# Image Steganography System using Modified BPCS Steganography Method

Vipul J. Patel
Student, Department of Computer Engineering,
SardarVallabhbhai Patel Institute of Technology,
Vasad, India

Ms. Neha Ripal Soni
Asst. Prof, Department of Computer Engineering,
SardarVallabhbhai Patel Institute of Technology,
Vasad, India

***Abstract*—Steganography is the technique of hiding information for secrete communication. Some of the traditional techniques have limited hiding capacity and security. In this paper, we proposed improved BPCS (Bit plane complexity segmentation) steganography technique. If we apply 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 method increases the insertion capacity and security compared to original BPCS technique.**

***Keywords—BPCS, Complexity, Data Security,Image Steganography, Information Hiding***

## I. INTRODUCTION

Digitization of information like text, audio, video and image is the faster and easier wayof communication. At the same time itmakes very easy to steel, copy and changes the digitized information. Thus creates a need for security.There are two way of securingdigital information during communication. First one is tocreate mechanism for representing information in such a way thatonly authorized person can identify original meaning which includes cryptography and steganography called data security. Second one is to create a set of protocols that prevent and monitor information in network called network security.

Cryptography and steganography are theart of secret communication through secret writing and hiding respectively [1] [2]. Cryptography involves the application of different encryption methods either in a symmetric way or asymmetric way. The whole security of cryptography lies in the key and loss of key is the loss of all past as well as future communication.

Steganography is a way of invisible communication by information hiding on carrier, where carrier can be a text, image, audio or video. Selection of carrier file is based on application and amount of information required to hide. The whole security of steganography lies in hiding algorithm. Anyone that identify hiding algorithm can easily extract data from carrier. As both the method do have security issues, for most sensible data the combined strategy of cryptography and steganography is used in general.

Most stenography utilities nowadays, hiding information inside images because images are popular used in internet and have batter hiding capacity. This is called image steganography.Two important factors needs to be considered before creating Image steganographic system is the hiding capacity and imperceptibility. Imperceptibility and the capacity have very close correlation with each other in steganography [3]. Capacity of hiding data and imperceptibility usually present the reverse relationship that means more information hiding it is, more distortion it will be.

The various image steganography techniques are as follow: (1) Substitution technique (Hide the data at bit level), (2) Transform domain technique (use transform techniques DCT, DWT and FFT), (3) Spread spectrum technique (message is spread over a wide frequency), (4) Statistical technique (hide after cover is divided into blocks) and (5) Distortion technique (Information is stored by signal distortion) [10].

From various steganography techniques, Substitution technique is wildly used and simple to implement. Substitution technique uses only the least significant bits of the cover object is replaced without modifying the complete cover object. It is a simplest method for data hiding but it is very weak in hiding capacity because of limited LSB bit-planes to hide data.

BPCS (Bit Plane Complexity Segmentation) steganography is a substitution based image steganography technique. BPCS performs hiding process at all bit-planesby finding complex block and replace it with information. BPCS steganography provides batter hiding capacity around 50% which depends on image complexity. Standard definition of image complexity and their maximum threshold value is most important to decide how secure BPCS steganographic system will be. There is no standard definition of image complexity. Niimi and Kawaguchi discussed this problem in connection with the image thresholding problem, and proposed three types of complexity measures [6][7][8]. Improved BPCS-steganography takes different threshold values of image complexity to deal with bit-plane accordingly: Set greater

threshold for MSB, while smaller for LSB, the objective is to resistant steganalysis of holistic complexity histogram [9].Bit plane complexity segmentation (BPCS) overcomes the shortcomings of the traditional Least Significant Bit (LSB) manipulation techniques of data hiding [4].

This paper aims to provide a proposed modified BPCS steganography that increase hiding capacity and enhance security.The remaining portion of the paper has been organized as following sections: Section II describes the Bit Plane Complexity segmentation along with algorithm and section III deals Hiding capacity Analyses of BPCS steganography. Improved BPCS steganography is discussed in Section IV.

## II. BIT PLANE COMPLEXITY SEGMENTATION

BPCS steganography was introduced by Eiji Kawaguchi and Richard O. Eason [5] [11]. BPCS is the expansion of LSB substitution method and it increases data hiding capacity with batter performance. The major idea behind BPCS is that characteristics of the human vision system whereby a human cannot perceive any shape information in a very complicated binary pattern. The basic flow of BPCS is as first thing is to divide gray scale or color image into different bit planes and then divide into fixed-size blocks. Every block has different complexity in which higher complexity block act like noisy region and other act like informative blocks. We can replace all of the "noisy" regions in the bit-planes of the vessel image with secret data. BPCS steganography can be applied on both gray scale image and color image.

The algorithm of BPCS Steganography is as follow:

1) Select the carrier image may be gray scale or color. Divide into 8 or 24 different Bit- Planes if gray image or color image respectively. The bit-planes divided into small pieces of the same sizeare called bit-plane blocks, such as 8 × 8.

2) Calculate the complexity of every block.

The complexity is defined as the number of changes in white and black pixel. The length of the black-and-black border in a binary image is a good measure complexity. If the border is long, the image is more complex. Complexity is equatedas follows,

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

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

3) Define threshold complexity valuefor the bit-plane block which is denoted by$\alpha_0$. The bit-plane block whose complexity is larger than $\alpha_0$is noisy and used to embed secret information. The smaller the value of$\alpha_0$, the more secret information can be embedded.

4) Divide the secret informationalso into block andapply complexity measurement to each message block. If a message block is determined as no-complex block, itshould beconjugated (write the meaning of conjugate). Conjugate is a process of joining message block with Wc (White checks) or Bc (black checks) using $\oplus$ (X-or)operation to increase complexity. Create conjugate map containing a record of the block which passed through conjugate processing. This conjugate map will be used during extraction process and needs to be hiding into the carrier.

5) After hiding conjugate map, replace all complex image block with message block with some extra information like length of payload, file name, file type etc. This extra information will be used to reconstruct original file with same type, name and length.

Secret information extraction process is simple as like embedding process. Firstly, extract all block containing conjugate map and extra information about hidden data. Extra hidden information is used to find size of hidden information and conjugate map is used to confirm the hidden information blocks that have passed through conjugate processing. Then pick up all the pieces of block which are bounded by size of hidden information and whose complexity is greater than$\alpha_0$.

## III. HIDING CAPACITY ANALYSES OF BPCS STEGANOGRAPHY

The original BPCS algorithm process all bit planes in same manner and tries to hide information at complex region of image. The original BPCS algorithm presented by Kawaguchi E has batter hiding capacity but in algorithm every bit planes is divided into to fix small 8 × 8 blocks. Due to fix size small block, sometime we get less block area for hiding and overall hiding capacity will reduce. Figure (1, 2) shows different hiding capacity effect on block size. Let consider thresold comlexity $\alpha_0 = 0.4$ for all the block. In figure 2, 16 × 16 block has complexity 0.64 which is grater then 0.4 and so hiding capacity is 256 bits. But if we divide 16×16 block into four 8×8 blocks (Fig.1) then may be total hiding capacity will reduce. In fig.1, 1, 3 and 4 blocks are complex and block 2 is non-complex. So due to 3 complex blocks, now hiding capacity reach up to 192 bits which is < 256. Figure (3, 4) represent totally opposite effect in between block size 8×8 and 16×16. 16×16 block has complexity 0.37 < 0.4. So it is not used for embed any data hiding process and hiding capacity is 0 bit and after we divide 16×16 block into four 8×8 blocks (Fig.3) than 3 and 4 blocks are complex and use to hiding data with capacity 128 bits.

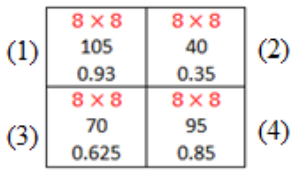


Fig.1. Example 1

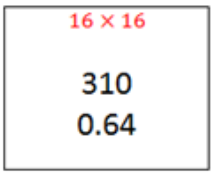


Fig.2. Example 2

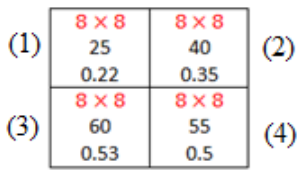


Fig.3. Example 3

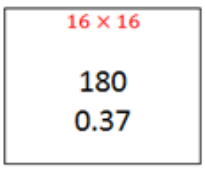


Fig.4. Example 4

This variation of hiding capacity due to block size can be solved by variable block size at different bit planes. Different bit planes have different characteristic as LSB planes have always large amount of complex blocks and MSB planes looks like simpler and contain very less complex block. Based on this characteristic, we perform different block size at different bit –planes.

## IV. IMPROVED BPCS STEGANOGRAPHY

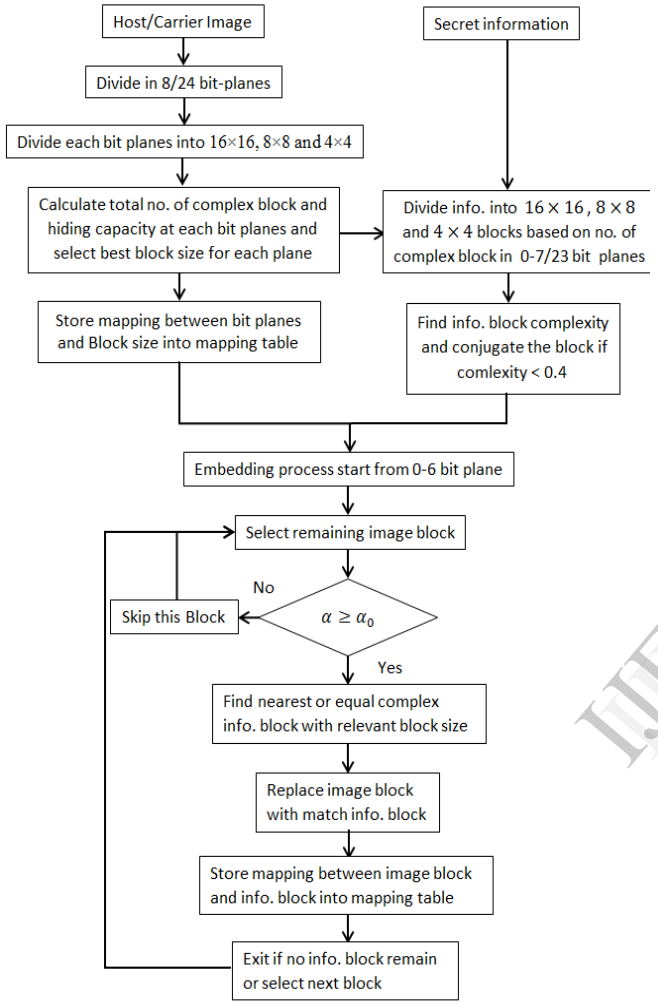


Fig.5. Proposed BPCS Algorithm

### A. *Information Hiding Algorithm*

BPCS steganography is based on complexity of image. If complexity is high then information hiding capacity of image is more otherwise it dependent on complexity of image. So selection of carrier image is most important. First we perform bit plane slicing to create 8 or 24 bit planes of an image. To increase image hiding capacity we can use variable block size at each bit planes of image. After bit plane slicing, divide each bit planes into 16×16, 8×8 and 4×4. After this, find total number of complex blocks and total hiding capacity at each bit planes. Based on maximum hiding capacity, we make selection from the block size 16×16, 8×8 and 4×4 for each bit planes. We store variable block size information in mapping table that includes which bit plane uses which block size. It is necessary to find number of complex blocks in different bit planes. Now we take secret information and divide information into $16 \times 16, 8 \times 8$ and $4 \times 4$ block sizes based on number of complex blocks in 0-7 bit planes. If complexity is more than 0.4 then conjugate information block. Now select each blocks, find complexity and if it is more than 0.4 then find nearest or equal complex information block with relevant block size. Replace this relevant block with image block. Mapping between image block and information block store in mapping table.

### B. *Information Extraction Algorithm*

Information extraction process is the reverse process of hiding process. First we perform bit plane slicing and then divide it into variable sized block based on information stored in mapping table. Calculate images block complexity and if it is more than 0.4 then it is information block and store it as temporary block. After extracting all information blocks, arrange blocks based on mapping information stored in table.

## V. CONCLUSION

BPCS steganography has some drawbacks about with data capacity and security. Here, proposed algorithm can solve these overcomes by increasing data hiding capacity using variable block size and give batter security using comparison and replace nearly equal complex data block. During variable block size and comparative replacement, mapping table is created and this mapping table is used as key to rearrange extracted information block. Information extraction process will be difficult without mapping table. We can use mapping table as like key in encryption techniques and use this table during extraction process.



## REFERENCES

[1] Behroz A. Forouzan, “Cryptography & Network Security”, McGraw Hill Publication-2008, New Delhi.
[2] William Stallings, “Cryptography & Network Security Principles and Practice”, 5th edition, Pearson Education, Inc.,pp 57 .
[3] Jin-Suk Kang, Yonghee You and Mee Young Sung, “Steganography using Block-based Adaptive Threshold”, IEEE, Nov. 2007
[4] Neil F. Johnson, ZoranDuric, SushilJajodia, Information hiding: Steganography and Watermarking- Attacks and Countermeasures, Kluwer Academic Publishers, 2001
[5] Eiji Kawaguchi and Richard O. Eason, “Principle and Applications of BPCS-Steganography”, Kyushu Institute of Technology, Kitakyushu, Japan – University of Maine, Orono, Maine.
[6] Kawaguchi, E. and Taniguchi, R., “Complexity of binary pictures and image thresholding – An application of DF-Expression to the thresholding problem”, Proceedings of 8th ICPR, vol.2, pp.1221-1225, 1986.
[7] Kawaguchi, E. and Taniguchi, R., “The DF-Expression as an image thresholding strategy”, IEEE Trans. On SMC, vol.19, no.5, pp.1321-1328, 1989.
[8] Kawaguchi, E. and Taniguchi, R., “Depth-First Coding for multi-valued figures using bit-plane decomposition”, IEEE Trans. On Comm., vol.43, no.5, pp.1961-1995.
[9] Tao Zhang, Zhaohui Li and Peipei Shi, “Statistical analysis against improved BPCS steganography”, IEEE, March 2010.
[10] Souvik Bhattacharyya, Indradip Banerjee and GautamSanyal, “A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier”, JGRCS 2010.
[11] BPSC : http://www.datahide.com/BPCSe/