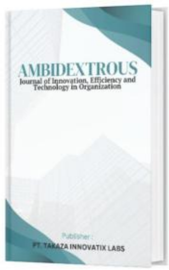
Ambidextrous: Journal of Innovation, Efficiency and Technology in Organizations

https://journal.takaza.id/index.php/ambidextrous

Vol. 05, No. 02, 2023, pp. 286-301
E-ISSN: 3031-7002

E-mail:ambidex@takaza.id



Implementation Using the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) Methods in Message Insertion in Digital Images

Theo Hasri Pratama
Muhammadiyah University of North Sumatra
Corresponding Author e-mail: dio966214@gmail.com

Article History:
Received: 02-08-2026
Revised: 01-09-2026
Accepted: 01-09-2026

Keywords: *Digital Image, Information Security, Least Significant Bit, Pixel Value Differentiation, Steganography*

Abstract: *The increasing use of digital information has created a growing need to protect data from interception, alteration, and unauthorized access. Steganography provides an alternative security mechanism by concealing secret information within digital images without causing significant visual distortion. This study aims to implement and compare the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods for embedding and extracting SQL files in PNG and BMP images. The study employed an applied research approach involving the development of a web-based steganography application using Python and Streamlit. The experiment used 50 digital images and SQL files as secret messages. The evaluation was conducted through functional testing, message-integrity verification, and image-quality measurement using Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The results indicate that both methods produced visually high-quality stego images, as reflected by relatively low MSE values and high PSNR values. The LSB method successfully preserved the integrity of all extracted SQL files, achieving a 100% message-integrity rate. The PVD method successfully embedded the messages, but some extracted SQL files contained character changes and therefore did not fully match the original files. These findings indicate that LSB was more reliable than PVD for preserving SQL-file integrity under the experimental conditions of this study, while both methods were capable of maintaining good visual image quality. The developed application can support the practical implementation and evaluation of image-based steganography for digital information protection.*

How to Cite: Theo Hasri Pratama. (2026). *Implementation Using the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) Methods in Message Insertion in DIGITAL Images. 5(2). pp 286-301* https://doi.org/10.61536/ambidextrous.v5i02.623

https://doi.org/10.61536/ambidextrous.v5i02.624

Introduction

The development of information and communication technology has transformed various aspects of life, such as education, government, the business world, and social activities.

These advances enable faster and more efficient data processing, storage, and distribution. In the field of Information Systems, data and information are key components that must be managed properly, as digital information has become a crucial asset in supporting various activities and decision-making.

The increasing use of information technology has also been accompanied by a growing need for information security. According to Akmal et al. (2023), data exchange processes that are no longer limited by space and time increase the risk of theft, misuse, interception, data alteration, and unauthorized access. Therefore, information protection is a crucial aspect of information system management.

One technique for improving information security is steganography, a method of hiding secret messages in digital media without the knowledge of others. According to Lasarus (2021), steganography can be applied to images, audio, and video. Among these media, digital images are the most widely used because they have a large number of pixels and bits that can be modified without causing significant visual changes. These characteristics make digital images effective as a medium for embedding secret information (Purbaningrum et al., 2023).

The steganography methods widely used in digital images are Least Significant Bit (LSB) and Pixel Value Differencing (PVD). The LSB method inserts a message by modifying the lowest bit in each pixel so that image changes are difficult to detect, while the PVD method utilizes the difference in values between pixels to determine the message insertion capacity. According to Gustiawan et al. (2023), the PVD method adjusts the number of inserted bits based on the characteristics of the pixels in the digital image.

The differences in the characteristics of LSB and PVD indicate that each method has advantages in the message insertion process. Therefore, implementation and testing are needed to determine the ability of both methods in maintaining image quality and the success of the message insertion and retrieval process based on the Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) parameters.

Based on these problems, this study aims to implement the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods in the process of embedding and extracting messages in digital images and analyzing the quality of the embedded images using PSNR and MSE. This research is important as an alternative application of steganography in improving digital information security. The novelty of the research lies in the implementation of both methods in one steganography application using PNG and BMP format images with messages in the form of SQL files that are evaluated based on the success of embedding, extraction, and the quality of the embedded images.

Research Methods

This research uses an applied research type with a system implementation method. The research focuses on the design and development of a steganography system for inserting and retrieving secret messages in digital images using the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods. The selection of these methods is based on the need to produce a system capable of maintaining information confidentiality while maintaining the quality of digital images after the message insertion process. The system development was carried out as a solution to information security problems in the digital data exchange process as explained by Akmal et al. (2023).

The research instrument is a web-based steganography system software developed to support the embedding and extraction process. The system accepts input in the form of digital images in PNG and BMP formats as embedding media and .sql files as secret messages. The system is equipped with image inspection features, embedding capacity analysis, LSB or PVD method selection, method detection in the extraction process, and image quality measurement using Mean Square Error (MSE)

https://doi.org/10.61536/ambidextrous.v5i02.624

and Peak Signal to Noise Ratio (PSNR) parameters. Data analysis techniques are carried out through functional testing of the embedding and extraction process, then evaluating image quality based on MSE and PSNR values and the success of the system in restoring .sql files according to the original embedded data.

The population in this study is digital images that can be used as steganography media. The research sample consists of digital images in PNG and BMP formats used as message insertion media and .sql files as inserted data and re-extracted using the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods.

The research procedure begins with the design of a steganography system based on the needs of the embedding and extraction processes. The next stage is the development of a web-based application that implements the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods. After the system is developed, the process of inserting a .sql file into a digital image is carried out using the selected method, then the system produces a stego image. Next, the extraction process is carried out to recover the inserted file. The final stage of the research is system testing by verifying the success of the embedding and extraction processes and evaluating the quality of the stego image using the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters.

Results and Discussion

System Requirements

System requirements are the initial design stage to identify the components needed for the system to run properly, including hardware, software, and functional requirements.

The system developed is a computer-based steganography application for the process of inserting and extracting SQL files in digital images using the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods, and is equipped with image quality evaluation based on the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters.

The system requirements in this study are grouped into hardware requirements, software requirements, and functional requirements to support the system implementation and testing process.

1. Hardware Requirements

   The hardware used in the development and testing of the system in this study was a MacBook Air M2 laptop. This device was used to run the designed steganography application, from message insertion to message retrieval in digital images. The hardware specifications used are as follows:

   Processor: Apple M2 Chip
   RAM: 8 GB
   Storage: 256 GB SSD

   In addition, this device is also equipped with input components in the form of a keyboard and touchpad which function to operate the system, as well as output components in the form of a screen (display) which is used to display the application interface and the results of the processes carried out.

   In general, the system being developed doesn't require high hardware specifications. It can still run on devices with minimal specifications, such as a dual-core processor or equivalent, at least 4 GB of RAM, and at least 128 GB of storage. With these specifications, the system can still run all key features optimally.

2. Software Requirements

   The software used in the system development and testing process in this study serves as a key component in building and running steganography applications. This software is used to support system development, data processing for message insertion and retrieval, and the presentation of the application interface to users.

https://doi.org/10.61536/ambidextrous.v5i02.624

The software used in this research includes:

1. Operating System: macOS
2. Programming Language: Python
3. Framework : Streamlit
4. Supporting Libraries: PIL (Python Imaging Library) for image processing and Numpy for numerical data processing
5. Code Editor: Visual Studio Code

The Python programming language was chosen for its ability to provide a variety of libraries that support digital image processing and ease of application development. The Streamlit framework is used to build interactive and user-friendly web-based application interfaces. Furthermore, libraries like PIL are used to facilitate the digital image manipulation required for the Least Significant Bit (LSB) and Pixel Value Differentiation (PVD) methods.

3. System Functional Requirements

The functional requirements of the system are those related to the main functions that the system must have in order to run according to the established research objectives. In this research, the system developed is a web-based steganography application used to perform the process of inserting and retrieving messages in digital images by utilizing the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods.

These functional requirements are designed to support the entire system's workflow, from data input and processing to output in the form of stego images and message extraction. With well-defined functional requirements, the system is expected to operate systematically, efficiently, and in accordance with user needs.

The functional requirements of the system in this research are as follows:

1. The system can accept input in the form of digital images as a medium for inserting messages.
2. The system can accept input in the form of an SQL file as a secret message to be inserted.
3. The system can check the image to determine whether the image contains a message or not.
4. The system can calculate the maximum capacity of the image in the insertion process using the LSB and PVD methods.
5. The system can provide information about image suitability based on a comparison of image capacity with message size.
6. The system can perform the message insertion process using the Least Significant Bit (LSB) method.
7. The system can perform the message insertion process using the Pixel Value Differencing (PVD) method.
8. The system can display the embedded image (stego image).
9. The system can calculate the quality of the embedded image using the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters.
10. The system can identify the embedding method used in stego images.
11. The system can perform the process of retrieving messages (extraction) from stego images.
12. The system can display the message extraction results in the form of SQL files.
13. The system provides features to download stego images and message extraction files.

https://doi.org/10.61536/ambidextrous.v5i02.624

14. The system can perform message checks to ensure that the extraction results match the original inserted file.

    With these functional requirements, the system developed is expected to be able to carry out the entire steganography process optimally, starting from the insertion stage to the message extraction process, while maintaining image quality in accordance with the research objectives.

System Implementation

System implementation is the stage of applying the previously designed results into an application that can be used directly by users. At this stage, the designed steganography system is realized as a web-based application utilizing the Python programming language and the Streamlit framework.

The developed system aims to embed and extract messages in the form of SQL files into digital images using the Least Significant Bit (LSB) and Pixel Value Differentiation (PVD) methods. Furthermore, the system is equipped with a feature to analyze the quality of the embedded images using the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters.

In its implementation, the application is divided into several main sections: the Home page, the Embedded page, and the Extraction page. Each section is designed to perform specific functions according to the user's needs in the steganography process.

1. Home Page Implementation

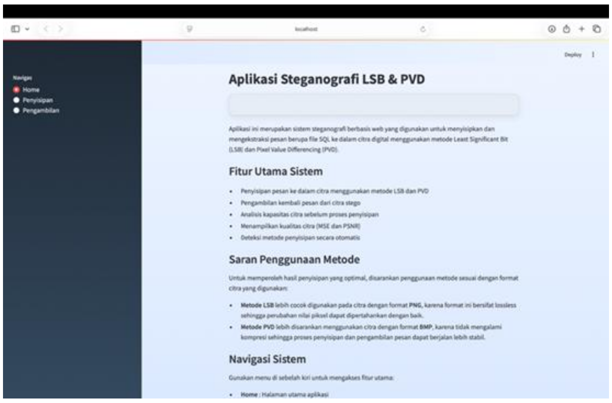


Figure 1 Home Page

Based on Figure 1, the Home page of the steganography application displays the application title, general information about the system's functions, and the main features available. Furthermore, there's a navigation menu in the sidebar that makes it easier for users to access the Insertion and Retrieval pages as needed.

2. Embedding Implementation

https://doi.org/10.61536/ambidextrous.v5i02.624

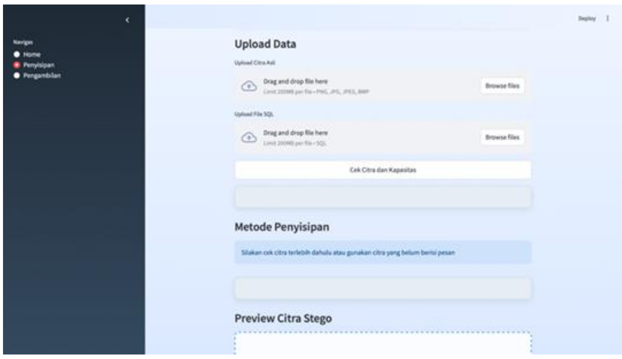


Figure 2 Initial Insertion Page

Based on Figure 2, the initial page of the embedding process in the steganography application is displayed. On this page, users can upload digital images and SQL files to be used in the message embedding process. The system also provides image and capacity checking features before the embedding process begins.

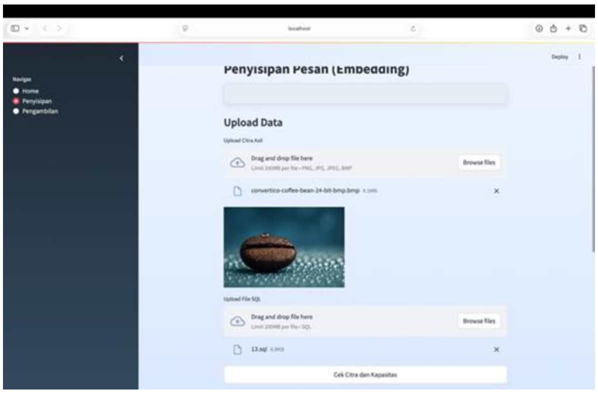


Figure 3 Data Upload Page

Based on Figure 3, the data upload page for the insertion process is displayed. At this stage, the user is asked to upload a digital image as the insertion medium and an SQL file as the message to be inserted. Additionally, the system displays a preview of the selected image to ensure it meets the insertion requirements.

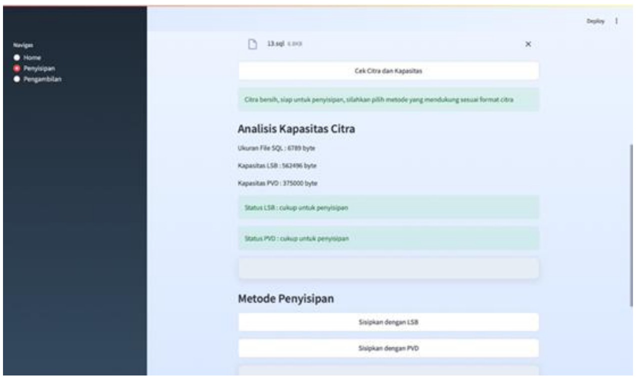


Figure 4 Image and capacity analysis

Based on Figure 4, the image verification process is performed before message insertion. At this stage, the system first verifies whether the image used is still clean or

https://doi.org/10.61536/ambidextrous.v5i02.624

contains a message. If the image is declared valid, the system proceeds to the image capacity analysis stage.

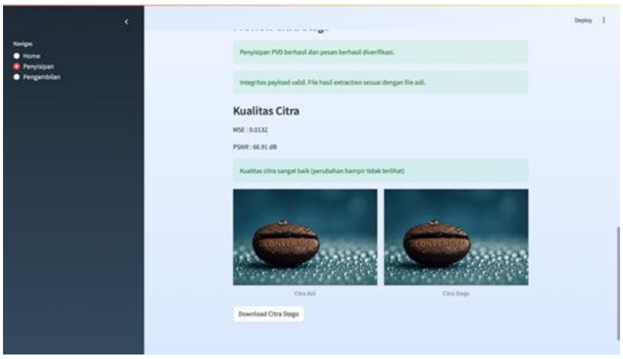


Figure 5 Insertion Results

Based on Figure 5, the results of the message embedding process into a digital image are displayed. Initially, the system displays image quality information in the form of Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) values, which are used to measure the degree of change in the image after the embedding process.

Based on the obtained values, the PSNR value is quite high, indicating that the changes occurring in the image are relatively small, so the image quality is maintained and the visual differences are not significantly visible. In addition to displaying image quality, the system also provides information regarding the results of the message inspection after the embedding process is complete. This inspection aims to determine whether the embedded message can be properly restored through the extraction process.

Next, the system displays a side-by-side comparison of the original and stego images to make it easier for users to see the differences in the embedding results. Visually, the differences between the original and stego images are not significantly visible, so image quality is maintained well after the embedding process. Finally, the system provides a feature to download the stego image as the result of the embedding process.

3. Extraction Implementation

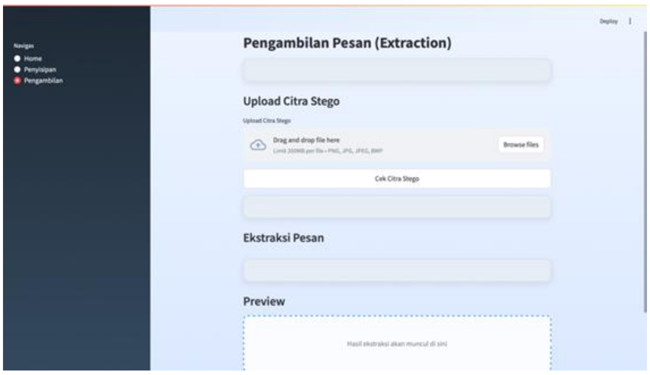


Figure 6 Initial Message Retrieval Page

Figure 6 displays the initial page of the message extraction process in the steganography application. On this page, users can upload the stego image to be used in the extraction process. The system also provides a feature to check the stego image before the message extraction process begins.

https://doi.org/10.61536/ambidextrous.v5i02.624

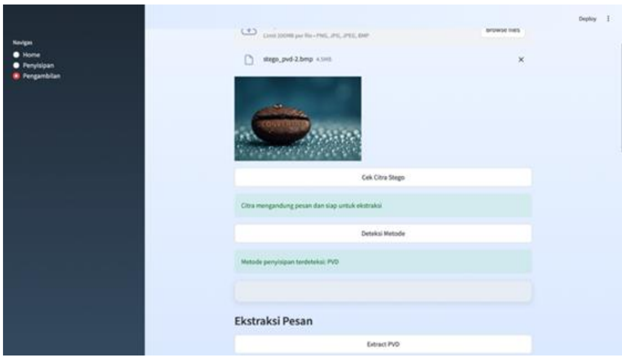


Figure 7 Extraction Process

Figure 7 shows the extraction process page in the steganography application used to retrieve the message embedded in the stego image. At this stage, the user first uploads the stego image to be used in the message retrieval process.

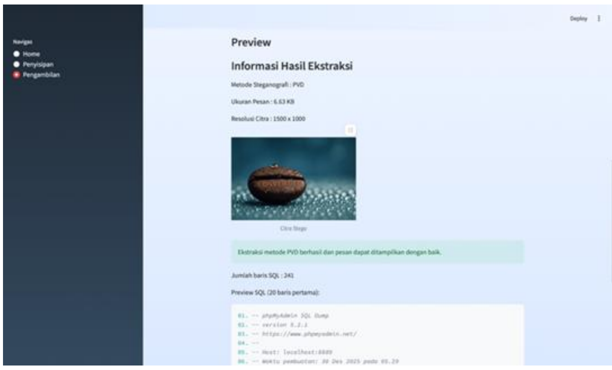


Figure 8 Results of the Extraction Process

Figure 8 displays the results of the extraction process in the steganography application after the message has been successfully extracted from the stego image. At this stage, the system displays the extraction results, including the steganography method used, the message size, and the resolution of the processed stego image.

System Testing

System testing was conducted to ensure that the steganography application could perform the embedding, extraction, and image quality measurement functions using the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) parameters.

The test used 50 digital images in PNG and BMP formats, along with SQL files as embedded messages. The Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods were tested based on the success of the embedding process, extraction, message integrity, and PSNR and MSE values.

The test results were obtained by comparing the extracted SQL file to the original SQL file, then analyzing the quality of the stego image based on the PSNR and MSE values.

The results show that the Least Significant Bit (LSB) method successfully performed the embedding and extraction processes on all test data. The Pixel Value Differentiation (PVD) method also successfully embedded all images, but still found character changes in some of the extracted SQL files, demonstrating higher sensitivity than the LSB method in maintaining message integrity.

1. Embedding Testing Using Least Significant Bit (LSB)

https://doi.org/10.61536/ambidextrous.v5i02.624

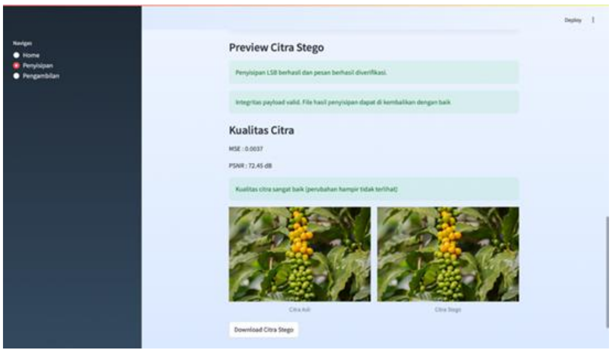


Figure 9 Test Results of One LSB Embedding

Based on Figure 9, it shows the results of the embedding process test using the Least Significant Bit (LSB) method on digital images. From the test results obtained, the message insertion process can be carried out well by producing a PSNR value of 72.45 dB and an MSE value of 0.0037. These values indicate that the changes in the stego image are relatively very small so that the image quality remains good and the visual differences are almost indistinguishable from the original image. In addition, the results of the message inspection show that the extracted SQL file remains consistent with the original inserted file so that the embedding and extraction processes can run smoothly.

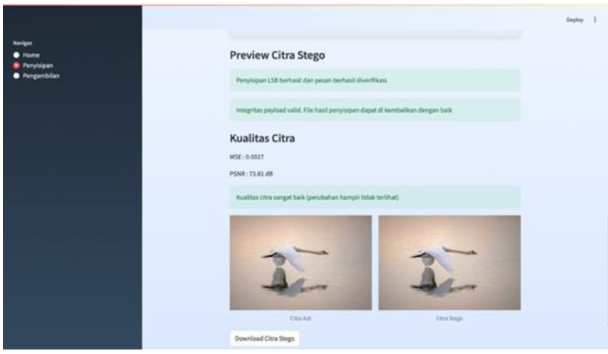


Figure 10 Results of the Second LSB Embedding Test

Figure 10 shows the results of the Least Significant Bit (LSB) embedding test on the second digital image. The test results indicate that the message embedding process was successful, with a PSNR value of 73.81 dB and an MSE value of 0.0027.

2. Extraction Testing Using Least Significant Bit (LSB)

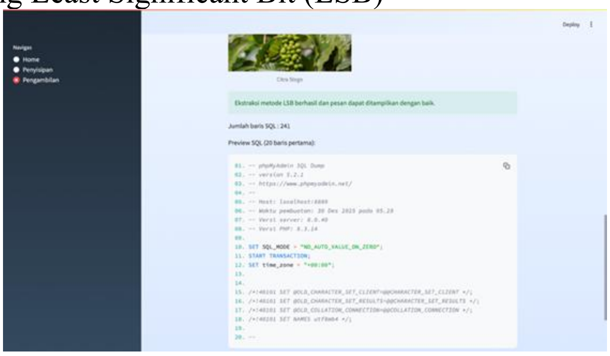


Figure 11 Test Results of one SLB Extraction

Ambidextrous: Journal of Innovation Efficiency and Technology in Organizations
https://doi.org/10.61536/ambidextrous.v5i02.624

Based on Figure 11, the results of the extraction process test using the Least Significant Bit (LSB) method are displayed. In this test, the system successfully detected the insertion method used and successfully retrieved the SQL file from the stego image. The extraction results are then displayed as a preview of the SQL file contents to make it easier for users to view the retrieved data. Furthermore, the message inspection results indicate that the extracted SQL file remains consistent with the original inserted file, so the extraction process using the LSB method can run smoothly without experiencing any data changes.

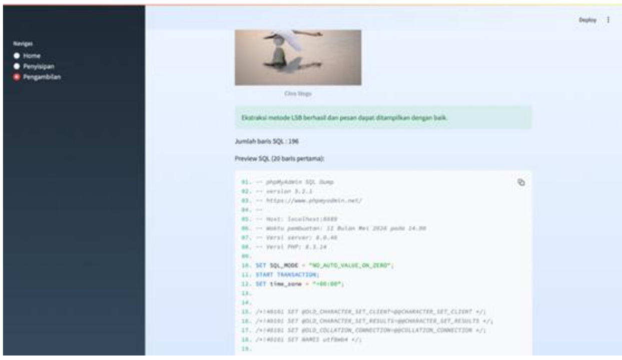


Figure 12 Results of the Second LSB Extraction Test

Figure 12Figure 1 shows the results of the second extraction test using the Least Significant Bit (LSB) method. Based on the test results, the system successfully retrieved messages from stego images and displayed the contents of the SQL file in preview form. The system also successfully checked the messages so that the extracted SQL file could be restored without any data changes. These results indicate that the Least Significant Bit (LSB) method is able to maintain message integrity during the embedding and extraction processes.

3. Embedding Testing Using Pixel Differencing (PVD)

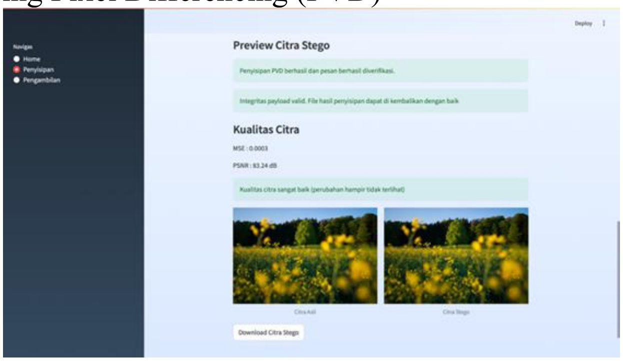


Figure 13 Test Results of One PVD Embedding

Based on Figure 13, it shows the results of the embedding test using the Pixel Value Differencing (PVD) method on digital images. From the test results, the SQL file insertion process was successfully executed, producing a PSNR value of 83.24 dB and an MSE value of 0.0003. These values indicate that the changes in the stego image are very small so that the visual quality of the image remains good and the difference between the original image and the stego image is almost indistinguishable visually.

https://doi.org/10.61536/ambidextrous.v5i02.624

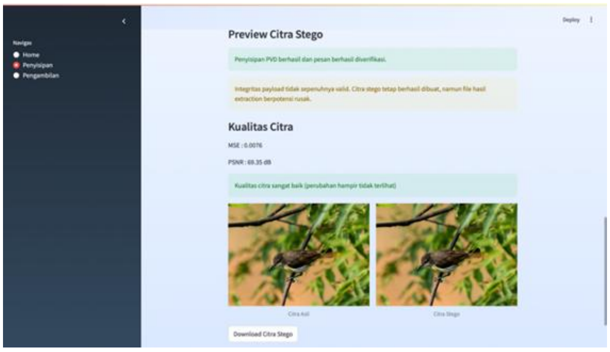


Figure 14 Results of the Second PVD Embedding Test

Based on Figure 14, it shows the test results of the two embedding processes using the Pixel Value Differencing (PVD) method. Based on the results obtained, the system successfully produced a stego image with a PSNR value of 69.35 dB and an MSE value of 0.0076. These values indicate that the changes in the image after the embedding process are still relatively small so that the visual quality of the stego image remains good and the differences with the original image are not visible.

4. Extraction Testing Using Pixel Value Differentiating (PVD)

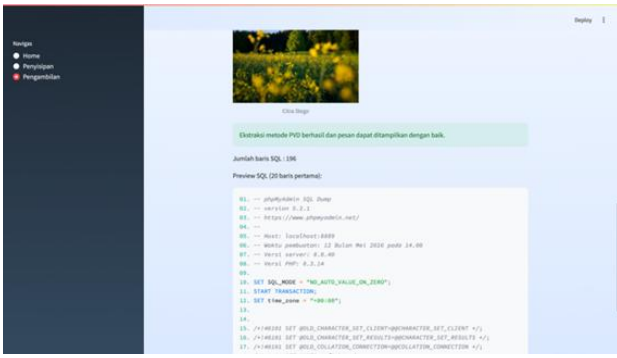


Figure 15 Results of One Extraction PVD Test

Based on Figure 15, the results of the extraction process using the Pixel Value Differentiation (PVD) method are shown. The test results showed that the system successfully recognized the insertion method used and successfully retrieved the SQL file from the stego image. The extracted file is then displayed in a preview format, allowing the user to directly view the retrieved data.

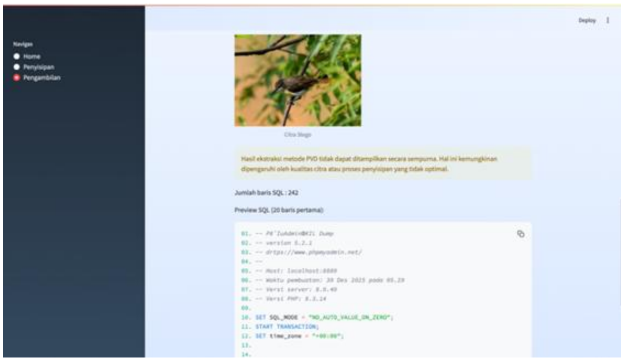


Figure 16 Results of the Second PVD Extraction Test

https://doi.org/10.61536/ambidextrous.v5i02.624

Based on Figure 11 shows the results of testing the two extraction processes using the Pixel Value Differentiation (PVD) method. Based on the test results, the system successfully executed the extraction process and displayed a preview of the extracted SQL file contents. However, a message inspection revealed that the resulting SQL file did not completely match the original file previously embedded into the stego image.

5. PSNR and MSE Value Testing

Table 1. PSNR and MSE results

NO	Image Name	PSNR LSB	MSE LSB	PSNR PVD	MSE PVD
1	Test 1	72.47 dB	0.0037	67.85 dB	0.0107
2	Test 2	72.45 dB	0.0037	67.33 dB	0.0120
3	Test 3	86.33 dB	0.0002	81.78 dB	0.0004
4	Test 4	74.56 dB	0.0023	69.37 dB	0.0075
5	Test 5	72.45 dB	0.0037	59.98 dB	0.0654
6	Test 6	72.94 dB	0.0033	66.59 dB	0.0143
7	Test 7	72.45 dB	0.0037	66.62 dB	0.0142
8	Test 8	73.00 dB	0.0033	67.12 dB	0.0126
9	Test 9	72.76 dB	0.0034	66.36 dB	0.0150
10	Test 10	73.03 dB	0.0032	66.12 dB	0.0159
11	Test 11	72.48 dB	0.0037	67.25 dB	0.0122
12	Test 12	72.46 dB	0.0037	66.29 dB	0.0153
13	Test 13	72.49 dB	0.0037	66.23 dB	0.0155
14	Test 14	72.49 dB	0.0037	67.96 dB	0.0104
15	Test 15	72.47 dB	0.0037	66.92 dB	0.0132
16	Test 16	71.76 dB	0.0043	67.55 dB	0.0114
17	Test 17	72.49 dB	0.0037	66.33 dB	0.0151
18	Test 18	72.50 dB	0.0037	66.83 dB	0.0135
19	Test 19	71.96 dB	0.0041	65.55 dB	0.0181
20	Test 20	72.46 dB	0.0037	66.65 dB	0.0141
21	Test 21	72.47 dB	0.0037	62.61 dB	0.0356
22	Test 22	72.41 dB	0.0037	66.96 dB	0.0131
23	Test 23	72.29 dB	0.0038	66.82 dB	0.0135
24	Test 24	72.45 dB	0.0037	66.58 dB	0.0143
25	Test 25	73.09 dB	0.0032	66.75 dB	0.0137
26	Test 26	73.03 dB	0.0032	66.45 dB	0.0147
27	Test 27	72.44 dB	0.0037	66.61 dB	0.0142

https://doi.org/10.61536/ambidextrous.v5i02.624

28	Test 28	72.45 dB	0.0037	66.10 dB	0.0160
29	Test 29	72.31 dB	0.0038	66.90 dB	0.0133
30	Test 30	72.59 dB	0.0036	61.22 dB	0.0491
31	Test 31	82.38 dB	0.0004	76.61 dB	0.0014
32	Test 32	72.48 dB	0.0037	66.65 dB	0.0141
33	Test 33	72.43 dB	0.0037	66.03 dB	0.0162
34	Test 34	72.42 dB	0.0037	67.39 dB	0.0119
35	Test 35	72.38 dB	0.0038	66.05 dB	0.0161
36	Test 36	72.45 dB	0.0037	66.93 dB	0.0132
37	Test 37	72.51 dB	0.0036	66.05 dB	0.0161
38	Test 38	72.42 dB	0.0037	65.34 dB	0.0190
39	Test 39	72.44 dB	0.0037	66.17 dB	0.0157
40	Test 40	72.11 dB	0.0040	67.19 dB	0.0124
41	Test 41	72.74 dB	0.0035	67.96 dB	0.0104
42	Test 42	72.48 dB	0.0037	67.08 dB	0.0127
43	Test 43	72.45 dB	0.0037	66.08 dB	0.0161
44	Test 44	72.51 dB	0.0036	66.28 dB	0.0153
45	Test 45	72.50 dB	0.0037	66.38 dB	0.0150
46	Test 46	72.83 dB	0.0034	66.45 dB	0.0147
47	Test 47	72.44 dB	0.0037	66.29 dB	0.0153
48	Test 48	72.98 dB	0.0033	67.03 dB	0.0129
49	Test 49	72.32 dB	0.0038	67.02 dB	0.0129
50	Test 50	72.46 dB	0.0037	67.38 dB	0.0119

Based on Table 1, the results of tests conducted on 50 digital images indicate that both the Least Significant Bit (LSB) and Pixel Value Differentiation (PVD) methods are capable of producing good-quality stego images. This can be seen from the relatively high PSNR values and relatively low MSE values in each test data set.

6. Message Integrity Testing

Table 2. Message Integration Test Results

No	Image Name	LSB Message Status	PVD Message Status
1	Test 1	In accordance	It is not in accordance with
2	Test 2	In accordance	In accordance
3	Test 3	In accordance	In accordance
4	Test 4	In accordance	It is not in accordance with
5	Test 5	In accordance	It is not in accordance with

https://doi.org/10.61536/ambidextrous.v5i02.624

6	Test 6	In accordance	In accordance
7	Test 7	In accordance	In accordance
8	Test 8	In accordance	It is not in accordance with
9	Test 9	In accordance	In accordance
10	Test 10	In accordance	It is not in accordance with
11	Test 11	In accordance	In accordance
12	Test 12	In accordance	In accordance
13	Test 13	In accordance	In accordance
14	Test 14	In accordance	In accordance
15	Test 15	In accordance	It is not in accordance with
16	Test 16	In accordance	It is not in accordance with
17	Test 17	In accordance	In accordance
18	Test 18	In accordance	In accordance
19	Test 19	In accordance	In accordance
20	Test 20	In accordance	In accordance
21	Test 21	In accordance	It is not in accordance with
22	Test 22	In accordance	It is not in accordance with
23	Test 23	In accordance	It is not in accordance with
24	Test 24	In accordance	In accordance
25	Test 25	In accordance	In accordance
26	Test 26	In accordance	In accordance
27	Test 27	In accordance	In accordance
28	Test 28	In accordance	In accordance
29	Test 29	In accordance	In accordance
30	Test 30	In accordance	It is not in accordance with
31	Test 31	In accordance	In accordance
32	Test 32	In accordance	In accordance
33	Test 33	In accordance	In accordance
34	Test 34	In accordance	In accordance
35	Test 35	In accordance	In accordance
36	Test 36	In accordance	In accordance
37	Test 37	In accordance	In accordance
38	Test 38	In accordance	It is not in accordance with
39	Test 39	In accordance	It is not in accordance with
40	Test 40	In accordance	It is not in accordance with

https://doi.org/10.61536/ambidextrous.v5i02.624

41	Test 41	In accordance	It is not in accordance with
42	Test 42	In accordance	In accordance
43	Test 43	In accordance	In accordance
44	Test 44	In accordance	In accordance
45	Test 45	In accordance	In accordance
46	Test 46	In accordance	It is not in accordance with
47	Test 47	In accordance	It is not in accordance with
48	Test 48	In accordance	In accordance
49	Test 49	In accordance	It is not in accordance with
50	Test 50	In accordance	In accordance

Based on Table 2, the Least Significant Bit (LSB) method demonstrated better message integrity preservation than the Pixel Value Differentiation (PVD) method. This is evident from the successful recovery of all SQL files extracted using the LSB method, which matched the original files, achieving a 100% message integrity success rate.

Conclusion and Recommendation

This research successfully implemented the Least Significant Bit (LSB) and Pixel Value Differencing (PVD) methods in a web-based steganography application for the process of inserting and retrieving SQL files in digital images in PNG and BMP formats. The test results showed that both methods were able to produce stego images with good quality based on high Peak Signal to Noise Ratio (PSNR) values and low Mean Square Error (MSE). However, the Least Significant Bit (LSB) method provided better performance in maintaining message integrity because all extracted SQL files were successfully restored according to the original files, while the Pixel Value Differencing (PVD) method still showed character changes in some of the extracted results.

This research is still limited to the use of digital images in PNG and BMP formats and messages in SQL files, so the results obtained cannot be generalized to other media and file types. Nevertheless, this research provides practical implications as an alternative application of steganography to improve digital information security by embedding messages in digital images. Future research is recommended to develop testing on a wider variety of image formats and file types and improve the Pixel Value Differencing (PVD) algorithm to improve the ability to maintain message integrity.

References

Akmal, R. A., Furqan, M. F., & Kurniawan, R. R. (2023). Implementasi metode least significant bit dalam teknik steganografi pada berkas audio dengan stego citra digital. *G-Tech: Jurnal Teknologi Terapan, 7*(2), 543-553. https://doi.org/10.33379/gtech.v7i2.2300

Dewi, & Munir. (2023). Perbandingan berbagai metode steganografi pada citra digital. *JIP (Jurnal Informatika Polinema).*

Firdaus, M. A., & Rahmatulloh, A. (2025). Implementasi steganografi citra digital LSB menggunakan enkripsi AES-256 dan embedding pseudorandom. *Jurnal Informatika dan Teknik Elektro Terapan, 13*(1). https://doi.org/10.23960/jitet.v13i1.5620

https://doi.org/10.61536/ambidextrous.v5i02.624

Gustiawan, A., Wahyudi, J., Suryana, E., et al. (2023). Perancangan aplikasi steganografi pada citra digital menggunakan metode pixel value differencing. *JUKI: Jurnal Komputer dan Informatika, 5.*

Hakim, F. N., & Sholikhan, M. (2024). Enhancing data security through digital image steganography: An implementation of the two least significant bits (2LSB) method. *International Journal of Graphic Design, 2*(2), 222-235. https://doi.org/10.51903/ijgd.v2i2.2124

Lasarus. (2021). *Penyembunyian pesan rahasia pada citra digital dengan teknik steganografi menggunakan metode least significant bit (LSB).*

Purbaningrum, A., Amalia, K. S., Saputro, I. A., & AMIKOM Surakarta. (2023). Penerapan metode least significant bit (LSB) dalam menyisipkan pesan rahasia pada citra digital: Sebuah pendekatan steganografi.

https://doi.org/10.61536/ambidextrous.v5i02.624