 only in the last four LSB bits. But in BPCS technique, data is hidden in most significant bit (MSB) planes along with the LSB planes provided secret data is hidden in complex region.

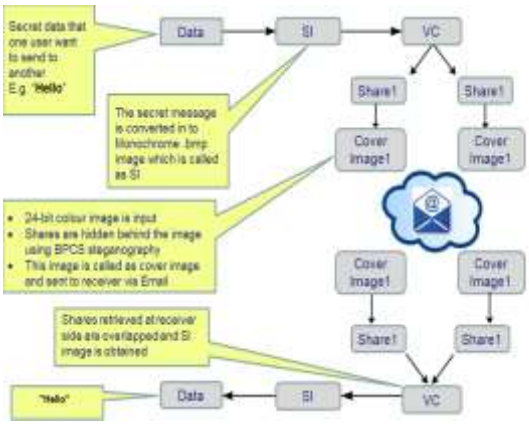


***Fig1.3. Architecture of VC and BPCS***

• 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 separate shares, make bit planes of shares. According to bits positions we store bits in corresponding planes. Make segments means divide plane into equal numbers of blocks. Then we can calculate the 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. Confidential communication and secret data storinge.g. Business communication that does not have be licked. Protection of data alteration e.g. military message that should not be changed by hackers. Alleged usage by terrorists and intelligence agencies Carrying out data encryption in places like banks.e.g. Security codes can be shared with protection these are the applications of this technique.

**Method of doing BSCS**

• Take 24-bit image as input and one share that we want to hide behind the 24-bit image.

• Read the image and covert byte data into bit data and then make 24 bit planes of the image.

• Then make segments of all the bit planes. Calculate complexity of each segment.

• And store share in that.

• The goal of steganography is to hide messages inside a cover image in a way that does not allow

any "enemy" to even detect that there is a secret message present.

Due to this technique there is no data alteration.Randomization of bits so as that it is nearly impossible to hacker to restore information, large information can be hidden nearly 65% of vessel.

**3.3. Calculating the Complexity**

Segmentation tells us about in which block we should store data according to complexity value. Data will be stored in highly complex segments.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 group 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.*

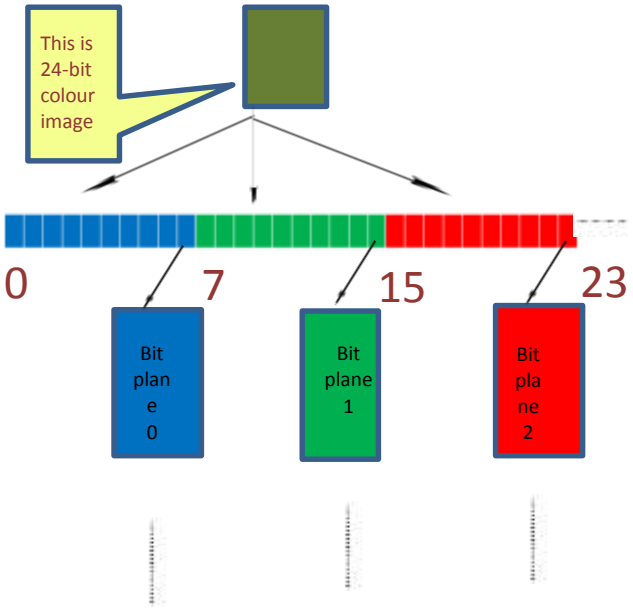


***Fig 1.4.Making bit planes from color image***

**4. Conclusion**

In this way we conclude that, we have presented a feasible solution for Image Steganography that takes the advantage of segmentation method by which we can find the position of the bits and retrieve data from the bit plane.It also makes use of complex mathematical calculations which bring down the computational time very less making it a very effective method for Image Steganography.

**5. Results**

• It can be very useful if can install it on web. Means if we make it web based then there will be no need of installing application on every computer.

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

**References**

[1] Information Hiding Using Least Significant Bit Steganography and Cryptography, Shailender Gupta,Ankur Goyssal, 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.