

Increasing Data Hiding Capacity of Carrier Image Using BPCS Steganography

Vaishali¹, Abhishek Kajal²

¹ M.Tech Student, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, India

² Assistant Professor, Department of Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar, India

Abstract: *Steganography means secret writing. It is an ancient technology that hides the data or information in such a way that nobody can see the hidden message or even its existence can't be predicted. There are several techniques of data hiding like text, audio, image, video etc but all these techniques have limited amount of data hiding capacity. Bit Plane Complexity Segmentation (BPCS) Steganography is a technique that provides near 50% of data hiding capacity. In this technique data is hidden into the bit planes of the cover image. This technique is based on the characteristics of human vision system (HVS) in which a human can't see any information in more complex blocks/binary patterns, So that all the complex blocks/binary patterns are replaced by secret data. The main aim of this paper is to provide an introduction to BPCS Steganography and the techniques that can be used to increase the data hiding capacity of BPCS Steganography.*

Keywords: Steganography, Information Hiding, Bit Planes, Cover Image, Secret image, BPCS

1. Introduction

Steganography is the art of hiding information in ways that prevent the detection of hidden messages [3]. Steganography derived from Greek word “steganographia”, which means “covered writing”. In cryptography data is unreadable by a third party but the goal of steganography is to hide the data from third party. In steganography, the cover carriers are innocent looking carriers (images, audio, video, text) which will hold the hidden information [1]. A message is the information hidden and it may be images, plaintext, cipher text, or anything that can be embedded into a bit stream. The cover medium and the embedded message create a stego medium. Data embedding may require a stego key which is additional secret information, such as a password. A possible formula of the process may be represented as [1]:

Cover Medium + Embedded Message + Stego-Key = Stego-Medium [1]

Images are the most popular cover objects used for steganography. Image steganography, image is used as a cover object. In this technique pixel intensities are used to hide the information [6]. In image Steganography, secret message is embedded into cover image (used as the carrier to embed message into) and a stego-image (generated image which is carrying a hidden message) is generated. Block diagram of image steganography is shown in figure 1 without stego-key. Embedding algorithm required a cover image with secret message for embedding. Output of embedding algorithm is a stego-image which simply sent to extracting algorithm, where extracted algorithm un-hides the secret message from stego-image.

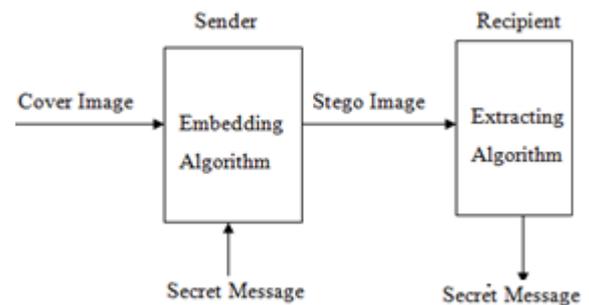


Figure 1: Image Steganography

Image Steganography Classifications

Generally Image steganography is categorized in following aspects and Table-1 shows the best steganography measures [6]:

- **High Capacity:** Maximum size of information can be embedded into image.
- **Perceptual Transparency:** After information hiding into cover image, perceptual quality of stego-image will be degraded as compare to cover-image.
- **Robustness:** After embedding, data should stay intact if stego-image goes into some transformation.
- **Temper Resistance:** It should be difficult to alter the message once it has been embedded into stego-image.
- **Computation Complexity:** Computationally how much expensive it is for embedding and extracting a hidden message?

Table 1: Image Steganography Measures [6]

Measures	Advantage	Disadvantage
High Capacity	High	Low
Perceptual Transparency	High	Low
Robustness	High	Low
Temper Resistance	High	Low
Computation Complexity	Low	High

Image Steganographic Techniques: Image steganography techniques can be divided into two groups:

- **The Image Domain:** Also known as spatial domain technique [5], embed messages in the intensity of the pixels directly. Least significant bit (LSB)-based steganography is the simplest technique that hides secret data in the LSBs of pixel values without introducing any distortion.
- **The Transform Domain:** Also known as frequency domain [5]. In this, images are first transformed and then the message is embedded in the image. Transform domain techniques have an advantage over spatial domain techniques as they hide information in areas of the image that are less exposed to transformation such as compression, cropping or image processing.

2. Bit-Plane Complexity Segmentation Steganography

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason [19]. In traditional techniques data hiding capacity of carrier is limited. They can hide only 10 – 15 % of the carrier data amount. BPCS overcome the short coming of traditional steganography techniques by replacing secret data block with complex binary patterns of bit planes of cover image. In BPCS technique data hides in MSB plane along with the LSB planes which provide more embedding capacity. The major idea of BPCS is that bit-planes of the cover images are divided into fixed-size blocks. This technique depends on the characteristics of the human vision system whereby a human cannot see any shape information in a very complex binary pattern; therefore, all complex binary patterns in the bit-planes of the cover image are replaced with secret data without destroying the image quality.

The advantages of BPCS steganography are [10]:

1. Information hiding capacity of color image is 50%.
2. Sharpening operation on the cover image increases the embedding capacity a bit.
3. Canonical Gray Coded (CGC) bit planes are more suitable for BPCS steganography than Pure Binary Coded (PBC) bit planes.
4. Data compression and encryption operation on secret data makes the embedded data more intangible.
5. Customization of a BPCS Steganography program for each user is easy.
6. It protects against eavesdropping on the embedded information.
7. It is most secured technique and provides high security.

Basic Principle of BPCS Steganography

The basic principle of BPCS steganography is that an image is first divided into its bit planes after that all bit planes are segmented into informative and noise like patterns. Informative patterns consist of simple information easily seen by human but noise like patterns are complex patterns that are used to hide information. Let B is an 8-bit grayscale image, therefore B= [B7 B6 B5 B4 B3 B2 B1 B0] are the bit planes of the image where B7 is the most significant bit plane and B0 is the least significant bit plane.

Image data is represented by pure binary coding (PBC) which provides greater data hiding capacity but it suffers from “Hamming cliff” [9] that’s why in BPCS steganography Canonical Gray Coding (CGC) is used.

Complexity measure for Binary image

The important step in BPCS steganography is to find “complex” pattern/region in the cover image so that secret image can be hidden without any suspicion. Basically, BPCS-steganography uses black-and-white border complexity method [10]. In this method, the length of the black-and-white border of a binary image is used as a good measure for image complexity. If the length of border is long, the image is more complex otherwise not. Total length of the black-and-white border equals to the summation of the number of color-changes along the row and columns in an image. We define the image complexity as

$$\alpha = \frac{k}{\text{The max. possible B - W pixel changes in image}}$$

Where, k is the total length of black-and-white border in the image and the value ranges over $0 \leq \alpha \leq 1$.

The eqⁿ for maximum length of the border for $(2^n \times 2^n)$ binary image is given by $2 * 2^n * (2^n - 1)$.

Thus, image complexity is also given by

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

Conjugation of a binary image

Binary image consists of noise like and informative regions. Informative regions are simple while noise like regions are complex. If secret data is noise-like then it is directly embedded in noise-like regions of the cover image. If secret data is informative then conjugation operation is used to transform it to complex pattern [9].

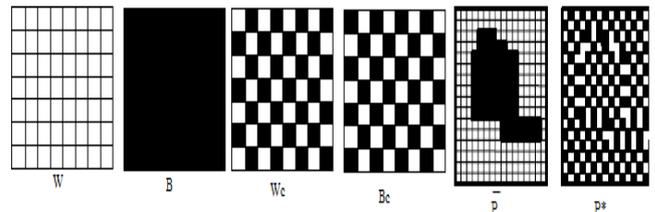


Figure 2: Each possible binary pattern (N=4) [10]

We define P* as the conjugate of P which satisfies:

1. The foreground area shape is the same as P.
2. The foreground area has the Bc pattern.
3. The background area has the Wc pattern.

Conjugation operation is kind of XOR operation of image with Wc and Bc. Correspondence between P and P* is one-to-one. There are certain property of P and P* as follow [10].

- 1) $P^* = P \oplus Wc$
- 2) $(P^*)^* = P$
- 3) $P^* \neq P$
- 4) $\alpha(P^*) = 1 - \alpha(P)$

BPCS Steganography Algorithm

The steps for embedding algorithm in BPCS-Steganography [10] are (Fig 3):

1. Transform the cover image from PBC to CGC system.
2. Segment each bit-plane of the cover image into informative and noise-like regions by using a threshold value (α_0). Typical value of threshold is $\alpha_0 = 0.3$.
3. Group the bytes of the secret file into a series of secret blocks.
4. If a block (S) is less complex than the threshold (α_0), then conjugate it to make it a more complex block (S*). The conjugated block must be more complex than α_0 .
5. Embed each secret block into the noise-like regions of the bit-planes. If any of the blocks is conjugated, then record these blocks in a "conjugation map."
6. Also embed the conjugation map as was done with the secret blocks.
7. Convert the embedded cover image from CGC back to PBC.

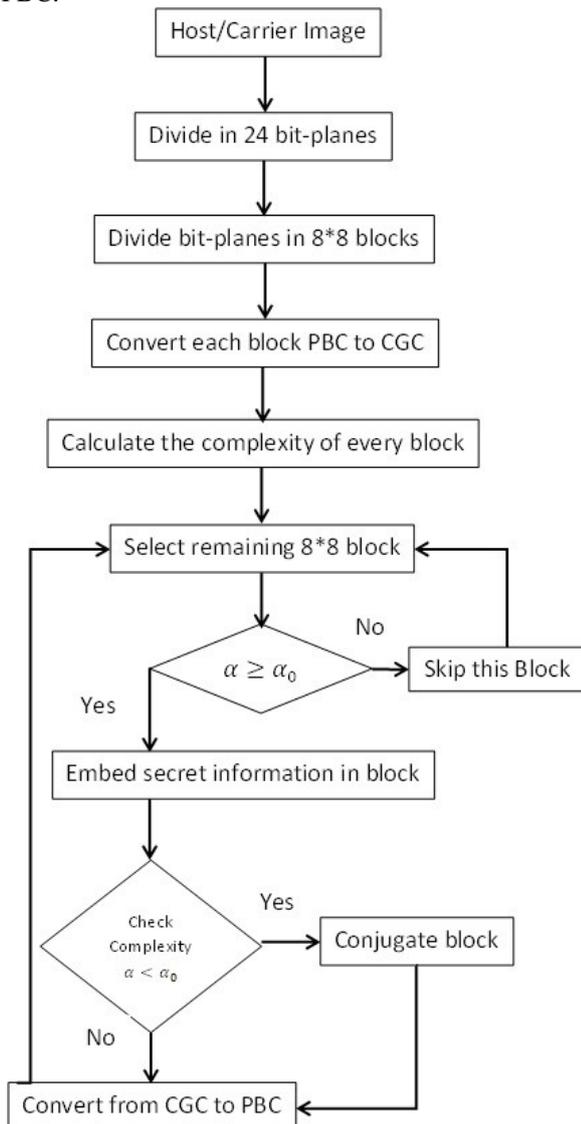


Figure 3: Flowchart- BPCS steganography [19]

The Decoding algorithm (i.e., the extracting operation of the secret information from an embedded cover image) is just the reverse procedure of the embedding steps.

3. Related Work

BPCS steganography provides 40% to 50% of data hiding capacity but there are several other techniques that can be

used to increase the data hiding capacity. The original BPCS algorithm divides the carrier image into bit-planes, and there is high correlation between the bit planes. So setting the same embedding strength for different bit-planes have an influence on the correlation between the bit-planes and leading to the abnormalities of the complexity histogram, consequently, affect the security of steganography.

[12] Describe improved bit-plane complexity segmentation (BPCS) steganography. The Improved bit-plane complexity segmentation (BPCS) steganography carries on different processing's to different bit-planes. It will set high threshold value at the high bit-plane and low threshold value at the low bit planes. Through different bit-planes using different embedding strength, it can realize that embedding less secret information in higher bit-planes to have good visual imperceptibility and embedding more in lower bit-planes to have high data embedding capacity. [12] Concretely designs and carries out a steganography of the text secret information. In this, for the encryption of the text secret information RSA algorithm is used. The introduction of chaos theory conveniences to the test of steganography characteristics and enhance the safe of steganography. It provides good visual imperceptibility and data embedding capacity.

Vipul J. Patel and Neha Ripal Soni [13] provide a proposed modified BPCS steganography that increase hiding capacity and enhance security. With the use of fix block size and insert information into all bit planes, hiding capacity of image is not utilized. Security issues can be solved by comparative replacement of message block during hiding process. Therefore, we investigated the variable block size at each bit planes that increases hiding capacity and comparative replacement which increases security. As a result, the proposed modified BPCS Steganography method increases the embedding capacity and security compared to original BPCS technique.

On the other hand, [14] describes the techniques used in Steganography to hide information and deliver the message to the end user using Bit-planes without any loss of data. The method used is to replace lowest 3 or 4 LSB with message bits or image data (assume 8 bit values). We take the image and hide information in the LSB first and see the result and then implement by changing the pixel value from 1 to 7 bits. This Steganography algorithm based on embedding into the bit planes of the cover image and even tested for RS steganalysis, using a steganalysis tool "vsl1.1". The analyzer failed to detect the text which has been sent to the end user and LSB decryption which failed to detect the message by this we can say that our method is efficient.

Robust steganography using BPCS is proposed in [15]. This algorithm permits to implement hiding information into images for its secure transmission through no secure channels. This algorithm offers higher hiding capacity due to that it exploits the variance of complex regions in each bit plane. Unlike the similar methods based on BPCS, it uses the variance of complexity in each region of the image to determine optimal regions to insert the secret message. Simulation results of the proposed algorithm show that it is robust against noisy channels.

HIOKI Hirohisa [16] presents a new method for embedding data into an image called "A Block Complexity based Data Embedding". This method based on same principle as that of BPCS-Steganography. The two new complexity measures called the run-length irregularity and the border noisiness are proposed to properly discriminate noisy regions. An M-sequence is employed for converting data to be embedded into noisy data. ABCDE can be successfully applied to various images. We can expect that near 50% pixels of an image can be used for embedding without degrading its quality.

Rosane English [17] implements the bit plane complexity segmentation (BPCS) algorithm and provides a comparison in terms of effectiveness and hiding capacity with the list significant bit (LSB) algorithm using four bits. The Bit Plane Complexity Segmentation algorithm was chosen due to the effective high data hiding capacity.

On the other hand, [18] demonstrate the effectiveness of bit plane complexity segmentation in hiding medical records in color cervical images. Medical records of patients are extremely sensitive, needing uncompromising security during both storage and transmission. In addition, these records often have to be traceable to patient medical data such as X-ray or scan (CAT, MRI etc.) images. The BPCS approach presented here outperforms the current state-of-the-art in high capacity steganography, both in terms of data hiding capacity and in terms of robustness of the encoding mode.

References

- [1] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique" International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010, PP 19-23.
- [2] Ronak Doshi, Pratik Jain, Lalit Gupta, "Steganography and Its Applications in Security", International Journal of Modern Engineering Research (IJMER) Vol.2, Issue.6, Nov-Dec. 2012, PP 4634-4638.
- [3] N. Johnson and S. Jajodia, "Exploring steganography: seeing the unseen", IEEE February 1998, PP 26-34.
- [4] Ross J. Anderson and Fabien A. P. Petitcolas, "On the Limits of Steganography", IEEE Journal on Selected Areas in Communications, Vol. 16, No. 4, May 1998, PP 474-481.
- [5] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An overview of image steganography", Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa, 2005.
- [6] Mehdi Hussain and Mureed Hussain, "A Survey of Image Steganography Techniques" International Journal of Advanced Science and Technology Vol. 54, May 2013, PP 113-124.
- [7] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Elsevier Signal Processing 90 (2010), PP 727-752.
- [8] Steve Beaulieu, Jon Crissey, Ian Smith, "BPCS Steganography" University of Texas at San Antonio.
- [9] Shrikant S. Khaire, Sanjay L. Nalbalwar, "Review: Steganography – Bit Plane Complexity Segmentation (BPCS) Technique", ISSN: 0975-5462, 2012 PP 4860-4868.
- [10] Eiji Kawaguchi and Richard O. Eason, "Principle and Applications of BPCS-Steganography", Kyushu Institute of Technology, Kitakyushu, Japan-University of Maine, Orono, Maine 04469-5708.
- [11] Sheetal Mehta, Kaveri Dighe, Meera Jagtap, Anju Ekre, "Web Based BPCS Steganography" International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 2, Issue 2, PP 126-130.
- [12] Ms. Pradnya R. Rudramath, M. R. Madki, "High Capacity Data Embedding Technique Using Improved BPCS Steganography" International Journal of Scientific and Research Publications, Volume 2, Issue 7, July 2012.
- [13] Vipul J. Patel, Neha Ripal Soni, "Image Steganography System using Modified BPCS Steganography Method" International Journal of Engineering Research & Technology (IJERT), vol. 3, Issue 6, June-2014, PP 728-730.
- [14] B. Ramesh Kumar, K. Suresh, S. K. Basheer, M. Raja Krishna Kumar, "Enhanced Approach to Steganography Using Bitplanes" International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012, PP 5472-5475.
- [15] Silvia Torres Maya, Mariko Nakano Miyatake, Ruben Vazquez Medina, "Robust Steganography using Bit Plane Complexity Segmentation" 1st International Conference on Electrical and Electronics Engineering 2004, PP 40-43.
- [16] Hioki Hirohisa: A Data Embedding method using BPCS principle with new Complexity measures, in: Proceedings of Pacific Rim Workshop on Digital Steganography, July 2002, PP 30-47.
- [17] Rosane English, "Comparison of High Capacity Steganography Techniques" International Conference of Soft Computing and Pattern Recognition, IEEE-2010, PP 448-453.
- [18] Yeshwanth Srinivasan, Brian Nutter, Sunanda Mitra, Benny Phillips, and Daron Ferris, "Secure Transmission of Medical Records Using High Capacity Steganography" Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems, 2004.
- [19] Vipul J Patel, Neha Ripal Soni, "Uncompressed Image Steganography using BPCS: Survey and Analysis" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727 Volume 15, Issue 4 (Nov. - Dec. 2013), PP 57-64.