IMAGE STEGANOGRAPHY USING BIT PLANE COMPLEXITY SEGMENTATION

Zin Mar Htun[1], Zar Ni Zin[2]

Technological University (Taunggyi), Lecturer, +095, Myanmar

Abstract

The security of information has become an essential part in digital communication environment. Enhanced security is not kept by secret word insurance however it is picked up by concealing the presence of the information, which must be finished by Steganography. Moreover, all of the traditional stenographic techniques have limited information-hiding capacity. They can shroud just 10 to 15 % of the information measures of the vessel. Bit-Plane Complexity Segmentation, (BPCS), is one of the steganography techniques that grouping the set of the original message to bit-planes. The data concealing limit is around half of the container size. Thus, the proposed system tends to use BPCS Steganography for embedding secret information within an image vessel which unchanged to human visual eyes. The primary standard of BPCS strategy is that, the binary image is separated into informative region and noise-like region. The system is implemented by using python programming language.

Keyword: BPCS, vessel, python

1.INTRODUCTION

aphy, from the Greek, implies secured, or mystery composing, and is a since a long time ago rehearsed type of concealing data. Albeit identified with cryptography, they are not the equivalent. Steganography's aim is to conceal the presence of the message, while cryptography scrambles a message so it can't be comprehended. All the more correctly, the objective of steganography is to conceal messages inside different innocuous messages in a manner that doesn't permit any adversary to try and identify that there is a subsequent mystery message present. Steganography incorporates a huge range of strategies for concealing messages in an assortment of media. Among these techniques are undetectable inks, microdots, computerized marks, clandestine channels and spread-range correspondences. A message is embedded in a cover media in an invisible manner so that one could not suspect about its existence [1].

Image steganography techniques can be gruoped into two significant classes for example spatial domain procedures and frequency domain techniques. In spatial area procedures, the secret message is covered up inside the image by applying some control over the various pixels of the picture. In frequency domain techniques the image is changed to another form by applying a change like discrete wavelet change and afterward the message is covered up by applying any of the standard installing strategies. This research focuses on the spatial domain in image steganography [2].

The image in which secret message is covered up is called as the stego-image. There are various classes of techniques in spatial space, (i) LSB steganography, (ii) RGB based steganography,(iii) pixel value differencing steganography, (iv) mapping based steganography, (v) palette based steganography,(vi) collage based steganography, (vii) spread spectrum steganography, (viii) code based steganography, and(ix) others[3].

All of the conventional steganography procedures have restricted data concealing limit. They can conceal just 10% (or less) of the information measures of the vessel. Eiji Kawaguchi and R. O. Eason [16And] discovered the new technique to overcome the short comings of traditional steganographic techniques. It is called Bit-Plane Complexity Segmentation (BPCS). The data concealing limit is around half of the container size. It is replaced all of the ”noise-like” regions in the bit-planes of the vessel image with secret data without deteriorating the image quality. As a result, this research is selected BPCS technique for image steganography.

2. LITERATURE REVIEWS

Steganography is the workmanship and study of imperceptible correspondence. This is cultivated through concealing data in other data, hence concealing the presence of the conveyed data. MoerlandT.presented that word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing" defining it as "covered writing". In many rivalry environments, concealing the existence of communication is desirable to avoid suspicion from adversaries. The goal here is to have a covert communication channel between two parties. Steganography can protect the information from unwanted parties. Covert communications have a long history and firstly they were mainly used in military and intelligence agencies. Today steganography is mostly and widely used on computers with digital data being the carriers and networks being the high speed delivery channels [4].

Walton, S. and Matsui, K. and Tanaka,K. pointed out that watermarking has been considered to be a promising solution to protect the copyright of multimedia data through transcending, because the embedded message is always included in the data. There is no proof that watermarking methods can accomplish a definitive objective to recover the correct proprietor data from the got information after a wide range of substance saving controls. Due to the devotion limitation, watermarks must be inserted in a restricted space in the interactive media information. There is constantly a one-sided advantage for the assailant whose target is just to be freed of the watermarks by misusing different controls in the limited watermarking implanting space. The primary intrigue is worry over copyright that drives ongoing examination into advanced "watermark" and "fingerprints". The purpose of the mark is to supply some additional information about the image without visibly modifying the image.This thesis intends to offer a state of the art overview of the different algorithms used for image steganography to illustrate the security potential of steganography for business and personal use [5].

JaewonYoo, Jihong Kim, S. I offered that text steganography using digital files is not used very often since text files have a very small amount of redundant data as compared with a picture or a sound bite. While it is often possible to make imperceptible modification to a picture, even an extra letter or period in text may be noticed by a casual reader.Data hiding in text is an exercise in the discovery of modifications that are not noticed by readers. Three major methods of encoding data are considered: open space methods that encode through manipulation of white space (unused space on the printed page), syntactic methods that utilize punctuation, and semantic methods that encode using manipulation of the words themselves [6].

D. Ghosh presented a linguistic approach for Steganography through Indian Languages by considering the flexible grammar structure of Indian Languages. The addition of security to the system, as an alternative of hiding the original message the data is converted to an irrelevant binary stream by associating the message bits with the pixel values of an Image. Then, the bits of this binary stream are encoded to some part-of-speech and by creating meaningful sentences starting with a suitable word belonging to the mapped part-of-speech, the proposed strategy conceals the message inside a spread record containing some harmless sentences. Also in accepting side, the calculation finds the comparing grammatical form of the beginning expression of each sentence and spot the bit stream of the mapped grammatical form to recuperate the changed over message. Subsequent to contrasting these bits and the Image pixels, the calculation separated the first message from the spread document. The method exhibits satisfactory result on some Indian Languages like Bengali [7].

Kalavathi, A. and Ramineni, S. R. P.have proposed a few text based steganographic methods. The methods worked by using the linguistic properties of Telugu language. The primary technique chooses insert position of the mystery data in the spread content by utilizing Telugu Ottulu. In view of the two level arrangement of Ottulu, they are alloted somewhat 0 or somewhat 1. These images implant the mystery data in the third character of Telugu spread Text information. It maps a single bit of the data with a Telugu character in the specified manner [8l].

3. METHODOLOGY

Eiji Kawaguchi and Richard O. Eason introduced BPCS in 1998 by [9] to overcome the shortcomings of the traditional Least Significant Bit (LSB) manipulation techniques. While the LSB control procedure works very well for most dark scale and RGB shading pictures, it is seriously disabled by its constraint in limit, which is confined to about oneeighth the size of the base picture. BPCS depends on the basic thought that the higher piece planes could likewise be utilized for installing data gave they are covered up in apparently "complex" districts.

3.1. Working Principles of BPCS

The first step in BPCS Steganography is to find "complex" regions in the image where data can be hidden imperceptibly. There is no universal definition for the complexity of an image (or a region of an image). Kawaguchi and Niimi discuss two different complexity measures, one based on the length of the black-and-white border and another based on the number of connected areas that could be used to find the complex regions in an image [10].

This measure is defined on the 4-connected neighborhood of a pixel. The total length of the black-and-white border is defined as the sum of the color changes along the rows and columns in the image. For example, a single white pixel surrounded by 4 black pixels, i.e., having all its 4-connected neighbors as black pixels, will have a border length of 4 (2 color changes each along the rows and columns).

Extrapolating this idea to a square binary image of size 2N x 2N, the minimum border length possible is 0, obtained for an all white or all black image, and the maximum border length possible is 2 *2N *(2N- 1), for the black and white checker board pattern ((2N- 1) changes along each of the 2N rows plus the same along the columns). The image complexity measure, α, is then defined as the normalized value of the total length of the black and white border in the image, i.e.

$$\alpha = \frac{k}{2\times 2^{N}\times(2^{N}-1)}, 0 \le k \le (2\times 2^{N}\times(2^{N}-1)) ,$$

where k is the actual length of the black and white border in the image. It is evident that α lies in [0, 1] [10].

This measure is again based on the 4-connected neighborhood, β is defined as

$$\beta = \frac{m}{2^{N} x 2^{N}} ,$$

where m is the number of connected areas in the 2^N x 2^N square binary image. It is easily seen that P lies in [1/(2^N x 2^N), 1] with the maximum in the range obtained for the checker board pattern and the minimum obtained for the plain white or plain black image.

3.2. Encoding Procedure

The step-by-step procedural of encoding process can be summarized as follows:

Step 1: Read the image, convert the intensity values into Gray code and perform bit-plane decomposition.

Step 2: Determine a threshold for the complexity, α_{th}. For each exclusive 8x8 block in the bit-planes, calculate the complexity α. If $\alpha > \alpha t_{h}$, mark up the 8x8 block to becomplex (say by marking it up with 1. For a 512x512 image, this "mark up" matrix would be 64x64, for each bit-plane).

Step 3: Get the number of resource files to be embedded, n, make it the first byte of the Overall Header (OH), and embed that into the first complex block of the base image, conjugating it if necessary. Repeat steps 4 to7 'n' times or till the maximum embeddable capacity is reached.

Step 4: Read in the resource file and form it into a sequence (or vector) of ASCII values. Pad the sequence so that the number of bytes in the sequence is a multiple of 8. This is done because the encoder embeds blocks of 8 bytes at a time. Attach the 24 byte file header containing the file name and size to it.

Step 5: Read the file header, 8 bytes at a time, and form it into 8x8 binary blocks. Calculate α for the block and do one of the following:

- If $\alpha > \alpha_{th}$, then embed the resource block "as is" into the 8x8 block marked ' 1' in the base image (i.e., complex block in the base image) and append a '0' to the conjugation map to indicate that the block has not been conjugated.

- If $\alpha < \alpha_{th}$, then conjugate the resource block to increase its complexity to $(1 - \alpha)$ (it is assumed that α_{th} is less than 0.5, which it usually is) and then embed the resource block "as is" into the 8x8 block marked ' 1' in the base image. Append a ' 1' to the conjugation map to indicate that the block has been conjugated.

Step6: Break the conjugation map into blocks of 63 bits each, padding with zeros for the final block, if necessary. Make the first bit (top-left bit) ofan 8x8 block '0' and add the 63 bit block, into it, by rows. If the block is complex, embed it "as is' into the next available complex block in bit plane base image. If the block is not complex, then conjugate it andembed it into the next available complex block in the bit-plane base image. For the file header there will be just one such block.

Step 7: Repeat steps 5 and 6 substituting the resource file sequence for the file header.

Step 8: Put back the 24 bit-planes together to form 3 color planes, R, G & B, convert from CGC to PBC, and save the image, either under a new name or under the same name as its original to eliminate suspicion. This is the encoded image.

The decoding procedure is the reverse process of encoding process.

4. PROPOSED SYSTEM DESIGN

Data hiding techniques have been widely used to transmit of hiding secret messages for long time. Ensuring data security is a main challenge for computer users. Businessmen, professionals, and home users may have some important data that they want to secure from others. Steganography technique is quite useful to frustrate opponent attacks from unauthorized access. As a result, the proposed system is developed data hiding in image process using bit-plane complexity segmentation algorithm as shown in Figure 1.

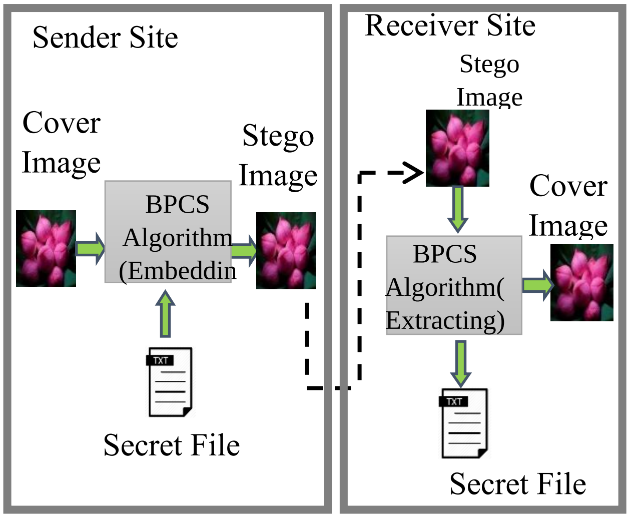

Figure 1. Proposed System Design

The proposed system is demonstrated with two portions: sender site and receiver site. At the sender site, the original text message is embedded into the image file using BPCS embedding technique without deteriorating the image quality. Then, the sender gets the stego image file to send the receiver over the internet. At the receiver site, the receiver receives the stegoimage file from the sender. Then it is extracted the secret message (secret file) from the stegoimage file by using BPCS extracting technique to get the original secret message. There are five steps to embed the text message as illustrated in Figure 4.2. These steps are as follows:

- Choosing the secret text message (.txt) file
- Choosing the cover image (.png) file
- Embedding the message in secret file (text file) into the cover image file by using BPCS insertion algorithm
- Getting the stegoimage (.png) file
- Showing the histogram

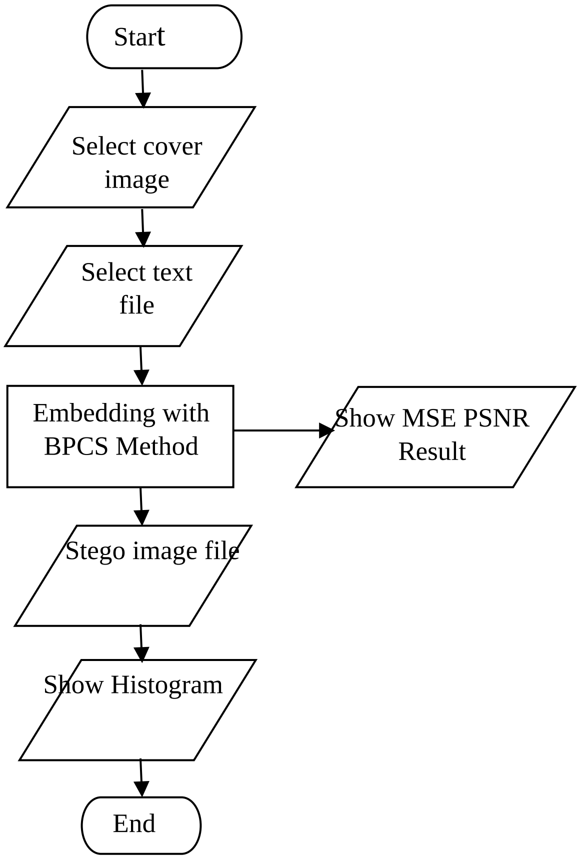

Figure 2. Flow Chart Of Embedding Process

The second one is extracted secret message from a stego image. Here, stego image file always save as appout.png. There are three steps to extract the original secret message (secret text file). Figure 4.2 shows system flow diagram for data extracting process.

- Choosing the stegoimage (.png) file
- Extracting the secret message fromstego image file by using BPCSextractiontechnique and Getting the original text message

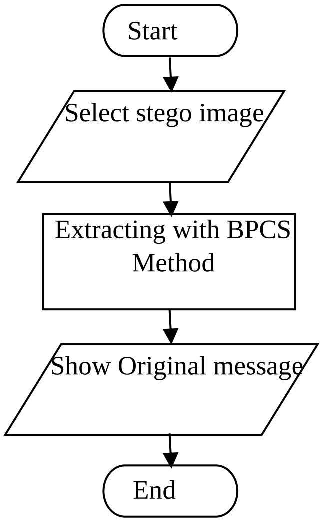

Figure 3. Flow Chart of Extraction Process

5.PERFORMANCE ANALYSIS

Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) value is also calculated and displayed under embedding process. The MSE is calculated as the following equation.

$$\text{MSE}=\frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy}-C_{xy})^2$$

$$\text{PSNR}=20\log_{10}\left(\frac{C_{\max}^2}{\sqrt{MSE}}\right)$$

It shows how close the vessel image compared to the original image. The closer the distance, the better the result.MSE and PSNR values with various secret text file size are shown as in Figure 4.

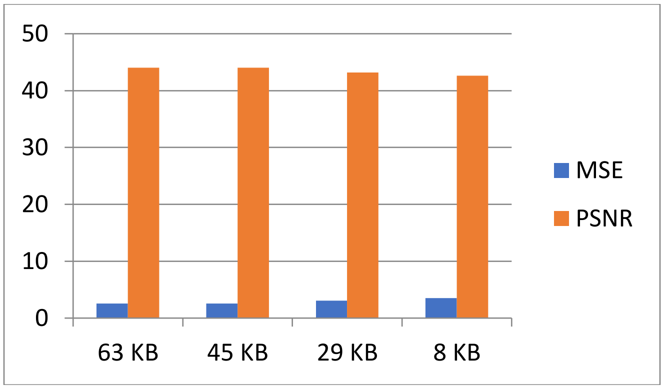

Figure 4. Comparison Result of MSE and PSNR Values with Same Size of Cover Image and Different Size of Secret Messages

The proposed system uses the steganographic technique to obtain the security of data. Embedding and extracting are the principal tasks of this proposed system. it is concluded that the BPCS technique has high data embedding capacity as 50–60%. Also, it is seen that the original image and the final embedded image appear to be identical to the human eye. This experiment has been carried on .png images.

6. CONCLUSION

The proposed system focuses on basic Steganography and various characteristics necessary for data hiding. The main contribution of this work is to develop BPCS algorithm that provides the concealing the existence of the data within the color vessel image. The proposed system is implemented by using python programming language. It is shown that the final embedded image with BPCS algorithm seems to be the same as the original image and locates noise-like regions in a cover image more exactly. In the system, image histograms are analyzed to identify the embedding capacity of different types. According to the histogram distribution, the proposed system showed that the embedding capacity is not only affected the host image quality but also the image size.

REFERENCES

Article/ Research Paper

[1] Surabhi, A.: A Review on Improving Data Security Using BPCS Steganography, International Journal of Innovative Research in Computer and Communication Engineering,Vol. 4, Issue 12, December (2016).

[2] Cheddad, J. et al.: Digital imag steganography: survey and analysis of current methods, Signal Processing, vol. 90, pp.727-752 (2010).

[3] Gandharba, S. and Kumar, S. L.:Classification of Image Steganography Techniques in Spatial Domain: A Study, International Journal of Computer Science & Engineering Technology (IJCSET),ISSN: 2229-3345 Vol. 5 No. 03 March(2014).

[5] Walton,S.: "Image Authentication for a Slippery New Age", Dr. Dobb's Journal of Software Tools, 20(4) (1995) 18-26.

[8] Kalavathi, A. and Ramineni, S. R. P.:A New Approach to Telugu Text Steganography, IEEE Symposium on Wireless Technology and Applications, p 25-28, 2011

[9] M.Bhavani and S.Vinod kumar, "A Data Mining Approach For Precise Diagnosis of Dengue Fever", International Journal of Latest Trends in Engineering and Technology, Vol (7), Issue(4), pp.352-359, nov 2016, DOI: http://dx.doi.org/10.21172/1.74.048

[10] Kawaguchi, E., Michiharu, N.: Modeling Digital Image into Informative and Noise-Like Regions by Complexity Measure, Information Modeling &Knowledge Bases IX,lOS Press, pp.255-265, April, (1998).

Books

[1] Morkel et al.: An Overviewof Image Steganography, Fifth Annual Information Security South Africa Conference(ISSA2005), Sandton, South Africa, July (2005).

[2] Jaewon, Y. et al.: Digital Steganography Hiding data within data, Oregon State University, (2007).

[3] Eiji, K and Richard, O. E.:Principle and Applications of BPCSSteganography, SPIE's International Symposium on Voice, Video and Data Communications, (1998).