RESEARCH ARTICLE OPEN ACCESS

Enhancing the Security of Information Using Bit Plane Complexity Segmentation

Kishore Kumar R, Harikrishna
Dept. of ECE, BIT Institute of Technology, Hindupur, India
kishorekumar435@gmail.com
Asst. Prof., Dept. of ECE, BIT Institute of Technology, Hindupur, India.
hari05ec@gmail.com

Abstract—
Security of secret information can be increased by hiding the data. Protecting the contents of the secret information from intruders is the main challenge. The old technique Steganography can be used to hide the data. In steganography the data can be hidden in the image and we can transmit it to the receiver. All of traditional techniques have limited information hiding capacity. They can hide only certain amounts of data in host image. This is because the principle of those techniques was either to replace a special part of the frequency components of the vessel image, or to replace all the least significant bits of a multivalued image with the secret information. This paper focuses on BPCS (Bit Plane Complexity Segmentation) steganography. This technique makes use of the characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. We can replace all of the
"noise-like" regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. The main principle of BPCS technique is that, the binary image is divided into informative region and noise-like region. The secret data is hidden into noise-like region of the vessel image without any deterioration.

Keywords— Steganography, Bit Plane Complexity Segmentation, Least Significant Bit method

I. INTRODUCTION

Information hiding is an emerging research area, which encompasses applications such as copyright protection for digital media, watermarking, fingerprinting, and steganography. In watermarking applications, the message contains information such as owner identification and a digital time stamp, which usually applied for copyright protection. Fingerprint, the owner of the data set embeds a serial number that uniquely identifies the user of the data set. This adds to copyright information to makes it possible to trace any unauthorized use of the data set back to the user [8].Steganography hide the secrete message within the host data set and presence imperceptible and is to be reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be invisible to an information analysis. The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data. It is not to keep others from knowing the hidden information, but it is to keep others from thinking that the information even exists. If a steganography method causes someone to suspect the carrier medium, then the method has failed.

The advantage of Steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny. Plainly visible encrypted messages-no matter how unbreakable-will arouse interest, and may in them be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the contents of a message alone, Steganography is concerned with concealing the fact that a secret message is being sent, as well as concealing the contents of the message. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.

Modern steganography entered the world in 1985 with the advent of the personal computers being applied to classical steganography problems. There has been a rapid growth of interest in steganography for two main reasons:

i. The publishing and broadcasting industries have become interested in techniques for hiding encrypted copyright marks and serial numbers in digital films, audio recordings, books and multimedia products.

ii. Moves by various governments to restrict the availability of encryption services have motivated people to study methods by which private messages can be embedded in seemingly innocuous cover messages.

II.BPCS STEGANOGRAPHY

In BPCS, a multi-valued image (P) consisting of n-bit pixels can be decomposed into set of n – binary pictures. Ordinary image data is represented by a pure binary code system which is commonly used in image processing. However CGC is preferred over PBC in BPCS steganography. Example: P is an n-bit gray image say n=8. Therefore P = [P7 P6 P5 P4 P3 P2 P1 P0] where P7 is the MSB bit plane and P0 is the LSB bit plane. Each bit plane can be segmented into "informative" and "noise" region. An informative region consists of simple pattern while noise-like region consists of complex pattern. In BPCS, we replace each noise-looking region with another noise-looking pattern without changing the overall image quality. Thus, BPCS steganography makes use of this nature of human vision system. In this method we transfer the original image into grey scale image, this step is to reduce the size because the colour bitmap image is three times higher in size than greyscale image with the same dimensions, hence the grey scale image could be used as a cove image, this 8-bit grey scale image which is in PBC (pure binary coding) form is converted into CGC (canonical gray coding) form. CGC allows us to manipulate each bit plane without affecting the other bits that represent each gray scale value. 8*8 pixel blocks are segmented within the image and each of the bits (8 bits per pixel) in CGC form will have their own corresponding 8x8 plane. Each bitplane will be measured for complexity, which is determined by the number of borders (transitions between black and white in each pixel plane) present in an 8x8 bit plane versus the maximum borders possible. If a region is complex enough, we will embed our data into the cover image, which is broken up into appropriately sized 8x8 blocks for each bit plane.

If the data to embed (8x8 blocks at a time) in the vessel image is statistically complex, it can be embedded into the complex blocks of the image. If not, we will conjugate (exclusive or) the data with a checkerboard pattern (the most complex pattern possible) to ensure complexity. Once the data has been embedded, the image is converted back into the original format from CGC and saved.

III. ALGORITHM FOR EMBEDDING IMAGES

- Step 1: Consider a color image as vessel image .Make the size of image as 1024*1024.
- Step 2: Convert the vessel image to gray scale image
- Step 3: Consider a four color images as secret images. Make the size of those images as
- 256*256.
- Step 4: Convert those colour images to gray scale images.
- Step 5: Convert the both vessel image and four secret images which are in pure binary code (PBC) to canonical gray code (CGC) form.
- Step 6: Perform the bit plane splicing on both vessel image and the secret images.
- Step 7: Calculate complexity measure „alpha‟ (α) for each block of each bit plane of vessel image.
- Step 8: Calculate „α‟ for each block of each bit plane of secret images.
- Step 9: Perform conjugation operation on the „simple‟ or „informative‟ block of secret images.
- Step 10: Perform embedding operation to embed secret images in vessel image. Resulting embedded image will be called as „STEGO‟ image.
- Step 11: Convert the CGC form of „STEGO‟ image to PBC image.

IV.ALGORITHM FOR EXTRACTING IMAGES

Step 1: Consider the „STEGO‟ image and convert to CGC form.
Step 2: Perform the bit plane splicing on the
„STEGO‟ image.
Step 3: Extract the embedded blocks of secret images from the
„STEGO‟ image.
Step 4: Segregate the images into four different images. Step 5: Convert the CGC form secret images to PBC form.

V. ANALYSIS AND RESULTS

It gives the details about each processing steps of embedding and extracting algorithms which are included in this method. It also gives the measure of BPCS steganography, parameters such as MSE and PSNR values for different number of images embedded.

The graphical user interface has been provided. This can run separately for Single image in single image and multiple images in a single image. The variation of MSE and PSNR values depending on the number of images hidden is shown using bar graph. It also displays these values in table.

Here, the considered vessel image is,

The following figures show the secret images, we are choosing four secret images.

After the secret images are chosen, these secret images are embedded into host image to produce "stego" image. stego

image is displayed as final embedded image.

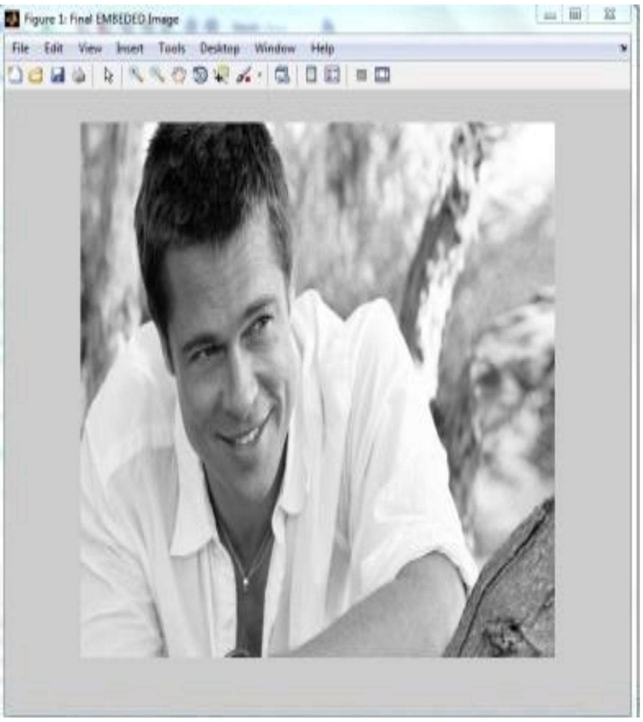


Figure 1: Final EMBEDED Image
File Edit View Insert Tools Desktop Window Help

After the Stego image is chosen, we can extract the secret images from the stego image. The extracting process is executed and the obtained secret images are displayed as extracted secret images. Hence all secret images are separated from stego image.

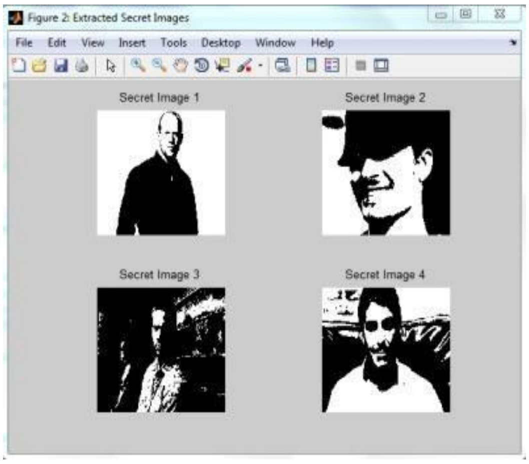
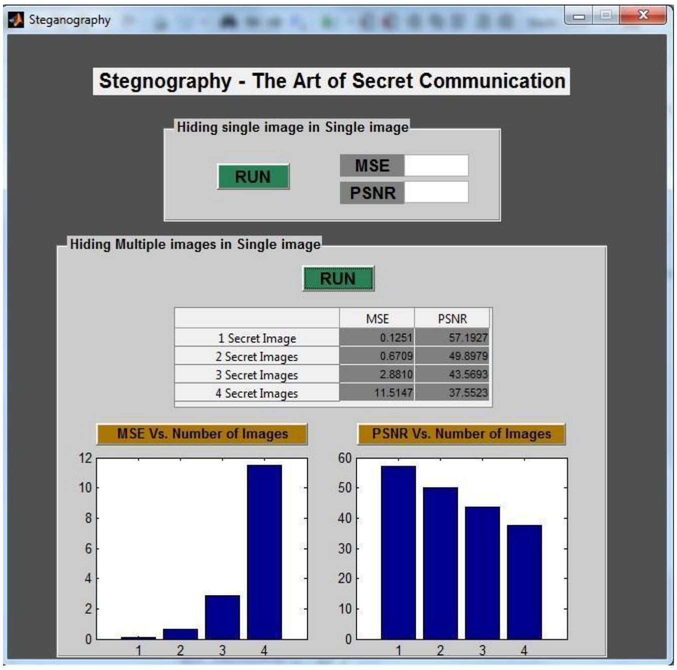


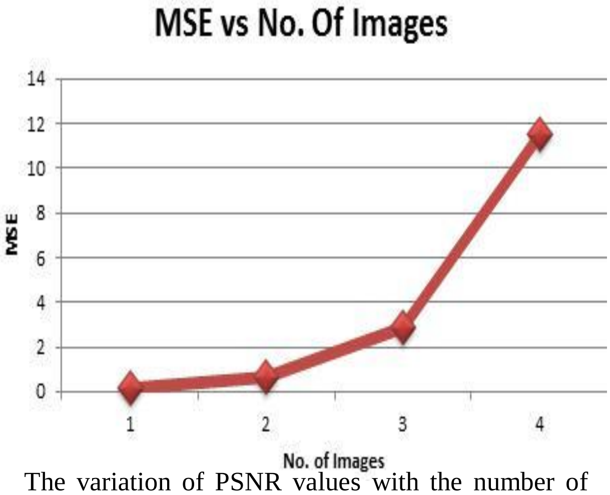
Figure 2: Extracted Secret Images
File Edit View Insert Tools Desktop Window Help
Secret Image 1
Secret Image 2
Secret Image 3
Secret Image 4

The MSE and PSNR values are calculated in the program. They are calculated for single image hidden, two images hidden, three images hidden and four images hidden in a single vessel image. These values are tabulated in table in graphical user interface. The variation of MSE and PSNR values is represented in the form of graphs. MSE vs. No. of images shows the variation of MSE with the number of images. Similarly PSNR vs. No. of images shows the variation of PSNR with the number of images.

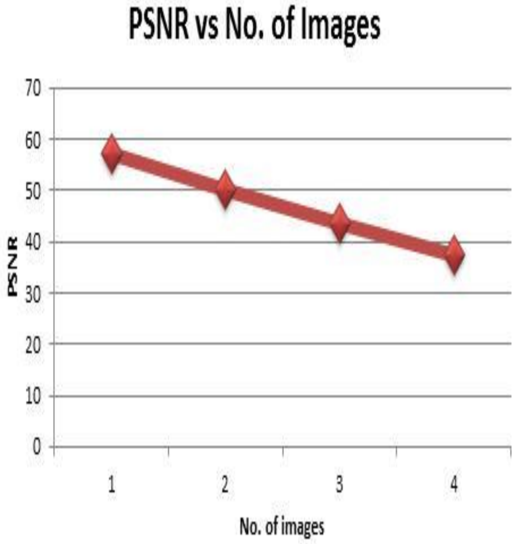

Steganography
Stegnography - The Art of Secret Communication
Hiding single image in Single image
RUN
MSE
PSNR
Hiding Multiple images in Single image
RUN
MSE Vs. Number of Images
PSNR Vs. Number of Images
12
10
8
6
4
2
0
1
2
3
4
60
50
40
30
20
10
0
1
2
3
4

	MSE	PSNR
1 Secret Image	0.1251	57.1927
2 Secret Images	0.6709	49.8979
3 Secret Images	2.8810	43.5693
4 Secret Images	11.5147	37.5523

The variation of MSE values with the number of secret Images hidden is as shown in the below graph.



The variation of PSNR values with the number of secret Images hidden is as shown in the below graph.



VI. CONCLUSION

Thus, from the experiment for three different sets of images, it is concluded that the BPCS technique has high data embedding capacity. Also, it is seen that the original image and the final embedded image appear to be identical to the human eye. Here, four secret images are hidden in a single vessel image and have been extracted. From the comparison of MSE and PSNR values for different number of images hidden, we can conclude that, embedding more than one image in an image loses its resolution. However where image quality is not needed and number of images are of more important, than we can go for this technique.

VI. ACKNOWLEDGEMENT

The author would like to thank Harikrishna (Asst. Prof), Prof. Jagadish naik (Project-Coordinator) and Sudarshan Raj(HOD) for their support.

REFERENCES

[1.] *J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. USENIX Security Symp., pp. 15-28, 2003.*

[2.] *F. Ferreri, M. Bernaschi, and L. Valcamonici, "Access Points Vulnerabilities to Dos Attacks in 802.11 Networks," Proc. IEEE Wireless Comm. and Networking Conf., 2004.*

[3.] *D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.*

[4.] *Q. Li and W. Trappe, "Relationship-Based Detection of Spoofing- Related Anomalous Traffic in Ad Hoc Networks," Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON),* *2006.*

[5.] *B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.*

[6.] *A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677-686, 2005.*

[7.] *Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength," Proc. IEEE INFOCOM, Apr. 2008*