

Text Hiding in Digital Image using BPCS Method

¹ Leni Marlina , ¹ Andysah Putera Utama Siahaan, ² Dimas Maulana

¹Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

²Degree Student, Faculty of Science and Technology, Universitas Pembangunan Panca Budi, Medan, Indonesia

Email: ¹lenimarlina@dosen.pancabudi.ac.id, ¹andiesiahaan@gmail.com, ²araymaulana66@gmail.com

Abstract: *Steganography is a technique of hiding secret messages into other media so that the secret message is not known in plain view in a stego-image. At present many steganography techniques are developed, such as one example is LSB. However, this technique has a minimal storage capacity, which is only about 10-20% of the size of the original image. The steganography technique used in this final project is the BPCS technique, where this technique provides greater message insertion capacity, which is around 30% -50%. This technique replaces the bit-plane area that is noise-like by the secret passage. The results of embedded images generated from this technique are not very visible in the visible difference. In this study, the media used are digital images with JPG, JPEG, and PNG. The testing process is done by inserting a message file into several types of cover images using the steganography application that was built. The test results showed that the stego results did not appear visually different from the original image. Testing the value of PSNR (Peak Signal to Noise Ratio) also proves that the higher the resolution the quality of the stego results will be good. Moreover, the results of testing the effect of the threshold value prove that the higher the threshold value the stego quality will be better.*

Keywords: *Steganography, BPCS, PSNR, Digital Image.*

1. INTRODUCTION

Data security is an essential and vital component of electronic data communication. At present several techniques have emerged to secure data, one of which is steganography. Steganography technique is a technique to hide secret information by inserting it into specific media. In steganography, several methods have been developed, one of the simplest is LSB (Least Significant Bit) [1]. However, in the LSB method, there are some disadvantages, for example, the capacity to store confidential data is minimal [2]. The LSB method can only accommodate 10% to 20% of media capacity, so it cannot accommodate media with large capacity. Also, the LSB method will have a distortion effect if the capacity of the media to be inserted is too large. Of course, this method will be less effective in steganography. To improve the techniques available at the LSB, there is a newer method called BPCS (Bit-Plane Complexity Segmentation) introduced by Eiji Kawaguchi and Richard O. Eason [3]–[5]. This method can store confidential data up to about 50%. The BPCS method uses random storage techniques that are divided into two types, namely informative and noise-like areas. In this study, a steganography application will be developed that will apply the BPCS method to hide text messages on digital image media [6][7]. Message container media used are digital images with JPG, PNG and BMP formats of different sizes, types, and resolutions. In this research, the stego-image uses a password during insertion, so that secret messages inserted with this method become safer. It is expected that the BPCS method can work well and efficiently. BPCS is also expected to be able to accommodate more messages than other methods.

2. THEORIES:

2.1 Steganography

The word steganography itself comes from Greek, namely "steganos" which means hidden or veiled and "graphein" which means writing [8]. It can be interpreted as hidden writing. At present, steganography is defined as a science to hide messages on certain media. Media can be like pictures, audio or even video. Steganography has been known for thousands of years ago. The writing of the ancient Egyptian nation known as hieroglyphic writing is considered as the first application of the concept of steganography [9]. The writing consists of symbols that have certain meanings. Furthermore, steganography develops from time to time, until the digital period like today. Steganography is the science and art of hiding secret messages in other messages so that the existence of the secret message cannot be known [10]. Whereas according to Doni Ariyus, steganography is a branch of learning about how to hide "confidential" information in other information. Steganography itself requires two aspects, such as storage media and confidential information that will be hidden. The steganography method is advantageous if used on computer steganography because of the digital file format that can be used as a medium to hide messages. Digital steganography uses digital media as a place to hide messages, such as images, audio, and video. Steganography is different from cryptography; the difference lies in how the process of hiding data and the final results of the process. Cryptography processes the original data to produce encrypted data that is completely random and different from the original [11]–[13], while steganography hides in other data that it will occupy without changing the data that is boarded so that the data it occupies before and after

the embedding process is almost the same [14]. There are various goals to be achieved in using this steganography to hide confidential information. One of the objectives of this steganography technique is to insert confidential information through the network without arousing suspicion.

2.2 Bit-Plane Complexity Segmentation

Bit-Plane Complexity Segmentation (BPCS) is one of the steganographic techniques introduced by Eiji Kawaguchi and R. O. Eason in 1997 [3]. In BPCS digital image documents are divided into 8x8 pixel segments in each segment. In 8-bit image documents, each one segment will have 8 bits of the plane that represent the pixels of each bit. The process of data insertion is carried out on segments that have high complexity, called noise-like regions. In these segments, the insertion is carried out not only at the least significant bit but in the entire bit-plane.

3. METHODOLOGY:

3.1 Bit Slicing

A multi-valued image with a depth of n bits can be broken down into the form of n-binary images (bit-plane) with the operation of bit slicing (Kawaguchi, 1997). Bit-plane slicing can be described as follows.

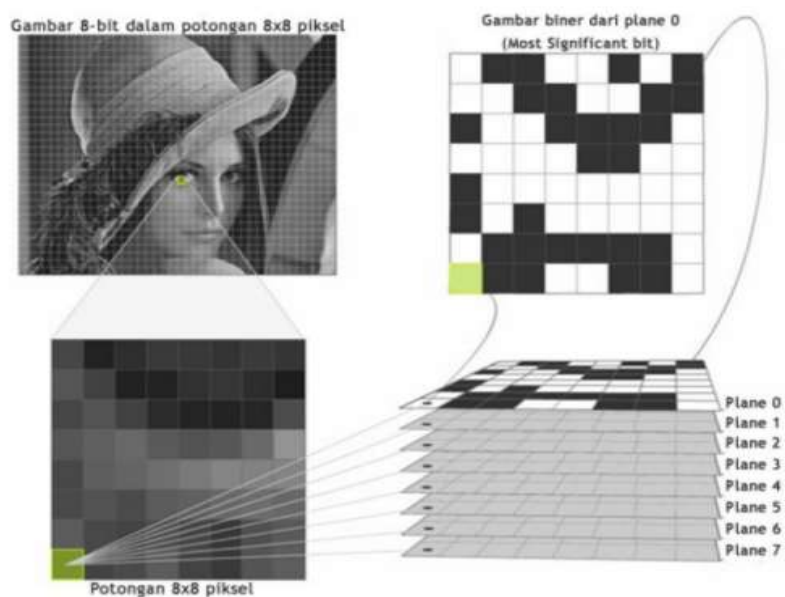


Figure 1. Process of bit-slicing in an 8x8 pixel segment

In 8-bit images, the intensity of each pixel is represented by 8-bits. An 8-bit image consists of a 1-bit plane, from bit-plane 0 (LSB) to bit 7 (MSB). The '0' plane contains all the lowest sequence bits (LSB) of all pixels while the '7' plane contains all the highest order bits (MSB).

3.2 Canonical Gray Code (CGC)

CGC is a binary image system that is recommended for embedding because CGC tends to be better than PBC. Indeed Pure Binary Code (PBC) can provide a larger area for embedding bit-plane, but PBC has the problem of "Hamming Cliff", where small changes in color affect many bits of color values. So it was recommended to change the binary image system from PBC to CGC. For example, in an 8-bit image, there are two pixels which have an intensity value of 127 and 128, respectively. In PBC, 127 can be represented as 01111111 and 128 represented as 10000000. Both pixels are visible the eye will look identical, the inside is very different in its bit representation. If confidential data is embedded, then there is a possibility that the representation of the bit will be 11111111 01111111 and can be 00000000,000,000. This concept is known as "Hamming Cliff." In these circumstances, before the embedding process is carried out, there is a difference in one gray level that is ignored by the human eye. After the embedding process, the gray level difference is that of 255, one pixel appears dark black while the other pixels appear pure white. The changes will be obvious to the human eye. Therefore, this weakness can be avoided by the Canonical Gray Coding (CGC) system, wherein the gray coding technique is used. That way, 127 which is represented as 01111111 in PBC is now represented to be 01000000 in the CGC. Similarly, binary 128, which is 10000000, becomes 11000000. Now the two pixels look the same but differ by only one bit. It is the opposite of the PBC system. So after the embedding process, 01000000 can be 11000000 and 11000000 can be 01000000. So the change in intensity level in pixels is not too flashy. Therefore, the CGC system is recommended to be used rather than PBC in the BPCS system.

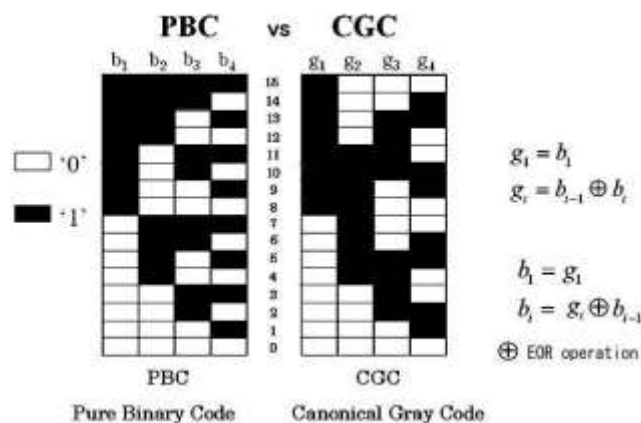


Figure 2. PBC vs CGC pixel pattern

3.3 Binary Image Complexity

The most important thing from the BPCS method is finding a "complex" bit-plane area on the vessel image so that data from secret images can be inserted without suspicion. In calculating the value of complexity, there is no standard definition for calculating it. There are several methods of measuring complexity values, but in this paper, we will focus on calculating complexity values based on the length of the black and white border in the black-white border image complexity.

3.4 Informative Region and Noise-Like Region

After calculating the complexity values in each plane, we can determine which planes are "informative" and "noise-like." The complexity of a bit-plane area is a parameter used to determine a bit-plane is an informative group or noise-like region. Informative region means a binary image area that is simple or has a simple complexity value, while the noise-like region means a complex binary image area. There must be a limiting value or the threshold value (α) to determine whether the plane includes the informative region or bit-plane region. The threshold value limit is $0 < \alpha < 1$. Generally the threshold value used is $\alpha = 0.3$. Thus, it can be concluded, that for all planes that have complexity values below the threshold value is "informative region." Conversely, all planes that have complexity values above the threshold value are noise-like regions. It is in this noise-like region that we will insert confidential data. For the threshold, the greater the value used, the higher the noise limit taken, so the less amount of noise that can be utilized. However, by increasing the threshold value, the stego image produced will be of better quality, because the less noise is replaced by the message.

3.5 Binary Image Conjugation

Binary imagery consists of informative regions and noise like regions, as well as confidential data that also has informative regions and noise like regions. If confidential data has a noise region like region, it can be embedded in the noise like region part of the binary image for insertion. However, if confidential data has an informative region, then it must undergo conjugation surgery to be complex. Conjugation from a binary image P is another binary image that has a complexity value of one minus the complexity value P. An example of a black and white P image measuring 8x8 pixels has a white background color and a black foreground color. W is a pattern with all white pixels and B is a pattern with all black pixels. Wc and Bc are chessboard patterns, where Wc is a chessboard pattern with white pixels on the upper left, while Bc is a chessboard pattern with black pixels on the upper left. P* is a new form of conjugation of P.

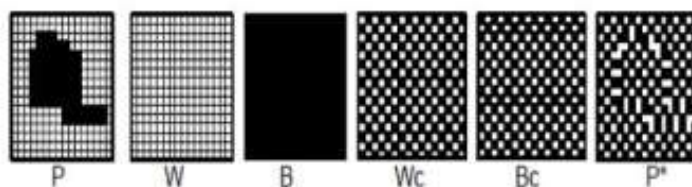


Figure 3. Conjugation Process

3.6 Conjugation Map






Conjugation maps are collections of conjugated blocks. It is made to be a marker and a guide for the program in the decryption process. The conjugate map will be permanently placed in the noise section of the container image. The conjugate map is made in the form of a bit-plane and will be conjugated to add value to its complexity. The first line of the conjugate map will be filled with the value of bit 1, which is 00000001, as a marker that the container image

contains a secret message. Then the second row contains the amount of noise that must be translated back into a secret message string. This number is also made in the form of bits, add a marker to conjugate the last plane noise if needed in line 3 on the map. The rest of the conjugate map will be filled with a value of 00000000 until it becomes a bit plane, then it is conjugated to add noise and inserted to replace the first noise from the container image.

4. RESULT AND DISCUSSION:

In testing, the authors provide a vessel for insertion in various types of resolutions described in the following table.

Table 1. Vessel Image

Image	File Name	Size	Type	Resolution
	img64x64	2,2 KB	JPG	64 x 64
	img100x100	14,4 KB	PNG	100 x 100
	Img300x300	94,6 KB	JPG	300 x 300
	img550x415	54,7 KB	JPEG	550 x 415
	Img1050x1050	2,0 MB	PNG	1050x1050

In this test, there are three criteria to be tested, namely program functionality, PSNR value as a parameter of stego-image quality, and the effect of the threshold value on image quality. From several tests for inserting text message files in several different images, it can be presented in the following table form.

Table 2. PSNR Comparison

Text File	Vesel Image	Stego Size	PSNR
Test#2	Img64x64.JPG	12,3 KB	20,63
Test#2	Img100x100.PNG	27,7 KB	25,28
Test#2	Img300x300.JPG	262,9 KB	35,06
Test#2	Img550x415.JPEG	665,9 KB	36,60
Test#2	Img1050x1050.PNG	3,3 MB	48,73

From the results of the above tests, it can be seen that the PSNR value is higher, along with the increasing image resolution. PSNR values below 30 dB indicate that the quality of the inserted image is relatively low, where the distortion will be seen. However, if the inserted image quality is at a value of 40 dB or more, then the quality of the results is high. Moreover, from the test results, it can be concluded, that the higher the resolution of an image, the better the quality of

the inserted image. In this test, the message file test # 2.txt will be inserted into the image file img550x415.JPEG. by using a threshold value of 0.1, 0.2, 0.3, 0.4, 0.5.

5. CONCLUSION:

From some of the discussions above, conclusions can be drawn. The application that implemented steganography with the BPCS method was successfully built. By using the BPCS method, the inserted image results look the same as the original image; the difference is not visually visible. Testing the PSNR value shows that the higher the resolution of the image, the better the quality of the inserted image. The threshold value affects the quality of the embedded image, where the higher the threshold value, the better the quality of the inserted image.

REFERENCES:

1. Hermansyah and A. P. U. Siahaan, "Technique of Hiding Information in Image using Least Significant Bit," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 67–70, 2018.
2. R. D. Sari and A. P. U. Siahaan, "Least Significant Bit Comparison between 1-bit and 2-bit Insertion," *Int. J. Innov. Res. Multidiscip. F.*, vol. 4, no. 10, pp. 110–113, 2018.
3. A. P. U. Siahaan, "High Complexity Bit-Plane Security Enhancement in BPCS Steganography," *Int. J. Comput. Appl.*, vol. 148, no. 3, pp. 17–22, 2016.
4. A. P. U. Siahaan, "Noise-Like Region Security Improvisation in BPCS Steganography."
5. A. P. U. Siahaan, "Vernam Conjugated Manipulation of Bit-plane Complexity Segmentation," *Int. J. Secur. Its Appl.*, vol. 11, no. 9, pp. 1–12, Sep. 2017.
6. S. Sun, "A New Information Hiding Method Based on Improved BPCS Steganography," *Adv. Multimed.*, vol. 2015, pp. 1–7, 2015.
7. S. Sun, "A New Information Hiding Method Based on Improved BPCS Steganography," *Adv. Multimed.*, vol. 2015, pp. 1–7, 2015.
8. R. Rahim *et al.*, "Combination Base64 Algorithm and EOF Technique for Steganography," in *Journal of Physics: Conference Series*, 2018, vol. 1007, no. 1.
9. W. Fitriani, R. Rahim, B. Oktaviana, and A. P. U. Siahaan, "Vernam Encrypted Text in End of File Hiding Steganography Technique," *Int. J. Recent Trends Eng. Res.*, vol. 3, no. 7, pp. 214–219, Jul. 2017.
10. A. P. U. Siahaan, "RC4 Technique in Visual Cryptography RGB Image Encryption."
11. W. Stallings, *Cryptography and Network Security: Principles and Practice*. New Jersey: Prentice Hall Press, 2013.
12. A. P. U. Siahaan, "Factorization Hack of RSA Secret Numbers," *Int. J. Eng. Trends Technol.*, vol. 37, no. 1, pp. 15–18, 2016.
13. M. Iqbal, M. A. S. Pane, and A. P. U. Siahaan, "SMS Encryption Using One-Time Pad Cipher," *IOSR J. Comput. Eng.*, vol. 18, no. 6, pp. 54–58, 2016.
14. K. Kordov and B. Stoyanov, "Least Significant Bit Steganography using Hitzl-Zele Chaotic Map," *Int. J. Electron. Telecommun.*, vol. 63, no. 4, pp. 417–422, Nov. 2017.