International Journal of Science and Informatics Technology (IJOSIT)
Vol 1, No 1, April 2026, pp. 1-7
https://www.ijosit.org/index.php/ijosit
ISSN: XXXX-XXXX

Implementation of the Bit Plane Complexity Segmentation (BPCS) Steganography Method for Embedding Secret Messages in Image Media

Yadi Limanta Maha, Andre Septianus Nababan, Lonia Harefa
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

Abstract. Rapid developments in information technology have increased the need for data security and confidentiality. Steganography, as a technique for hiding messages in digital media, is an effective solution for keeping messages hidden. One steganography method that has high capacity and is capable of maintaining image quality is Bit-Plane Complexity Segmentation (BPCS). This study aims to implement the BPCS method on digital color images (RGB) using the Python programming language with a Graphical User Interface (GUI) that makes it easy for users to insert and extract secret messages. The research process includes separating images into bit planes, calculating the complexity of each bit plane block, embedding secret messages in complex bit planes, and extracting messages to ensure information integrity. Manual calculation examples and message embedding simulations show that the BPCS method can embed large messages without reducing image visual quality. Test results show that changes only occur in the low bit-planes, so the image remains visually unchanged. The implementation of this GUI application makes it easier for users to insert and extract secret messages without having to deeply understand the BPCS algorithm, while also proving the reliability of this method in digital image steganography.

Keywords: First keywords, Second keywords, Third keywords,Third keywords.

This is an open access article under theCC BY-NClicense

Corresponding Author:
Yadi Limanta Maha
Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Katolik Santo Thomas Medan Sumatera Utara, Indonesia

1. Introduction

The rapid development of information technology has led to an increase in data exchange in various digital forms. Communication activities via the internet, cloud-based storage, and digital file distribution make data more vulnerable to interception, manipulation, and theft by unauthorized parties. This situation requires a security mechanism that not only protects the content of messages but also ensures that the messages themselves remain undetectable. Until now, cryptography techniques have been widely used to secure information by converting messages into a form that cannot be read without a specific key [1]. Although effective in maintaining the confidentiality of content, cryptography still reveals the existence of hidden messages, which can arouse suspicion from other parties. Therefore, an additional approach is needed to disguise the existence of these messages. Steganography provides a solution by embedding secret messages into digital media such as text, audio, video, or images so that the message appears to be a normal part of the media [2].

Digital images are the most widely used medium in steganography because they have relatively large data sizes and pixel structures that allow manipulation without significant visual changes. One popular method is Least Significant Bit (LSB), which is a technique for embedding messages in the least significant bit of each pixel [3]. This method is simple and easy to implement, but it has weaknesses in terms of security and resistance to statistical analysis. In addition, its insertion capacity is limited and it is easily detected if special testing is performed. As a more robust alternative, the Bit Plane Complexity Segmentation (BPCS) method was developed. This method takes advantage of the characteristics of the human visual system, which has difficulty distinguishing random patterns in images. In BPCS, the image is decomposed into several bit planes, and then complexity analysis is performed on each block. Blocks with high complexity levels that visually resemble noise are selected as message insertion locations. With this approach, messages can be inserted in larger quantities without causing significant visual changes [4].

The advantage of the BPCS method lies in its high insertion capacity and its ability to preserve the visual quality of the steganographic image [5]. This technique utilizes complex regions within bit-planes, allowing a larger amount of data to be embedded without producing noticeable distortion. Furthermore, because the message is hidden in visually complex areas, the probability of detection is significantly lower compared to simpler techniques such as LSB [6]. As a result, BPCS offers a better balance between capacity and imperceptibility. Therefore, this study focuses on implementing the BPCS method

for embedding secret messages in digital images and evaluating its performance in capacity, image quality, and security aspects.

2. Literature Review and Problem Statement

Recent research shows that image-based steganography techniques continue to evolve in line with the increasing need for digital communication security. Several recent studies reveal that the Least Significant Bit (LSB) method is still widely used because it is simple and has low computational complexity, but it is vulnerable to statistical steganalysis attacks and image manipulation such as lossy compression and noise addition [7]. On the other hand, recent research on Bit Plane Complexity Segmentation (BPCS) confirms that the bit-plane complexity analysis-based approach can significantly increase insertion capacity without drastically reducing image visual quality [8]. This method utilizes bit-plane segmentation and complexity level measurements to determine areas that resemble noise, making them safer to use as message insertion media.

Based on this study, the BPCS method is considered superior to conventional approaches in terms of capacity, visual quality, and resistance to detection. The issue raised in this study is how to implement the Bit Plane Complexity Segmentation (BPCS) method into an easy-to-use Graphical User Interface (GUI)-based application that is capable of effectively inserting and extracting text messages. The designed application is expected to provide users with the convenience of securing confidential messages in digital images without having to understand the technical processes of the algorithm in depth, while maintaining the quality of the steganography image.

3. Material and Method

The method used in this study is Bit-Plane Complexity Segmentation (BPCS) with the following steps

3.1 Data Preparation

The process begins with preparing an 8-bit grayscale digital image that will be used as a medium for storing secret messages. This image is chosen because each pixel has an 8-bit representation (0–255), allowing for manipulation at the bit level without significantly altering the visual quality [9]. Next, a secret message in text form is prepared and converted into a binary representation so that it can be inserted into the image. After that, a bit-plane conversion process is carried out, which is to break down each image pixel into eight bit layers (bit-planes), starting from the least significant bit to the most significant bit. This separation aims to analyze and determine the appropriate bit-plane as the location for inserting the message based on its level of complexity [10].

3.2 Bit-Plane Complexity Segmentation Calculation

This subsection describes the calculation steps in the Bit-Plane Complexity Segmentation (BPCS) method used to determine image areas with high complexity levels as media for message insertion [11]. This process involves breaking the image down into bit planes, dividing it into small blocks, and measuring complexity values to determine the suitability of each block for data hiding [12].

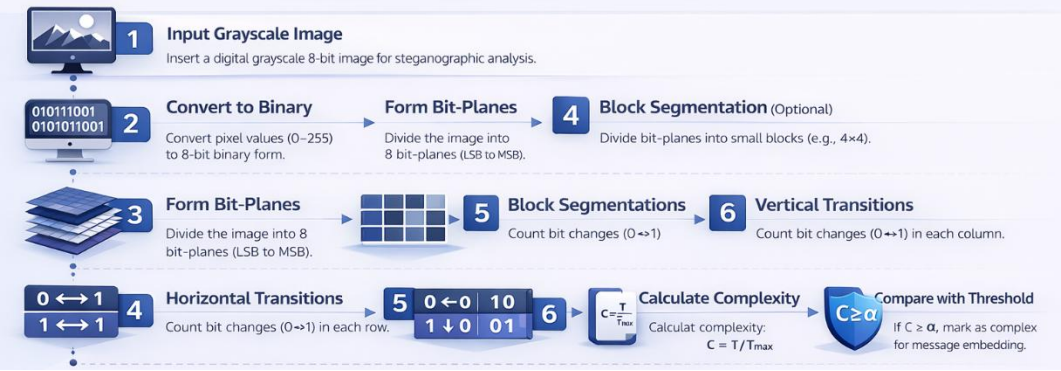

Figure 1. Bit Plane Complexity Segmentation Formation Process

Figure 1 illustrates the step-by-step process of the Bit-Plane Complexity Segmentation (BPCS) method for steganographic analysis. The process begins with inputting an 8-bit grayscale image, followed by converting pixel values into binary form and separating the image into eight bit-planes (from LSB to MSB). The bit-planes may then be divided into smaller blocks for

further analysis. Horizontal and vertical bit transitions are calculated to determine the complexity value using the formula $C = T/T_{max}$. Finally, the calculated complexity is compared with a predefined threshold to decide whether a block is classified as complex and suitable for message embedding [9].

4. Result And Discussion

4.1 Calculation example

Manual calculations in the Bit Plane Complexity Segmentation (BPCS) method are performed to gradually understand the bit-plane complexity analysis process before it is used as a medium for inserting secret messages. This stage begins with the formation of a grayscale image matrix, the conversion of pixel values to binary form, the selection of specific bit planes, and the calculation of the number of horizontal and vertical transitions to obtain the complexity value. The complexity value is then compared to a specified threshold to decide whether the bit plane can be used for encoding with the matrix requirements in Table 1.

Table 1. Grayscale Image Matrix, Pixel Value Conversion

150	152	149	151
148	150	153	149
151	149	150	152
150	151	148	149

Nilai	Biner
150	10010110
152	10011000
149	10010101
151	10010111

Bit-Plane Formation

Pada tahap ini dilakukan pemisahan lapisan bit (bit-plane) dari setiap piksel citra grayscale 8-bit. Jika diambil bit-plane ke-0 (Least Significant Bit / LSB)**,** maka yang digunakan adalah bit paling kanan dari setiap representasi biner piksel. Contoh:

150 → 0 → 0 0 1 1
149 → 1 → 0 0 1 1
151 → 1 → 1 1 0 0

Dengan Jika seluruh piksel pada matriks 4×4 diambil bit LSB-nya, maka diperoleh matriks bit-plane sebagai berikut:

$$\begin{matrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{matrix}$$

Bit-Plane Complexity Calculation

After the bit-plane is formed, the next step is to calculate its complexity level to determine whether the bit-plane is suitable for use as a message insertion medium. In this example, a bit plane with m = 4 rows and n = 4 columns is used. Complexity is calculated based on the number of bit value changes (transitions) from 0 to 1 or from 1 to 0. The calculation begins by counting the horizontal transitions, which are the bit changes that occur between elements in each row of the bit plane matrix. For the following horizontal and vertical transitions, A transition is counted if the bit changes (0 → 1 or 1 → 0)

Row 1: 0 → 0 → 1 → 1 → 1 transition
Row 2: 0 → 0 → 1 → 1 → 1 transition
Row 3: 1 → 1 → 0 → 0 → 1 transition
Row 4: 0 → 1 → 0 → 1 → 3 transition
Total horizontal transition:
T_h = 1 + 1 + 1 + 3 = 6Vertical transition
Column 1: 0 → 0 → 1 → 0 → 2 transitions
Column 2: 0 → 0 → 1 → 1 → 1 transitions
Column 3: 1 → 1 → 0 → 0 → 1 transitions
Column 4: 1 → 1 → 0 → 1 → 2 transitions
Total vertical transitions:
T_v = 2 + 1 + 1 + 2 = 6
Total Transition
T = T_h + T_v

T =6 + 6
T = 12

Complexity Calculation

The complexity calculation is performed by comparing the total number of transitions obtained with the maximum number of transitions that can occur on an m×n bit-plane. $m = 4, n = 4$ then

$$T_{max} = 4(4-1) + (4-1)4$$
$$T_{max} = 4(3) + 3(4)$$
$$T_{max} = 12 + 12$$
$$T_{max} = 24$$

If the total transitions obtained are T=12, then the complexity value is calculated using the formula:

$$C = \frac{T}{T_{maks}}$$
$$C = \frac{12}{24}$$
$$C = 0{,}5$$

The bit-plane complexity value obtained is 0.5

Bit-Plane Decision (BPCS)

Threshold value is defined as:

$$\alpha = 0{,}3$$

The calculated complexity value is:

$$C = 0{,}5$$

Because:

$$C \geq \alpha (0{,}5 \geq 0{,}3)$$

the bit-plane is classified as complex and is eligible for secret message embedding.

Message Embedding (Encoding)

Manual Assume the secret message is:

'A'

ASCII code:

$$A = 65$$

Binary representation:

$$65 = 01000001_2$$

The first 8 bits of the complex bit-plane are replaced with the binary message.

Initial bit-plane values:

$$0\ 0\ 1\ 1\ 0\ 0\ 1\ 1$$

Binary message:

$$0\ 1\ 0\ 0\ 0\ 0\ 0\ 1$$

After replacement, the bit-plane stores the secret message bits.

Message Extraction (Decoding)

Decoding steps

1. Select the complex bit-plane used for embedding.
2. Read the embedded bits sequentially:

$$0\ 1\ 0\ 0\ 0\ 0\ 0\ 1$$

Convert binary to decimal:

$$01000001_2 = 65_{10}$$

Convert decimal to ASCII:

$$65 = \text{'A'}$$

The original secret message is successfully recovered.

Conclusion of Manual Calculation

Based on the manual calculation for a 4×4 bit-plane, the complexity value obtained is:

$$C = 0{,}5$$

Since this value exceeds the threshold $\alpha = 0{,}3$, the bit-plane is categorized as complex and suitable for message embedding. The encoding and decoding processes are successfully performed without any loss of information.

4.2 Insertion of Secret Messages

This application is designed to insert secret messages into digital images using the Bit-Plane Complexity Segmentation (BPCS) method. This method allows information to be hidden effectively without significantly reducing the visual quality of the image, making the secret message difficult to detect with the naked eye, as shown in the following image:

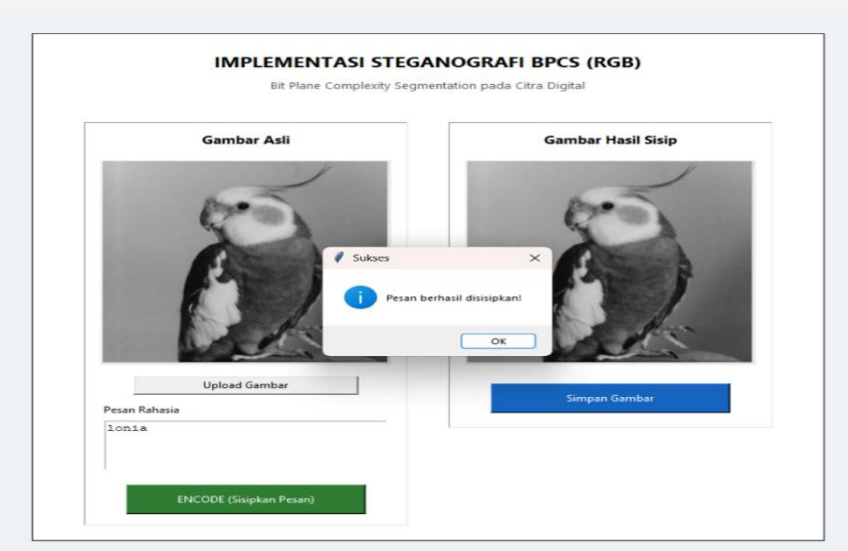

Figure 2. Secret Message Insertion Process

Figure 2 shows a system designed to insert secret messages into digital images using the Bit-Plane Complexity Segmentation (BPCS) method. This method allows information to be hidden effectively without significantly reducing the visual quality of the image, making the secret message difficult to detect with the naked eye. The application provides a number of key functions that support the steganography process. Users can upload digital images to be used as media for message insertion. The secret information entered is then converted into binary form and mapped to the image's bit-plane. The insertion process is carried out through the BPCS mechanism by sorting the RGB bit-plane, identifying areas with high complexity levels, and selectively inserting messages so as not to damage the image display. After the embedding process is complete, the application allows users to save the steganographic image that contains the secret message. With this approach, the application is able to maintain a balance between information security and image visual quality, making it suitable for use in digital steganography-based data protection.

4.3 Program Analysis for Insertion Simulation

Message insertion simulation using the BPCS method was performed to analyze how pixel values change during the embedding process. In this simulation, an image measuring 256 × 256 pixels with a block size of 8 × 8 and a complexity threshold of 0.3 was used. The secret message embedded was “loni,” which was converted to binary form before being embedded in the bit plane that met the complexity criteria. This analysis aimed to observe pixel value changes in detail and ensure that the modifications did not significantly affect the visual quality of the image in the table.

Table 2. Simulation Parameters

Parameters	Nilai
Image Size	256 × 256
Block Size	8 × 8
Threshold (α)	0,3
Secret Message	loni

The table above shows the configuration used in the simulation. Bit plane 0 (LSB) was selected as the insertion medium because it met the complexity value above the threshold. The message was converted into binary form so that it could be embedded directly into the pixel bit level.

Table 3. Pixel Change Data

No	Position	Channel	Initial Decimal	Massage Bit	Final Decimal	Change
1	(0,0)	Blue	186	0	186	0
2	(1,0)	Blue	184	1	185	+1
3	(2,0)	Blue	187	1	187	0
4	(3,0)	Blue	187	0	186	-1
5	(4,0)	Blue	189	1	189	0
6	(5,0)	Blue	187	1	187	0
7	(6,0)	Blue	190	0	190	0
8	(7,0)	Blue	190	0	190	0

The table shows that pixel value changes only occur in the least significant bit (LSB). If the message bit differs from the initial LSB, the pixel value changes by ±1. If they are the same, there is no change. The maximum change that occurs is only 1 intensity level, so it is visually indistinguishable to the human eye.

Table 4. Simulation Results

Description	Value
Total Pixels Changed	56
Bit-planes Used	0
Range of Value Changes	±1
Visual Impact	Not significant

Based on the simulation results, 56 pixels underwent changes during the message insertion process. All changes occurred in the low bit plane (LSB), resulting in only ±1 pixel value changes. Thus, the BPCS method in this simulation successfully inserted messages without causing significant visual changes to the digital image.

4.4 Discussion

Through an embedding simulation using a 256 × 256 pixel image, 8 × 8 blocks, and a complexity threshold of 0.3, the embedding process was carried out selectively on bit-planes that met the complexity criteria. The message “loni” was converted into binary form and embedded into the 0th bit-plane (LSB), which had been identified as a suitable region based on complexity calculations. Although the LSB was used as the embedding medium, the area selection followed the BPCS principle, meaning that embedding was performed only in blocks classified as complex, thereby adhering to the complexity-based segmentation approach.

Simulation results indicate that, throughout the embedding process, a total of 56 pixels experienced changes. Each modification was limited to a range of ±1 intensity value, indicating that alterations occurred only in the least significant bit without affecting the main structure of the image. This demonstrates that the visual quality of the image was preserved and that the changes were not perceptible to the naked eye.

These implementation results support statements in the literature that the BPCS-based approach is capable of maintaining a balance between embedding capacity and image quality. Furthermore, the GUI-based application developed in this study addresses the research problem statement, namely how to implement the BPCS method in a user-friendly system without requiring users to understand the technical details of the algorithm. The processes of image input, message conversion, complexity analysis, embedding, and stego image storage are performed in an integrated manner. Therefore, this study not only confirms the theoretical advantages of the BPCS method but also demonstrates its successful practical implementation as a digital steganography-based information security solution.

5 Conclusion

Based on the results of the design, implementation, and testing stages, it can be concluded that the Bit-Plane Complexity Segmentation (BPCS) method was successfully implemented for steganography in color (RGB) digital images. The developed application is capable of embedding secret messages into images by utilizing complex bit-planes in each color channel without causing significant visual distortion.The embedding process begins by converting the text message into its binary representation using 8-bit ASCII encoding. The binary message is then inserted into 8×8 pixel blocks that have complexity values exceeding the defined threshold. With this approach, embedding is performed only in complex regions of the image, making the presence of the hidden message visually imperceptible. Testing results indicate that pixel value changes after the embedding process remain within a small range. This is demonstrated by comparing pixel values before and after embedding in both decimal and binary forms, where modifications occur only in the lower bit-planes. Therefore, the visual quality of the image is preserved even after the secret message has been embedded.

6. Referensi

[1] f. Kurniawan, z. Sitorus, and r. R. Putra, "combination of cryptography and steganography in improving text data security using des (data encryotion standard) and lsb (least significant bit) methods."

[2] a. Phipps, k. Ouazzane, and v. Vassilev, "computer network and information security, 2022, x, xx-xx," 2022. [online]. Available: http://www.mecs-press.org/

[3] a. Arya, s. Soni, and] m-tech scholar student, "performance evaluation of secrete image steganography techniques using least significant bit (lsb) method," *international journal of computer science trends and technology (ijcst)*, vol. 6, [online]. Available: www.ijcstjournal.org

[4] h. Alshamrani, dr. S. H. Alajmani, dr. R. Y. Alyami, and dr. Ben soh, "comprehensive comparison of image steganography techniques with security enhancement," *international journal of recent technology and engineering (ijrte)*, vol. 14, no. 2, pp. 7–19, jul. 2025, doi: 10.35940/ijrte.a8249.14020725.

[5] h. Caballero, v. Muñoz, and m. A. Ramos-corchado, "a comparative study of steganography using watermarking and modifications pixels versus least significant bit," *international journal of electrical and computer engineering*, vol. 13, no. 6, pp. 6335–6350, dec. 2023, doi: 10.11591/ijece.v13i6.pp6335-6350.

[6] r. Panigrahi and n. Padhy, "an effective steganographic technique for hiding the image data using the lsb technique," *cyber security and applications*, vol. 3, dec. 2025, doi: 10.1016/j.csa.2024.100069.

[7] aqilah syaima' fadel, rianto david saputra, y. Fatma, and risky nanda putra, "analisis keamanan steganografi teks dengan metode lsb (least significant bit) pada citra digital," *jurnal coscitech (computer science and information technology)*, vol. 5, no. 1, pp. 36–41, apr. 2024, doi: 10.37859/coscitech.v5i1.6759.

[8] k. Dharma kusumah, j. Pragantha, and n. Jaya perdana, "steganography implementation of insertion of confidential data on digital image media," *international journal of application on sciences, technology and engineering*, vol. 1, no. 2, pp. 695–702, may 2023, doi: 10.24912/ijaste.v1.i2.695-702.

[9] c. Do xuan, "a proposal to improve the bit plane steganography based on the complexity calculation technique." [online]. Available: www.ijacsa.thesai.org

[10] p. P. Khairnar and p. V. S. Ubale, "steganography using bpcs technology," 2013.

[11] e. Kawaguchi and r. O. Eason, "header for spie use principle and applications of bpcs-steganography." [online]. Available: http://www.datahide.org/bpcse/qtechhv-program-e.html

[12] r. Hidayat, "klasifikasi bit-plane noise untuk penyisipan pesan pada teknik steganography bpcs menggunakan fuzzy inference sistem mamdani," *jurnal rekayasa elektrika*, vol. 11, no. 3, apr. 2015, doi: 10.17529/jre.v11i3.2238.