ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 3, March 2012

Improved BPCS Steganography Based Novel Approach for Data Embedding

Pradnya R. Rudramath, M. R. Madki

***Abstract*— Bit-Plane Complexity Segmentation (BPCS) steganography uses an image as the vessel data and secret information is embedded in the bit-planes of the vessel. 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. All the "noise-like" regions in the bit-planes of the vessel image are replaced with secret data without deteriorating the image quality.**

***Index Terms*—BPCS, Steganography, Data Hiding, Information Hiding, Vessel image, Compression, Bit planes.**

I. Introduction

Internet communication has become an integral part of the infrastructure of today's world. The information communicated comes in numerous forms and is used in many applications. In a large number of these applications, it is desired that the communication be done in secrete. Such secret communication ranges from the obvious cases of bank transfers, corporate communications, and credit card purchases, on down to a large percentage of everyday email. With email, many people wrongly assume that their communication is safe because it is just a small piece of an enormous amount of data being sent worldwide. After all, who is going to see it? But in reality, the Internet is not a secure medium, and there are programs "out there" which just sit and watch messages go by for interesting information. Furthermore, in many cases it is desirable to send information without anyone even noticing that information has been sent. Steganography is the ancient art of embedding a secret message into a seemingly harmless message. Most of the newer applications use steganography like a watermark, to protect a copy right on information. In many cases it is desirable to send information without anyone even noticing that information has been sent.

All of the traditional steganographic techniques have limited information-hiding capacity. They can hide only 10% (or less) of the data amounts of the vessel. 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 multi valued image with the secret information. A new BPCS steganography uses an image as the vessel data, and embed secret information in the bit-planes of the vessel [1]. The information hiding capacity of a true color image is around 50%. All the "noise-like" regions in the bit-planes can be replaced with of the vessel image with secret data without deteriorating the image quality, which is termed as "BPCS-Steganography". This system is used to produce same quality of image while compressing and embedding the image, there will be no change in the quality of image and can be retained the same as the first. By using BPCS (Bit Plane Complexity Segmentation) the embedding process has been done here, so the security is very high for the embedded image.

Digital images are categorized as either binary (black-and-white) or multi-valued pictures despite their actual color. We can decompose an n-bit image into a set of n binary images by bit-slicing operations [2] [3]. Therefore, binary image analysis is essential to all digital image processing. Bit slicing is not necessarily the best in the Pure-Binary Coding system (PBC), but in some cases the Canonical Gray Coding system (CGC) is much better [4].

II. BPCS Steganography

Bit-Plane Complexity Segmentation Steganography is a new steganographic technique, which has a large information hiding capacity. The replacement of the complex regions in each bit-plane of a color image with random binary patterns is invisible to the human eye. This property can be used for information hiding (embedding) strategy. For a true 24-bit bitmap image, each of the RGB components takes one byte of memory. Each RGB component value ranges from zero 0 to 255, where zero represents darkest shade of the color and 255 represent brightest shade of this color. All other colors can be generated with the combinations of these ranges. A 4x4 sample image is given below Fig.1.

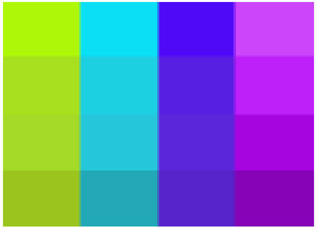
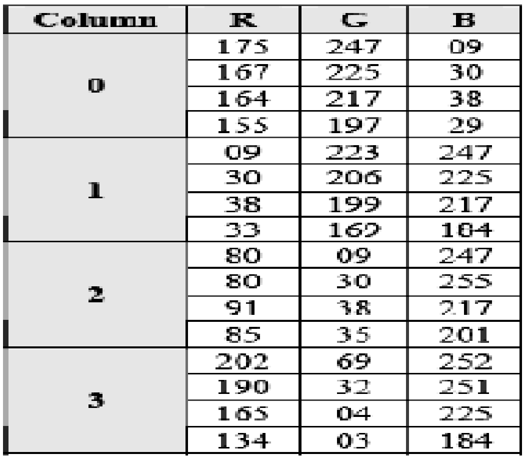


Fig. 1: Test image (4x4)

TABLE I: RGB values



Column	R	G	B
0	175	247	09
	167	225	30
	164	217	38
	155	197	29
1	09	223	247
	30	206	225
	38	199	217
	33	162	104
2	80	09	247
	80	30	255
	91	38	217
	85	35	201
3	202	69	252
	190	32	251
	165	04	225
	134	03	184

This image has total 16 pixels and each pixel has three components having one-byte for each component, therefore the total size of the image is 48 bytes. Each pixel is a combination of red, green and blue values. Their integer values are given in Table I.

A. BPCS Data Hiding

1. Bit plane decomposition.
2. Block segmentation.
3. Complexity measurement of each block.
4. Complexity measurement of secret message.
5. Replace complex image-data block to message block.

i) Bit plane decomposition

Alternatively the value of each RGB component can be represented in binary format as shown the Table II.

TABLE II: Binary representation of RGB values

Pixel	R	G	B
0	10101111	11110111	00001001
	10100111	11100001	00011110
	10100100	11011001	00100110
	10011011	11000101	00011101
1	00000001	11011111	11110111
	00011110	11001110	11100001
	00100110	11000111	11011001
	00100001	10101001	10111000
2	01010000	00001001	11110111
	01010000	00011110	11100001
	01011011	01011011	11011001
	01010101	00100011	11001001
3	11001010	01000101	11111100
	10111110	00100000	11111011
	10100101	00000100	11100001
	10000110	00000011	10111000

Following steps are followed for the constructions of the binary planes.

Step1: Formation of Channel Matrix:

The selected channel (R in this case) is picked from all the pixels of the image. The channel matrix contains the N elements where N is the total number of pixels in the image.

TABLE III: 'R' Channel matrix

R0	R1	R2	R3
10101111	00000001	01010000	11001010
10100111	00011110	01010000	10111110
10100100	00100110	01011011	10100101
10011011	00100001	01010101	10000110

Step 2: Get Corresponding Bits:

In next step get the corresponding *ith* bits from each of the channel to construct a plane. These bits are picked out using the same sequence in which the channel itself is allocated in the image. The height and width of a binary plane (as there are only 1's and 0's in plane) is the same as the height and width of the original image (4x4). Using this fact total number of bits in any of the plane can be easily calculated.

Step 3: Formation of 'N' Binary Planes:

Applying the same procedure described in the step 2, the following N planes are constructed. N is the number of bits per RGB component.

TABLE IV: Planes extracted from 'R' channel

Plane 1				Plane 2			
1	0	0	1	0	0	1	1
1	0	0	1	0	0	1	0
1	0	0	1	0	0	0	0
1	0	0	1	0	0	1	0
Plane 3				**Plane 4**			
1	0	0	0	0	0	1	0
1	0	0	1	0	1	1	1
1	1	1	1	0	0	0	0
0	0	1	0	1	0	1	0
Plane 5				**Plane 6**			
1	1	0	1	1	0	0	0
0	1	0	1	1	1	0	1
0	0	1	0	1	1	0	1
1	0	0	0	0	0	1	1
Plane 7				**Plane 8**			
1	0	0	1	1	1	0	0
1	1	0	1	1	0	0	0
0	1	1	0	0	0	1	1
1	0	0	1	1	1	1	0

Binary pixel blocks that form bit-planes are as shown in Fig.2.

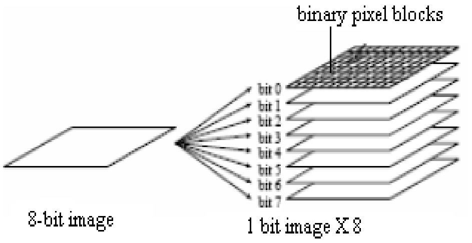


Fig. 2: Binary pixel blocks on bit-planes

i) Block segmentation

Each bit plane is segmented to blocks of 8x8 binary data.

ii) Complexity measurement of each block

In this work the method of steganography makes use of the more complex regions of an image to embed data. There is no standard definition of image complexity. A black and white border is adopted for image complexity. A maximum value from 0 to 1 is defined in each channel. The planes having complexity value less are considered informative and planes having more complexity than threshold are considered noisy. Now planes can be replaced with message to be embedded in the image. The threshold value to determine if a block is complex or not is given by

$$Th = 0.3\ Cmax,$$

Where Cmax is the maximum complexity value in each channel.

iii) Complexity measurement of secret message

Each 8 letters form a block of message, and complexity measurement is applied to each message block.

iv) Conjugation of a binary image

Let P be an 8X8 size black-and-white image with black as the foreground area and white as the background area. Two checkerboard patterns are introduced viz. Wc and Bc, where

Wc has a white pixel at the upper-left position, and Bc is its complement, i.e., the upper-left pixel is black. Regard black and white pixels as having a logical value of “1” and “0”, respectively.

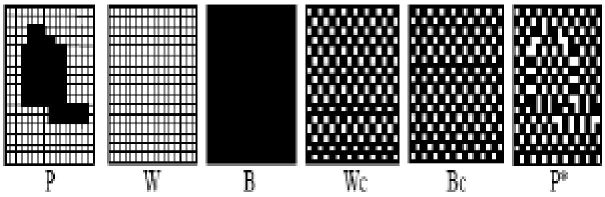


Fig. 3: Illustration of each binary pattern

P is interpreted as follows. Pixels in the foreground area have the B pattern, while pixels in the background area have the W pattern. Now we define P* as the conjugate of P. The most important property about conjugation is the following.

Let α(P) be the complexity of a given image P, then

α (P*) = 1- α (P).

The complexity value of P* is always symmetrical against P regarding α = 0.5.

For example, if P has a complexity of 0.7, then P* has a complexity of 0.3.

v) Replace complex image-data block to message block

All complex image-data blocks determined by step 3 are replaced by message blocks.

B. BPCS hidden data extraction process

1. Bit plane decomposition.
2. Block segmentation.
3. Complexity measurement of each block.
4. Conjugation map extraction:
    - The first complex blocks are corresponded to the conjugation map.
5. Hidden data extraction :
    - The complex blocks are extracted and conjugated if necessary to recover the secret message.

C. Embedding

1. Transformed image is decomposed into bit-planes.
2. Each plane is segmented into 8X8 blocks and complexity is measured for each block.
3. Threshold value is chosen to determine whether the block is complex or non-complex.
4. Each 8 letters form a block of message, and complexity is measured for each message block.
5. If a massage block is determined as no-complex block, the message block is conjugated.
    i. Conjugation map is constructed from conjugated blocks.
    ii. Complex image blocks are replaced by message blocks.

D. Extracting

1. Transformed image is decomposed into bit planes.
2. Each plane is segmented into 8X8 blocks and complexity is measured for each block.
3. Threshold value is chosen to determine whether the block is complex or non-complex.
4. Secret message is extracted from the complex blocks; blocks are conjugated if necessary based on conjugation map information.

III. Analysis

This paper takes many simulations and tests to various standard gray images. The experiments choose peak-signal to-noise ratio (PSNR) as objective criteria of visual imperceptibility, the definition of PSNR as follow [6]:

$$\mathrm{PSNR}=20\lg\frac{255}{\sqrt{\frac{1}{n}\sum_{i=0}^{n-1}(I_i'-I_i)^2}}$$

Where I_i represents the pixels of carrier image, while I'_i represents the pixels of image that embedded secret. The greater the PSNR is, the better the fidelity is, and the similar the two images are.

IV. Applications

1. The more obvious applications of BPCS Steganography relate to secret communications.
2. In some applications, the presence of the embedded data may be known, but without the customization parameters, the data is inseparable from the image. In such cases, the image can be viewable by regular means, but the data is tied to the image and can't readily be replaced with other data. Others may know the data is there, but without the customization parameters, they cannot alter it and still make it readable by the customized software.
3. Applications of BPCS Steganography are not limited to those related to secrecy. For such applications, the presence of the embedded data may be known, and the software for extraction and embedding can be standardized to a common set of customization parameters. An example of this is a digital photo album, where information related to a photo, such as date and time taken, exposure parameters, and scene content, can be embedded in the photo itself.

V. Conclusion And Future Scope

The system is proposed to design a lossless steganography system, in which BPCS steganography is used to get high data hiding capacity and low perceptibility. BPCS takes the advantage of human visual system which cannot recognize changes in complex positions of the image.

The system can be further developed to hide secret image in cover image.

REFERENCES

[1] Eijji Kawagauch and Richard O. Eason “Principle and Application of BPCS-Steganography” in Proc. SPIE, vol. 3529, 1998, pp. 464-473.

[2] Hall, Ernest L., Computer Image Processing and Recognition, Academic Press, New York, 1979.

[3] Jain, Anil K., Fundamentals of Digital Image Processing, Prentice Hall, Englewood Cliffs, NJ, 1989.

[4] Kawaguchi, E., Endo, T. and Matsunaga, J., “Depth-first picture expression viewed from digital picture processing”, IEEE Trans. on PAMI, vol.5, no.4, pp.373-384, 1988.

[5] R. Schyndel, A. Tirkel and C. Os born, “A digital watermark”, in Proc. IEEE Int. Conf. Image Processing. 1994, vol. 2, pp. 86-90.

[6] Wu X, Xu X Y, Huang Y R. BPCS steganography algorithm against statistical analysis [J]. Computer Engineering Applications, 2007, 43(7): 52-54.