Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique

SHRIKANT S. KHAIRE

Department of Electronics & Telecommunication,
Dr. Babasaheb Ambedkar Technological University,
Lonere, Dist: Raigad, Maharashtra, India.

DR. SANJAY L. NALBALWAR

Department of Electronics & Telecommunication,
Dr. Babasaheb Ambedkar Technological University,
Lonere, Dist: Raigad, Maharashtra, India.

Abstract:

Steganography is an ancient technique of data hiding. Steganography is a technique in which secret data is hidden into vessel image without any suspicion. All other traditional techniques have limited data hiding capacity and can hide up to 15% of data amount of vessel image. This paper focuses on basic steganography and various characteristics necessary for data hiding. More importantly, the paper implements a steganographic technique that has hiding capacity up to 50 – 60% [8] [9]. This technique is called Bit Plane Complexity Segmentation (BPCS) Steganography. 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. In our experiment, we used the BPCS Principle by "Eiji Kawaguchi & Richard O. Eason" and experimented by using two images i) vessel image of 512 x 512 size ii) secret image of 256 x 256 size. We performed this experiment for 3 different sets of images and calculated image hiding capacity.

Keywords: Information hiding, Steganography, Cryptography, Encryption, Bit plane slicing, complexity, conjugation.

1. INTRODUCTION

Steganography is basically stega + nography. 'Stega' means 'covered' coming from the Greek word "stegos" and 'nography' means 'writing' coming from the Greek word "graphia". Thus, Steganography means covered writing [1]. Steganography is an ancient art of conveying messages in a secret way such that only the receiver knows the presence of the message. The message is hidden in another media such that the transmitted media appears meaningful to the attacker. If the hidden message is extracted the steganography technique fails [5]. Steganographic technique allows one party to communicate with another party without third party being aware that communication is occurring [2] [7]. Steganography is the method of encoding secret data such that the existence of the information is concealed. Usually, the data is concealed inside an innocuous cover such that even if hostile agents discover the cover, there is no suspicions about the presence of data in that cover [3]. Steganography and Cryptography are cousins in the spy craft family [1]. However, Cryptographic & Steganographic technique differs from each other. In cryptography, the original message is scrambled i.e. its original structure is changed in order to make it meaningless [3]. Thus, when an attacker discovers the message it is still difficult for him to get the original message back. Cryptography does not try to hide the message. In steganography, the message is secretly hidden inside an image or audio/video file. Thus there arises no suspicion to the attacker. Steganography does not attempt to scramble the original message. The intention of both steganography & cryptography is to protect the original

message from the attacker. Both are excellent means, but when used alone can be broken. As a result, several experts have suggested the idea of using both the techniques in order to provide additional layer of security. Cryptographic technique encrypts the original message. This encrypted message is then hidden using steganographic technique. Now, even if attacker defeats the steganographic technique, he still requires cryptographic decoding key to decipher the encrypted message [3] [4].

1.1. *Different Steganographic Protocols:*

There are basically three types of steganographic protocols:
1) Pure – key steganography: In this model, there requires no exchange of stego – key. This method is the simplest but is the most unsecured means to communicate secretly.
2) Secret – key steganography: In this model, both the sender and the receiver shares common secret – key before conveying messages [4].
3) Public – key steganography: In this model, two keys are required; one is public key and the other is private key. The public key is used for embedding message while the private key is used for extracting message [4].

2. Basic Steganography Model

A basic steganographic model is shown in Figure 1. The message 'M' is the secret data that the Sender wishes to hide without any suspicion. The secret data can be audio, video, image, text. The cover 'X' is the original image, audio file, video file, in which the secret message 'M' is to be embedded. The cover 'X' is also called as "Message Wrapper". It is not necessary that the cover 'X' and the message 'M' should have homogeneous structure. For example, text message or an audio file can also be hidden into video or image. In this paper both the cover 'X' and Message 'M' are images.

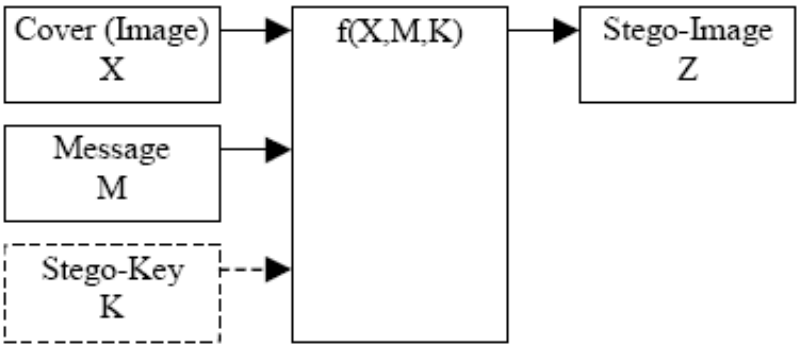


Figure 1: Basic digital Steganography Encoder

Stego – Image 'Z' is basically the image in which the secret image 'M' is embedded. It should be ensured that at any point, the stego-image should resemble the cover image else it will cause suspicion. Stego-key 'Z' is provided to the receiver so that only he can be able to extract the secret image from the cover image [3].

3. Characteristics of Steganographic techniques

In steganography, the message that is to be hidden inside the cover – media must consider the following features.
Hiding Capacity: This feature deals with the size of information that can be hidden inside the cover. A larger hiding capacity allows use of small cover and thus reduces the band-width required to transmit the stego – media [3].
Perceptual Transparency: Perceptual transparency is an important feature of steganography. Each cover – media has certain information hiding capacity. If more information or data is hidden inside the cover, then it results in degradation of cover – media. As a result, the stego – media and cover – media appear to be

different. Thus, if the attacker notices this distortion, then our steganographic technique fails and then there is every possibility that our original message can be extracted or damaged by the attacker [3].

Robustness: Robustness is the ability of the hidden message to remain undamaged even if the stego – media undergoes transformation, sharpening, linear & non-linear filtering, scaling & blurring, cropping and various other techniques [3].

Tamper – resistance: Of all the features, this feature is very important. This is because, if the attacker is successful in destroying the steganographic technique then the tamper – resistance property makes it difficult for the attacker or pirates to alter or damage the original data. Thus, various applications of steganography must ensure that the above features are satisfied. For e.g. copy – right protection must ensure better perceptual transparency, robustness & tamper – resistance so that the integrity of the original work is maintained [3].

4. Data embedding Technique – BPCS (Bit Plane Complexity Segmentation) steganography:

4.1. *Introduction*

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason, to overcome the short comings of traditional steganographic techniques such as Least Significant Bit (LSB) technique, Transform embedding technique, Perceptual masking technique. This traditional technique has limited data hiding capacity and they can hide up to 10 – 15% of the vessel data amount. 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 [8] [9]. In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits [7]. But in BPCS technique, data is hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region [8].

4.2. *Basic Principle of 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 [9] [10].

4.3. *Concept of Gray Scale Image*

Gray scale digital image is an image in which the value of each pixel is a single sample i.e. it carries only intensity information. Images of this type are also known as black and white image and are composed exclusively of shades of gray varying from black at the weakest i.e. '0' intensity to white at the strongest intensity '1'. Gray scale image is mostly preferred because less information needs to be provided for each pixel. Often the gray scale intensity is stored as an 8 – bit integer giving 256 possible different gray shades from black to white.

4.4. *CGC is preferred over PBC in BPCS*

The main goal of BPCS Steganography is to make use of as much capacity of image for data hiding without much distortion in the visual appearance of the original image. Pure Binary Coding (PBC) bit planes provides much greater region for embedding. But PBC suffers from "Hamming cliff", wherein a small change in color affects many bits of color value [8]. This can be better explained with the help of example. Consider in an 8 – bit image, there are two consecutive pixels having intensity values 127 and 128 respectively. In PBC, 127 is represented as 01111111 and 128 is represented as 10000000. Both the pixels appear identical to human eye but differ greatly in bit representation. This is called "Hamming Cliff" concept. If secret data is embedded, then there is every possibility that 01111111 can become 11111111

and 10000000 can become 00000000. Previously, there was a difference of one gray level which was negligible to human eye. Now, after embedding, the difference in gray level is that of 255 i.e. one pixel appears dark black while other pixel appears pure white. This change is easily noticeable to human eye. This drawback is avoided by Canonical Gray Coding (CGC) technique. In CGC, gray coding technique is used. Thus, 127 which is represented in binary form as 01111111 now by using gray code technique, where ex-oring of bits is done, is represented as 01000000 in CGC [12]. Similarly, 128 is represented in CGC as 11000000. Now, the two pixels appear similar, but differ only by one bit. This was exactly opposite to PBC. Thus, CGC does not suffer from "Hamming Cliff" [8]. After embedding, 01000000 can possibly become 11000000 and 11000000 can possibly become 01000000. Thus, both the pixels differ in intensity level which is unnoticeable. Hence, CGC is preferred over PBC in BPCS system [8] [12].

4.5. *Bit Plane Slicing Concept in BPCS*

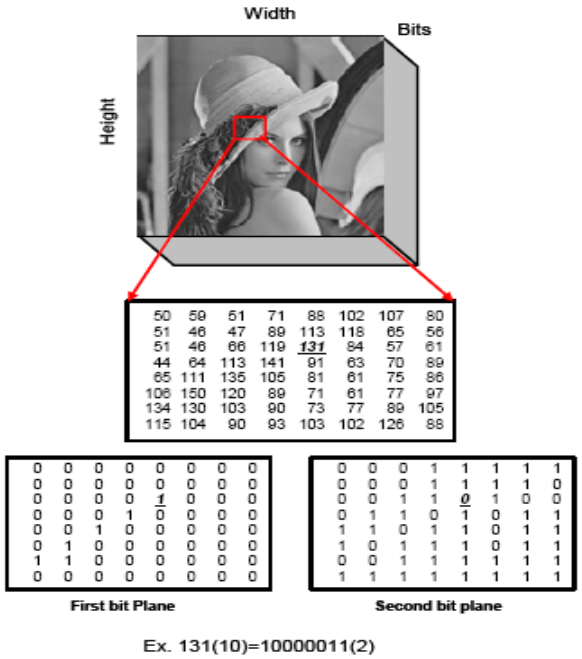


Figure 2: Bit Plane Slicing concept considering pixel having value 131.

The bit plane slicing can be better understood with the help of figure 2 [13]. The operation of splitting the image into its constituent binary planes is called "Bit plane slicing". Pixels are digital numbers composed of bits. In an 8-bit image, intensity of each pixel is represented by 8-bits. The 8-bit image is composed of eight 1-bit plane regions from bit plane '0' (LSB) to bit-plane '7' (MSB). Plane '0' contains all lowest order bits of all pixels in the image while plane '7' contains all higher order bits. Bit plane Slicing is useful for image compression. Complexity of each bit–plane pattern increases monotically from MSB to LSB [11].

4.6. *Complexity measure for Binary image*

The important step in BPCS steganography is to find "complex" region in the vessel image so that data from secret image can be hidden without any suspicion. Also there is no standard definition of complexity. There are basically three methods of complexity measure [12]. However, in our experiment and in this paper we focus on complexity measure based on length of black and white border in binary image. The total length of black and white border is equal to the summation of the number of color changes along the rows and columns in an image [8] [9].
Consider the following example.

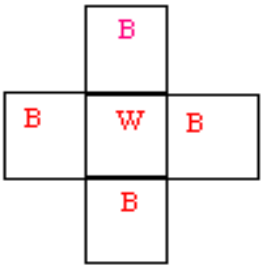
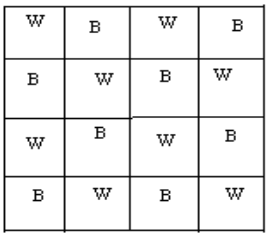


Figure 3: single white pixel surrounded by four black pixels

In figure 3, a single white pixel is surrounded by 4 black pixels. Thus we observe that, there are in total 4 color changes. Thus the total length of border is 4 [8].

Figure 4: (a) all white pixels in image



(b) black-white checker board

In figure 4(a), there are all white pixels. As a result there is no color change along the rows and columns. Hence, total border length is zero. Thus the minimum border length is zero. In figure 4(b), there are alternate white and black pixels i.e. checker board image. Visually, the total color change along rows and columns is 24. This can be also calculated with the help of formulae. The equation for maximum length of the border for (2^m x 2^m) binary image is given by 2*2^m*(2^m-1). Thus, in case of figure 4(b), it is a 4 x 4 binary image, m = 2. By using the formulae, we get the maximum length for figure 4(b) as 24.
The image complexity is denoted by 'α' and is given by

$$\alpha = \frac{k}{2 \times 2^m \times (2^m - 1)}$$

where 'k' is the total length of border in an image and α ranges between 0 and 1 [8] [9].

4.7. *Conjugation operation on binary image*

Binary image consists of informative and noise-like regions. Informative patterns are simple while complex regions are complex. If secret data is noise-like then it is directly embedded in noise-like regions of the vessel image. If secret data is informative then it has to undergo conjugation operation in order to transform it to complex pattern [8].

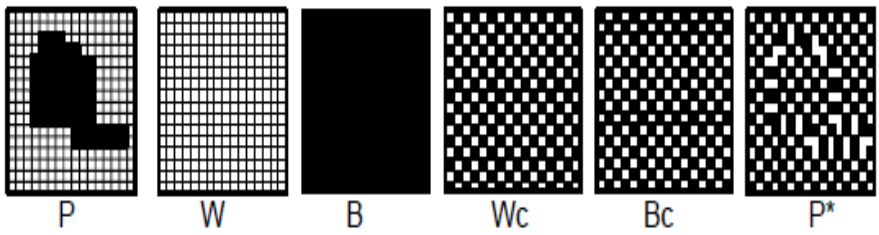


Figure 5: Illustration of Conjugation operation

Figure 5 illustrates the concept of Conjugation operation. We define P* as conjugate of P which satisfies:
1) Foreground area shape is the same as P.
2) Foreground area has Bc pattern.

3) Background area has Wc pattern.
One of the important property of conjugation is α (P*) = 1 – α (P) i.e. if complexity of P is 0.6 which is informative pattern then complexity of P* is 0.4 which is complex pattern [8] [9].

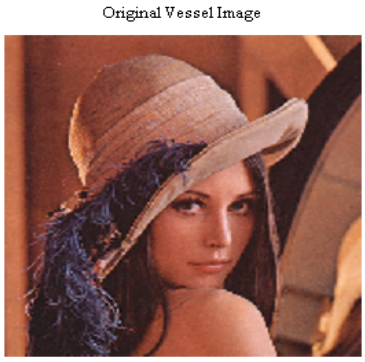
5. Proposed BPCS Steganography Algorithm

a) Consider a color image as vessel image. Make the size of image as 512 x 512.
b) Convert the vessel image to gray scale image.
c) Consider a gray scale secret image and make the size of image as 256 x 256.
d) Convert the vessel image and the secret image which are in pure binary Code (PBC) form into Canonical Gray Code (CGC) form.
e) Perform bit plane slicing on vessel image as well as on secret image.
f) Calculate complexity measure 'alpha' (α) for each block of each bit plane of vessel image.
g) Calculate α for each block of each bit plane of secret image.
h) Perform conjugation operation on the 'simple' or 'informative' blocks of the secret image.
i) Perform embedding operation to embed secret image in vessel image.
j) Convert the CGC form embedded image to PBC image [8] [9].

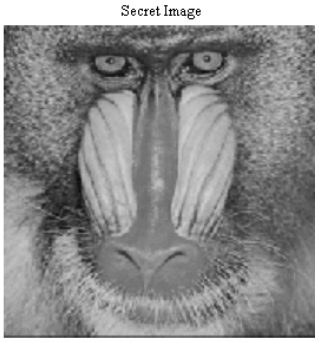
6. Results and Discussion

In accordance with the "Principle and Applications of BPCS Steganography" by Eiji Kawaguchi and Richard O. Eason, we performed the experiment by using MATLAB software and the results are below:

6.1. *Result for vessel "Lena" & secret "Baboon"*

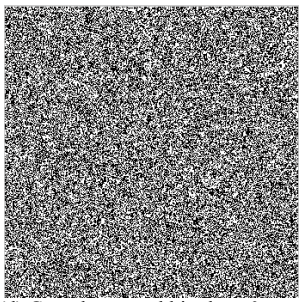


(a) Original image 512x512



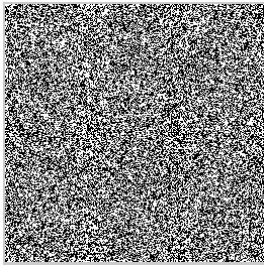
(b) secret image 256x256


(c) Vessel image in gray code


(d) Complex vessel bit plane 0


(e) Complex vessel bit plane 3


(f) Complex vessel bit plane 7


(g) Complex secret bit plane 0

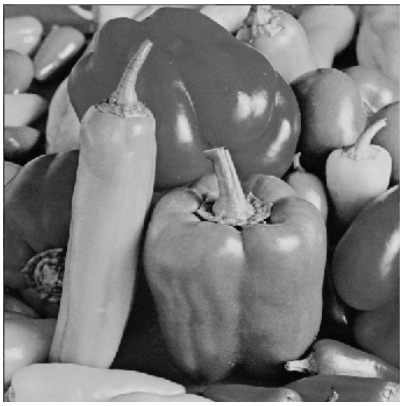

(h) Complex secret bit plane 3


(i) Complex secret bit plane 7

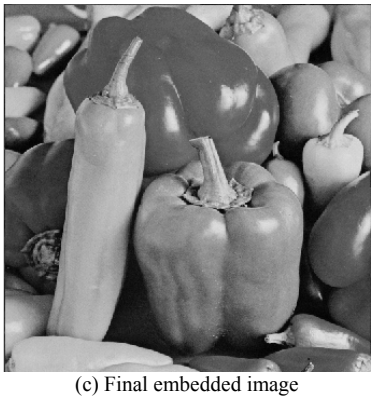

(j) final embedded images

Figure (a) to (j) was obtained. Figure (a) is the original vessel image and figure (j) is the image in which secret image is hidden.

6.2. *Result for vessel "Pepper" & secret "Couple"*


(a) Original image 512 x 512


(b) secret image 256 x 256

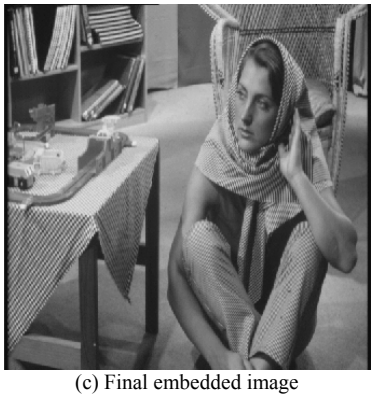


(c) Final embedded image

6.3. *Result for vessel "Barbara" & secret "airplane*

(a) Original image

(b) secret image



(c) Final embedded image

6.4. ***The table showing the details of embedding capacity***

Image	Std dev. 'σ' & complexity 'α' where A = 0.5 – 4 σ	Max. embeddable blocks	Total embedded Blocks	% of max. hiding capacity
Lena & Baboon	σ = 0.0529 α = 0.2884	15487	8192	52.89%
Pepper & couple	σ = 0.0476 α = 0.3096	15710	8192	52.10 %
Barbara & airplane	σ = 0.0652 α = 0.2392	16677	8192	49.12 %

Thus from the table it is seen that, the maximum embedding capacity ranges from 49 % to 52 % which is higher when compared to traditional steganography techniques.

7. Conclusion and Future work

Thus, from the experiment for three different sets of images, it is concluded that the BPCS technique has high data embedding capacity in the range 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 bitmap images. We can now experiment on other types of image like jpeg, tiff etc. and check the results. In this experiment, we used complexity technique based on length of black & white border. In future work, we can experiment using different complexity techniques and compare them based on the results obtained [12].

REFERENCES

[1] N. Johnson and S. Jajodia, (Feb 1998): Exploring steganography: seeing the unseen, IEEE Computer, pp.26-34
[2] A.Habes, (Feb 2006): Information Hiding in BMP image Implementation, Analysis and Evaluation, Information Transmission in Computer Networks.
[3] E. T. Lin and E. J. Delp: A Review of Data Hiding in Digital Images, Video and Image Processing Laboratory, Indiana.
[4] S.G.K.D.N. Samaratunge, (August 2007): New Steganography Technique for Palette Based Images, Second International Conference on Industrial and Information Systems, ICIIS 2007.
[5] Yeaun-Keun Lee and Ling-hwei Chen: Secure Error-Free Steganography for JPEG Images.
[6] R.J. Anderson, F.A.P. Peticolas, (May 1998): On the Limits of Steganography, IEEE Journal of Selected Areas in communication.
[7] A. Habes, (Dec 2005): 4 Least Significant Bits information Hiding Implementation and Analysis, GVIP 05 Conference, CICC, Cairo, Egypt.
[8] Eiji Kawaguchi, Richard O. Eason: Principle and applications of BPCS – Steganography.
[9] Michiharu Niimi, Hideki Noda and Eiji Kawguchi, (1997): An image embedding in image by a complexity based region segmentation method - 1997 IEEE.
[10] KIT Steganography Research Group: Principle of BPCS Steganography, Japan.
[11] Rafael C. Gonzalez, Richard E. Woods: Digital Image Processing, Third Edition, Pearson Education, pp. 117 – 119.
[12] Hioki Hirohisa: A Data Embedding method using BPCS principle with new Complexity measures.
[13] ENEE408G Multimedia Signal Processing (fall '03) – Overview of MATLAB Programming.