BIOS: Jurnal Informatika dan Sains
Volume 4 Number 01, 2026, DOI 10.54209/bios.v4i01
E.SSN 2988-6910(Online)
https://seaninstitute.or.id/bersinar/index.php/bios/index

Bit Plane Complexity Segmentation (BPCS)

Firamawati Hia[1], Fortina Lumban Gaol[2], Muhammad Rizqy Aditya Pratama[3]
Fakultas Ilmu Komputer, Prodi Teknik Informatika, Universitas Katolik Santo Thomas Medan

Article Info
Corresponding Author:
Firamawati Hia

ABSTRACT
Bit Plane Complexity Segmentation (BPCS) is a steganographic method that utilizes the visual complexity characteristics of digital images to embed secret information. This method works by dividing an image into several bit-planes, then measuring the level of complexity of each bit-plane block. Blocks with high complexity are considered similar to noise, making them suitable as a medium for data embedding without causing significant visual changes to the original image. The main advantage of BPCS lies in its large data embedding capacity and high level of security, as the hidden information is difficult to detect through visual observation or simple analysis. Therefore, BPCS becomes an effective solution for securing digital data, particularly in applications such as copyright protection, confidential communication, and information security.
Keywords: BPCS, Echo Hiding, visual complexity, digital image

INTRODUCTION

The rapid development of information and communication technology has driven an increasing need for digital data security. Information transmitted through digital media, especially images, is vulnerable to interception, manipulation, and data theft. Therefore, a technique is required that can protect the confidentiality of information without raising suspicion from unauthorized parties. One of the approaches widely used in data security is steganography, which is the technique of hiding information within digital media.

Image steganography has various methods, one of which is Bit Plane Complexity Segmentation (BPCS). This method utilizes the visual characteristics of digital images by dividing the image into several bit-planes. Each bit-plane is analyzed for its level of complexity to determine which parts resemble noise. Regions with high complexity can be used as locations for embedding secret data because the changes are difficult to distinguish by the human visual system.

The main advantage of the BPCS method compared to other steganographic methods is its relatively large data embedding capacity while maintaining the quality of the resulting image. In addition, BPCS offers a higher level of security because the hidden information is not easily detected through visual or simple statistical analysis. With these advantages, the BPCS method is widely applied in various fields, such as digital copyright protection, secure communication, and information security systems.

Literature Review

Various studies have been conducted in the field of image steganography to improve data security and embedding capacity. Conventional methods such as Least Significant Bit (LSB) are widely used due to their simple implementation; however, they have weaknesses in

terms of low security and are easily detected through statistical analysis. To overcome these limitations, more complex methods have been developed, such as transform domain techniques and visual perception-based approaches, one of which is Bit Plane Complexity Segmentation (BPCS).

BPCS was introduced as a steganographic method that utilizes visual complexity in the bit-planes of digital images. Several studies have shown that BPCS is capable of embedding large amounts of data without significantly degrading image quality. In addition, this method has proven to be more resistant to visual detection because the data is embedded in image regions that resemble noise. However, previous research also indicates that the selection of the complexity threshold and block size greatly affects the performance of the BPCS method.

Problem Statement

Although the BPCS method offers advantages in terms of data embedding capacity and security, there are still several issues that require further investigation. One of the main problems is determining the optimal complexity threshold value to distinguish between noise-like areas and informative regions in an image. An incorrect threshold selection can lead to a decrease in image quality or a reduction in the security level of the hidden data.

In addition, the application of the BPCS method to various types of images with different characteristics remains a challenge. Differences in resolution, level of detail, and color variation can affect the results of bit-plane segmentation and the effectiveness of data embedding. Therefore, further research is needed to comprehensively analyze the performance of the BPCS method and to optimize its parameters so that it can be applied more effectively in digital data security.

RESEARCH METHODOLOGY

Research Preparation

The preparation stage is carried out to ensure that all research requirements are fulfilled before the implementation of the BPCS method begins. At this stage, digital image data is prepared to be used as the medium for information embedding. The images used can be either color images or grayscale images in common formats such as BMP or PNG to avoid lossy compression, which may affect the embedding results.

In addition, secret data in the form of text or digital files that will be embedded into the image is also prepared. The software and development environment are determined at this stage, such as the programming language or image processing tools to be used. Initial parameters of the BPCS method, such as bit-plane block size and complexity threshold values, are set based on literature studies to obtain optimal embedding results.

Steps of the BPCS Method

The workflow begins with the decomposition of the image into several bit-planes. Each bit-plane represents different levels of bit significance in the digital image. After that, each bit-plane is divided into small blocks, for example 8×8 pixels, to facilitate complexity analysis in each part of the image.

Next, the complexity value of each bit-plane block is calculated. Blocks with complexity values exceeding the threshold are considered noise-like regions and are selected as locations for embedding secret data. The secret data is then converted into binary form and embedded into the selected blocks. After the embedding process is completed, all bit-planes are recombined to produce the stego image, which visually appears almost identical to the original image.

Result Evaluation

The final stage is the evaluation of the data embedding results using the BPCS method. The evaluation is carried out by comparing the quality of the original image and the stego image using parameters such as Peak Signal to Noise Ratio (PSNR) and Mean Squared Error (MSE). In addition, a successful extraction test is performed to ensure that the embedded information can be fully recovered without any distortion or data loss.

RESULTS AND DISCUSSION

Initial Display of the BPCS Steganography System

The figure shows the initial interface of the BPCS Steganography application before the data embedding process is performed. At this stage, the system does not yet display any image or steganography results because the user has not uploaded an image or entered a secret message. This interface functions as the main user interface that connects the user to the encoding process using the Bit Plane Complexity Segmentation method.

At the top of the interface, there is an “Upload Photo” button used to select a digital image as the medium for embedding the secret message. In addition, there is a text input field labeled “Write Secret Message Here...” which allows the user to enter the text message to be embedded into the image. The “Encode Process” button is used to start the embedding process after the image and secret message have been provided.

Discussion of the Initial Interface Function

This initial interface is designed to facilitate users in operating the steganography system without requiring deep technical knowledge. With a simple workflow, users only need to upload an image, type a secret message, and press the encode button. Once the encoding process is executed, the system processes the image using the BPCS method and displays the stego image along with supporting information such as complexity grids and image quality values.

The presence of additional buttons such as “Stego Result” and “Red Overlay Grid (Zoomed)” indicates that the system does not only display the final output but also provides a visualization of the BPCS process. This helps in understanding how data is embedded into high-complexity bit-plane blocks. Thus, this initial interface plays an important role in supporting the successful implementation and analysis of the BPCS method in this study.

Figure 1. Initial Interface

Image Selection Process (Upload Photo)

The figure shows the process of selecting a digital image to be used as the cover image in the Bit Plane Complexity Segmentation (BPCS) steganography method. At this stage, the system displays an Open File dialog window that allows the user to choose an image file from the computer storage. Supported image formats include .jpg, .png, and .bmp, in accordance with the requirements of the steganography system.

In the figure, the user is shown selecting an image file named *download (14).jpeg*. After the image is selected and the "Open" button is clicked, the system loads the image into the application and displays it in the image display area. This stage represents the initial step before the secret message embedding process is carried out.

Discussion of the Image Upload Process

The image upload process is an important stage because the quality and characteristics of the image significantly affect the embedding results using the BPCS method. Images with high levels of detail and color variation tend to have more bit-plane blocks with high complexity, thereby increasing the capacity for embedding secret data.

With the availability of a file selection feature through a graphical interface, the system simplifies the process for users in selecting appropriate images without requiring manual configuration. This demonstrates that the system not only focuses on the implementation of the BPCS algorithm but also emphasizes usability in the image steganography process.

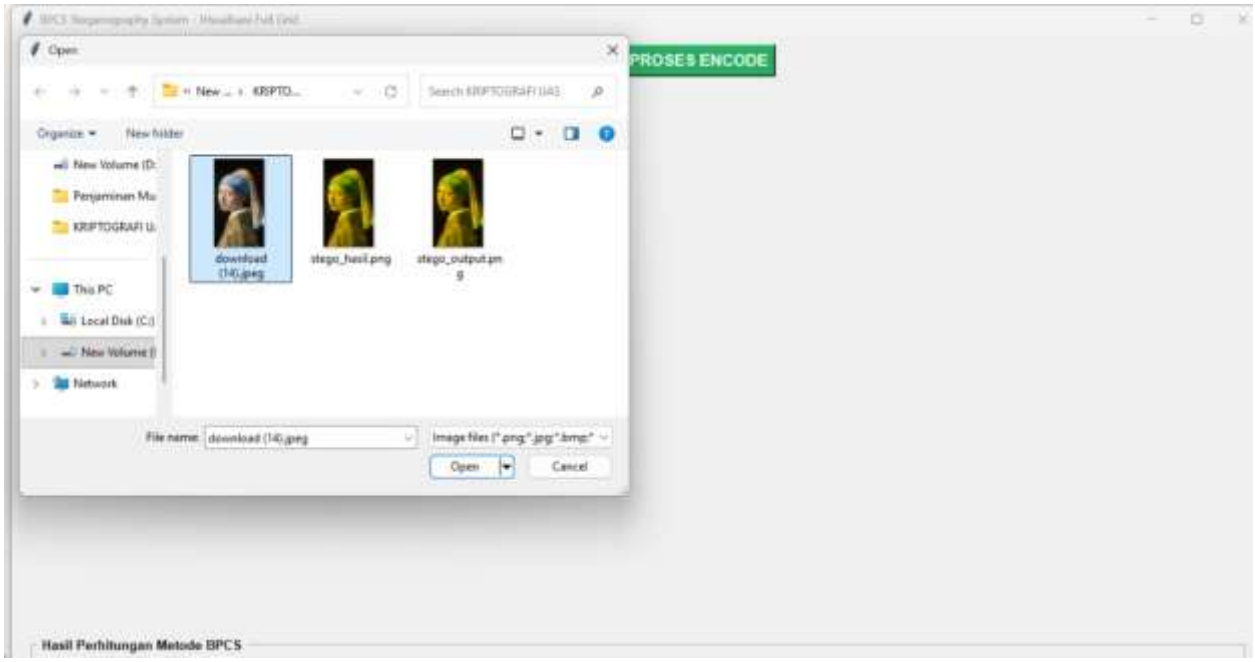

Figure 2. Digital Image Selection Process

System Notification After Image Loading

The figure shows a system notification displaying the message "Photo Successfully Loaded," which appears after the user selects and uploads a digital image into the BPCS steganography application. This notification indicates that the system has successfully read the image file and loaded it into memory without any errors.

The successful image loading serves as an initial indicator that the image format and size are compatible with the system specifications. At this stage, the image is ready for further processing, namely bit-plane decomposition and complexity analysis, which form the basis of the Bit Plane Complexity Segmentation (BPCS) method.

Discussion of the Image Loading Stage

The image loading stage plays an important role in the overall steganography process, as any error at this stage would prevent the encoding process from being executed. With the presence of a success notification, the system provides clear feedback to the user that the image is ready to be used as a cover image.

After the image has been successfully loaded, further functions such as the “Encode Process,” “Stego Result,” and “Red Overlay Grid” buttons become available. This demonstrates that the system is designed in a sequential manner, where each process can only be executed after the previous stage has been successfully completed. This approach helps prevent user errors and ensures that the BPCS steganography process runs according to the intended workflow.

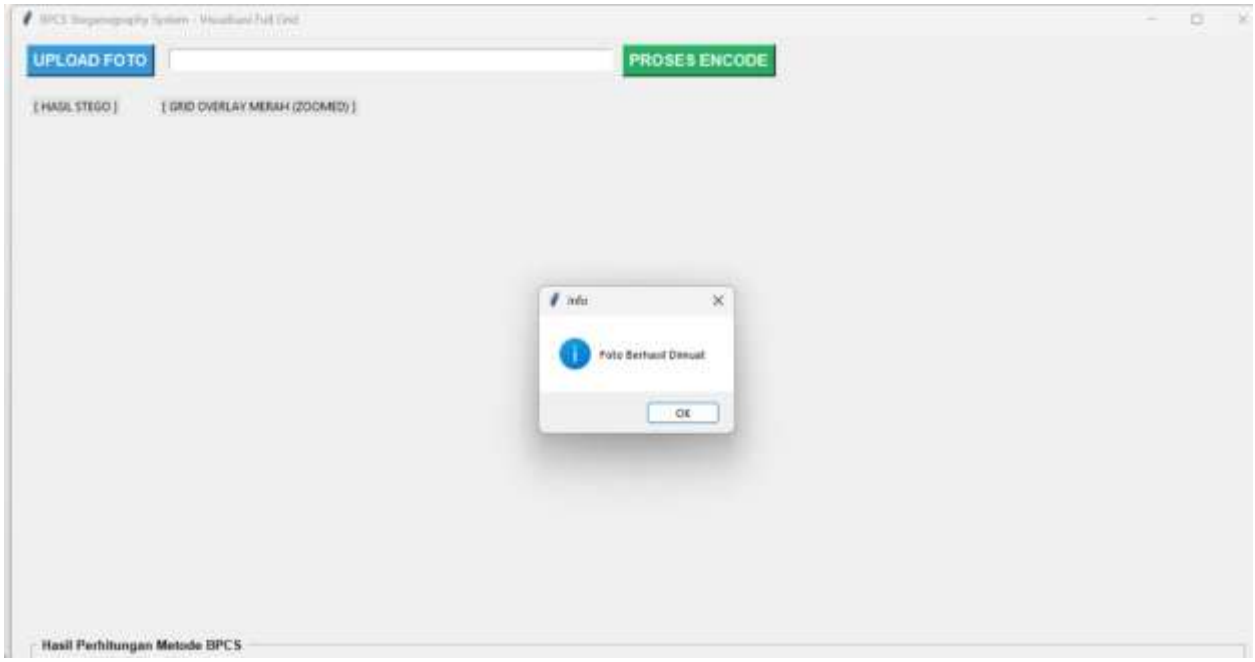

Figure 3. System Notification Message

Result of Secret Message Encoding Process

The figure shows the result of the encoding process using the Bit Plane Complexity Segmentation (BPCS) method. On the left side, the original image (cover image) is displayed, while on the right side, the stego image is shown, which is the image that has been embedded with a secret message in the form of the text: “SAYA BERKULIAH DI UNIVERSITAS KATOLIK SANTO THOMA.” The encoding process is performed after the image has been successfully loaded and the secret message has been entered into the input field.

Visually, there is almost no noticeable difference between the original image and the stego image. This indicates that the BPCS method successfully embeds secret data into high-complexity bit-plane blocks, so that the resulting changes do not significantly affect the visual perception of the image.

Full Grid Visualization in the BPCS Method

In the stego image, red grid markers can be observed in certain regions. These grids represent bit-plane blocks with high complexity that are used as embedding locations for the secret message. This visualization helps in understanding how the BPCS method determines data embedding areas.

By displaying the full grid, the system illustrates that data embedding is not performed randomly, but is based on complexity calculations of each block. Blocks that resemble noise

are selected because modifications in these areas are difficult for the human visual system to detect, thereby increasing the security of the steganographic process.

Image Quality Calculation and Analysis Results

At the bottom of the application interface, the results of the BPCS computation are displayed in the form of binary representations of several bit-plane blocks. This information shows that the system has successfully converted the image into binary form and calculated the complexity of each block according to the BPCS algorithm.

The Peak Signal-to-Noise Ratio (PSNR) value obtained is 87.85 dB. This high PSNR value indicates that the level of distortion between the original image and the stego image is very low. Therefore, the quality of the stego image is well preserved even after the secret message embedding process has been carried out.

Figure 4. Result of Secret Message Encoding Process

CONCLUSION

Based on the research results and implementation of the Bit Plane Complexity Segmentation (BPCS) method in the digital image steganography system, it can be concluded that the BPCS method is capable of embedding secret messages into images with a high level of security. The embedding process is performed on bit-plane blocks with high complexity so that the resulting changes are not easily detected by human visual observation. This indicates that the BPCS method is effective in maintaining the confidentiality of embedded information.

The image quality evaluation results show that the difference between the original image and the stego image is very small. The obtained Peak Signal to Noise Ratio (PSNR) value of 87.85 dB indicates that the distortion caused by the secret message embedding process is very low. Thus, the visual quality of the stego image remains well preserved even after the steganography process has been applied.

In addition, the full grid visualization of the bit-plane blocks demonstrates that data embedding in the BPCS method is performed in a structured manner based on complexity calculations, rather than randomly. With a large data embedding capacity and maintained image quality, the BPCS method can be considered an effective solution for digital data

security, particularly in applications involving confidential communication and information protection.

REFERENCES

1. Kawaguchi, E., & Eason, R. O. (1998). *Principle and applications of BPCS steganography*. Proceedings of SPIE – Electronic Imaging, 3528, 464–473.
2. Johnson, N. F., Duric, Z., & Jajodia, S. (2001). *Information hiding: Steganography and watermarking – Attacks and countermeasures*. Springer.
3. Provos, N., & Honeyman, P. (2003). *Hide and seek: An introduction to steganography*. IEEE Security & Privacy, 1(3), 32–44.
4. Gonzalez, R. C., & Woods, R. E. (2018). *Digital Image Processing* (4th ed.). Pearson Education.
5. Kurniawan, D., & Pratama, A. (2019). *Analisis steganografi citra menggunakan metode Bit Plane Complexity Segmentation (BPCS)*. Jurnal Teknologi Informasi, 13(2), 85–92.
6. Tarigan, R. S., & Dwiatma, G. (2022). *Analisa Steganografi Dengan Metode Bpcs (Bit-Plane Complexity Segmentation) Dan Lsb (Least Significant Bit) Pada Pengolahan Citra*.
7. Chidambaram, G., & Vijayalakshmi, S. (2022, December). Data Privatization and Security using Bit Plane Complexity Segmentation. In *2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)* (pp. 451-458). IEEE.
8. Yusdartono, D. Y., & Yusdartono, H. M. (2024). Combination of the Spritz Algorithm and the Bit Plane Complexity Segmentation Technique in Text Security. *Instal: Jurnal Komputer*, *16*(05), 1-8.
9. Kautsar, A., & Ikhsan, M. (2025). Implementation of the Advanced Encryption Standard (AES) Algorithm and Bit Plane Complexity Segmentation (BPCS) Steganography Technique for Enhancing Text File Security. *Sistemasi: Jurnal Sistem Informasi*, *14*(2), 956-968.
10. Debnath, S., Mohapatra, R. K., & Dash, R. (2023). Secret data sharing through coverless video steganography based on bit plane segmentation. *Journal of Information Security and Applications*, *78*, 103612.
11. Debnath, S., Mohapatra, R. K., & Kulkarni, T. S. (2023, November). Bit plane segmentation and lbp-based coverless video steganography for secure data transmission. In *International Conference on Computer Vision and Image Processing* (pp. 256-268). Cham: Springer Nature Switzerland.