06_IJGD-GALLEY_FNH-MS - TNT.docx

by Caroline Caroline

Submission date: 24-Nov-2024 02:43AM (UTC+0900)

Submission ID: 2426513043

File name: 06_IJGD-GALLEY_FNH-MS_-_TNT.docx (346.57K)

Word count: 4502

Character count: 26176

Enhancing Data Security through Digital Image Steganography: An Implementation of the Two Least Significant Bits (2LSB) Method

***Abstract**. This research explores the effectiveness of the Two Least Significant Bits (2LSB) method in digital image steganography, focusing on its capacity for data hiding and resistance to steganalysis detection. By utilizing 2LSB of each pixel, the 2LSB method significantly enhances the data storage capacity compared to conventional Least Significant Bit (LSB) techniques while maintaining high image quality. The study conducts quantitative analyses, measuring Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) before and after data embedding. Results indicate minimal impact on image quality, with PSNR values remaining above acceptable thresholds, demonstrating the method's efficacy. Additionally, the research discusses the method's tolerance to various image types and compression levels, highlighting its practical implications for secure communication and data protection in mobile applications. The findings contribute to the ongoing development of steganography techniques and emphasize the potential for future enhancements in security and capacity.*

***Keywords** Steganography, 2LSB, Data Hiding, Image Quality, PNSR, Digital Security*

INTRODUCTION

The advancement of digital information and communication technologies has created numerous opportunities while simultaneously posing new threats to information security. With the increasing transmission of sensitive data over public networks such as the Internet, the risk of cyberattacks, including eavesdropping, hacking, data theft, and privacy breaches, has escalated (Kholiavko et al., 2021)In this context, data protection techniques like cryptography and steganography have rapidly evolved to safeguard information's confidentiality and integrity.

Steganography is the art and science of concealing messages or information within digital media to prevent detection by unauthorized parties. Unlike cryptography, which merely obscures the content of a message, steganography attempts to hide the very existence of the message, ensuring that unauthorized individuals remain unaware of any secret communication taking place (Varghese & Sasikala, 2023). This technique has become crucial in the increasingly complex digital communication landscape, where privacy and information security threats are more challenging to manage. In steganography, hidden messages can be transmitted through digital media, such as images, without arousing suspicion, as the media retains its ordinary appearance (Mawla & Khafaji, 2023).

The most basic and widely used steganography technique for digital images is the Least Significant Bits (LSB) method. This method hides information in the LSB of each pixel within a digital image. Since the changes to these minor bits are minimal, the visual quality of the image remains unchanged to the human eye (Halboos & Albakry, 2022). As a result, LSB is famous for its simplicity in implementation and effectiveness in concealing information without significantly altering the image's appearance. However, despite its efficacy in hiding data, LSB has certain fundamental limitations that restrict its use (Shekhawat et al., 2021).

One of the main limitations of the LSB method is its limited data storage capacity, as it only utilizes the last bit of each pixel to hide information. This means that the amount of data that can be hidden is relatively tiny in comparison to the overall size of the image (Gutub & Al-Shaarani, 2020). This limitation becomes problematic when users wish to hide large messages without compromising image quality. Additionally, LSB is vulnerable to various image analysis techniques that can detect the presence of hidden data. Techniques such as histogram and spectral analysis can detect minor alterations in color distribution or pixel intensity, potentially revealing the presence of a secret message (Hussain et al., 2021). This vulnerability makes LSB easy to detect for parties attempting to uncover hidden information within an image.

To address these weaknesses, researchers have developed the 2LSB method. This method utilizes the last two bits of each pixel in a digital image to conceal information, allowing for greater storage capacity than conventional LSB. By employing the last two bits, this method not only increases the amount of data that can be hidden but also makes the hidden data patterns more random, making them harder to detect through standard image analysis techniques (Abduljaleel et al., 2022). Adding a second bit provides greater flexibility in concealing data without causing noticeable visual distortion, thus preserving high image quality.

The primary advantage of the 2LSB method over conventional LSB lies in its ability to store more data and provide better protection against detection attacks (Rinki et al., 2022). In a study by Rinki et al. (2022), the 2LSB method proved more effective in hiding data within digital images while maintaining acceptable visual quality. This method also demonstrated greater resilience against detection attacks utilizing histogram or spectral analysis techniques, which commonly reveal hidden messages in conventional LSB. With its increased storage capacity, 2LSB allows for significant data insertion without degrading image quality, making it more suitable for steganographic applications requiring the concealment of large amounts of data (Rinki et al., 2022).

In addition to enhanced capacity and security, the 2LSB method is also more resilient to changes in format and compression, which often occur on digital platforms. Images transmitted over the Internet are frequently compressed to reduce file size, which in some cases can corrupt hidden data if the data-hiding method lacks compression resilience (Bansal et al., 2020). However, the 2LSB method has shown more excellent resistance to these disruptions than conventional

LSB, ensuring the integrity of hidden messages even when images undergo format or size changes during transmission. This advantage makes 2LSB a superior steganographic method compared to traditional approaches (Sahu & Swain, 2022).

Nevertheless, 2LSB has drawbacks. Using the last two bits of each pixel also increases the risk of visual distortion if applied carelessly, especially in low-resolution images or images with sharp color variations. Therefore, it is crucial to consider the image characteristics used when applying the 2LSB method to ensure optimal message concealment without significantly compromising image quality. Further research is needed to optimize this technique, particularly in scenarios where images frequently undergo more aggressive modifications or compression. (Sahu & Swain, 2022).

Thus, this study aims to design and implement a digital image-based steganography application using the 2LSB method. The application is expected to offer a practical and secure solution for users needing to hide large amounts of data without compromising the visual quality of images. Additionally, this study aims to test how much the 2LSB method can increase data storage capacity and provide improved protection against detection attacks compared to the conventional LSB method. With this background, this research is expected to contribute to developing steganographic techniques and their application in information security within an increasingly complex digital era.

LITERATURE REVIEW

Steganography is a crucial method in information security, particularly in today's digital era. As the need to protect sensitive information from cyber threats increases, various steganographic techniques have been developed, including LSB, 2LSB, Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT). Each method has its advantages and disadvantages, depending on the desired storage capacity and security level (Yadahalli et al., 2020).

A. *Two Least Significant Bits (2LSB)*

The 2LSB method advances the LSB steganography technique, commonly used to conceal information within digital images. The LSB method hides data in the LSB of each pixel, producing minimal changes that remain undetectable to the human eye (Abduljaleel et al., 2022). However, conventional LSB only utilizes the last bit of each pixel, which limits storage capacity and is also vulnerable to detection through image analysis techniques. To overcome these limitations, the 2LSB method was developed, using the last two bits of each pixel to increase storage capacity and provide an additional layer of security through more randomized bit distribution (Prasanalakshmi et al., 2022).

Jabbar et al. (2022) demonstrated that the 2LSB method offers significant advantages in hiding data without degrading image quality. Using two bits, this method can conceal more information than LSB and provides better protection against detection techniques, such as histogram or spectral analysis. Furthermore, the image's visual quality remains intact because bit changes occur in insignificant parts of the pixel. This makes 2LSB a preferable choice for digital image-based steganographic applications requiring substantial storage capacity (Jabbar et al., 2022).

Nevertheless, the 2LSB method has its weaknesses, particularly regarding resilience against image compression and modification. When an image is compressed or reformatted, there is a risk that part of the hidden information may be lost. This is especially relevant for lossy compression formats such as JPEG, which reduce image quality by discarding some information (Alabaichi et al., 2020). Therefore, although 2LSB is superior to LSB, challenges remain in ensuring information security during transmission, especially in environments where images undergo frequent modifications.

B. Comparison with Other Steganographic Techniques

In addition to 2LSB, several other steganographic techniques have been developed to conceal information within digital images, particularly in the frequency domain, such as DCT and DWT. These techniques offer advantages in terms of resilience against image compression and modification, which is a known limitation of spatial domain-based methods like 2LSB (Majeed et al., 2021).

DCT is one of the most widely used methods for [3] image compression, especially for the JPEG format. This method works by transforming an image from the spatial domain to the frequency domain, where data is hidden within the low or mid-frequency coefficients of the image (Zhang et al., 2024). As it operates in the frequency domain, this method provides superior resilience to lossy compression formats such as JPEG, which typically compromise hidden data in spatial-based methods like LSB and 2LSB. One of DCT's main advantages is its ability to retain hidden data even when the image undergoes compression or format modification (Modupe et al., 2021).

However, although DCT excels in compression [3] resilience, it has limitations, particularly in complexity and implementation. The transformation from the spatial domain to the frequency domain requires more intensive computation than 2LSB, which is more straightforward to implement (Ince et al., 2022). Additionally, although DCT can hide a large amount of data, the image quality may slightly deteriorate, especially if too much data is embedded within the low-frequency coefficients. Therefore, DCT is more suitable for applications that require compression resilience but do not demand very high storage capacity (Kaur et al., 2022).

DWT is another technique frequently used in frequency-based image steganography. This method operates by decomposing an image into several frequency components, allowing data to be hidden in either the lower or higher frequencies according to the specific needs (Jamel, 2020). One of DWT's advantages is its capability to handle high-resolution images, as well as its resilience to steganalysis attacks, which is more robust compared to spatial-based methods (Alexan et al., 2020).

Compared to 2LSB, DWT offers greater resilience to detection techniques such as histogram analysis and noise detection. This is because DWT operates in the frequency domain, making pixel alterations less detectable through simple image analysis in the spatial domain. However, like DCT, implementing DWT is more complex and requires more excellent computational resources. While it provides enhanced security, this method may only sometimes be practical for applications requiring large-capacity data concealment efficiently and quickly.

C. Steganalysis Attacks and Protection Offered by 2LSB

In steganography, one primary challenge is protecting hidden data from various attacks, known as steganalysis. These attacks aim to detect and, in some cases, uncover hidden data within digital images. Several commonly used steganalysis techniques include histogram analysis, noise detection, and DCT steganalysis (Gilkarov & Dubin, 2024).

Histogram analysis is one of the simplest and most effective techniques for detecting hidden image data. This method analyzes an image's color distribution or pixel intensity to identify changes caused by data hiding. In the LSB method, alterations in the last bit of each pixel can create unusual patterns in the color histogram, which can be recognized as indicators of hidden information (Tiwari & Gangurde, 2021).

However, the 2LSB method offers enhanced protection against histogram analysis due to its dispersed bit-change patterns, making the hidden data distribution more random and challenging to detect. A study by Hacimurtazaoglu & Tutuncu (2022) demonstrated that 2LSB has a higher resistance to histogram analysis compared to LSB, as the use of the last two bits creates a pattern of changes that is more difficult for simple analysis techniques to detect (Hacimurtazaoglu & Tutuncu, 2022).

Noise detection is a technique to identify increased noise within an image resulting from data hiding. Any data insertion into a digital image adds slight noise, which this method can detect. In LSB and other spatial-based techniques, data hiding in the last bits of pixels often increases noise, making it measurable. However, the 2LSB method generates less noise because the bit changes are more evenly distributed throughout the image, making the resulting noise harder to detect with noise-detection techniques (Shah et al., 2022).

In frequency-based attacks, DCT steganalysis is an effective technique for detecting data hiding in images modified in the frequency domain. This technique analyzes frequency coefficients to identify anomalous patterns created by data-hiding (Berdich & Groza, 2022). Although this attack is effective against DCT-based steganography methods, the 2LSB method, which operates in the spatial domain, is more resistant to this technique as the modifications do not affect the frequency coefficients of the image (Jelušić et al., 2022).

D. Advantages and Challenges of the 2LSB Method

From this literature review, it is evident that the 2LSB method has several significant advantages, particularly regarding higher data storage capacity compared to conventional LSB (Laimeche et al., 2020). This literature review shows that the 2LSB method has several significant advantages, particularly higher data storage capacity than conventional LSB (Laimeche et al., 2020). By utilizing the last two bits of each pixel instead of just one, the 2LSB method effectively doubles the data storage capacity, making it ideal for applications that conceal larger data volumes without compromising image quality. Additionally, the 2LSB method demonstrates enhanced security features, as using two bits creates a more randomized data distribution pattern, rendering it less detectable to standard steganalysis techniques such as histogram and noise detection (Abduljaleel et al., 2022). This makes the method exceptionally resilient to attacks aimed at uncovering hidden data.

Moreover, the 2LSB method exhibits better tolerance to changes in image formats and compression, especially when using lossless compression formats such as PNG, ensuring data integrity during transmission. However, challenges arise when applying this method to images subjected to lossy compression formats like JPEG, where some hidden data may need to be recovered (Sahu & Swain, 2022). Furthermore, using the last two bits can increase the risk of visual distortion, particularly in low-resolution images or those with significant color variations, emphasizing the importance of selecting suitable images for optimal performance. Despite these challenges, the 2LSB method remains a robust and efficient steganographic technique, balancing high storage capacity and security with minimal impact on image quality.

METHODS

This study employs the 2LSB method as a steganographic technique for hiding data within digital images (Islam et al., 2021). This method was selected for its ability to enhance data storage capacity and reduce the risk of detection using steganalysis techniques. The first step in this research is data collection. The data consists of digital images as storage media and the information to be embedded. Pictures selected for message storage should have favorable visual characteristics, such as high resolution and uniform colors, to ensure that modifications are not easily detected. Once the images are chosen, the data to be embedded, such as text messages or binary files, is gathered. This data is then encrypted using the AES-256 algorithm to ensure the security of the information to be hidden. Encryption generates a randomized output, making recognizing steganalysis methods more challenging.

After data collection, the next step is data analysis and embedding. Using the 2LSB algorithm, the encrypted data is embedded into the image pixels' last two bits of each color component (red, green, blue). The embedding process begins by converting the image into binary format. Each image pixel is evaluated, and the last two bits of each color component are replaced with bits from the data to be embedded. This process continues sequentially until all data is embedded. Once embedding is complete, the modified image is exported back to its original format (e.g., PNG or BMP) to ensure that the result retains visual quality. At this stage, image distortion is minimized by selecting appropriate images and keeping storage capacity within an optimal limit. This helps to ensure that the modifications remain undetectable to the human eye.

The next step is security testing of the embedded image. This testing involves evaluating the image's resilience to steganalysis attacks, including histogram analysis and noise detection. Histogram analysis evaluates color distribution and identifies patterns that might indicate the presence of hidden data. Noise detection identifies any increase in noise in the image that may result from data embedding. Testing is performed by comparing the original and modified images to assess whether the distortion remains within an acceptable range.

Data obtained from testing is then interpreted to evaluate the effectiveness of the 2LSB method in hiding data. The results of the steganalysis tests are analyzed to determine how effectively this method protects the data from detection. If the data is successfully hidden without detection and the image's visual quality is maintained, then the 2LSB method is considered successful. Additionally, the analysis results include assessments of the achieved storage capacity and the efficiency of the embedding process. Figure 1 shows the framework method used in this study.

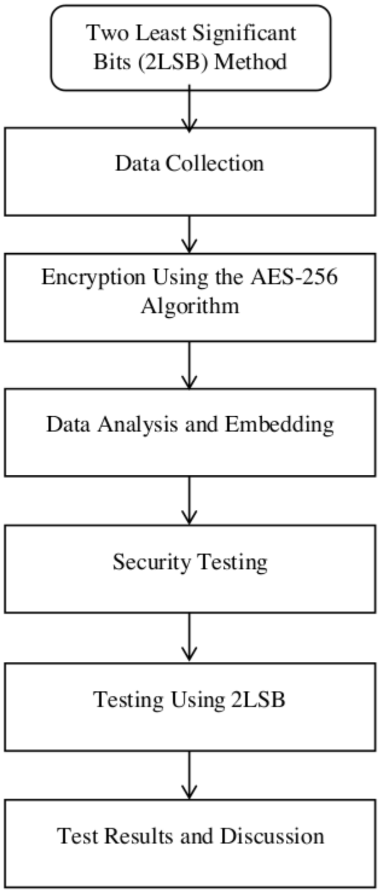
Two Least Significant Bits (2LSB) Method
Data Collection
Encryption Using the AES-256 Algorithm
Data Analysis and Embedding
Security Testing
Testing Using 2LSB
Test Results and Discussion

Figure 1. *Research Framework*

RESULTS

A. *Two Least Significant Bits (2LSB)*

The results of this study demonstrate the effectiveness of the 2LSB method in concealing data without significantly degrading the image's visual quality. Testing was conducted on various types of images to assess storage capacity and the impact of data embedding on image quality. A quantitative analysis was performed by calculating the MSE and PSNR before and after message embedding. MSE measures the average squared difference between the original pixel values and those in the modified image. At the same time, PSNR indicates image quality by comparing the maximum signal to the noise introduced. The test results for several images are presented in Table 1.

Table 1. *Test Results for Various Images*

Image Type	MSE Before Embedding	MSE After Embedding	PSNR Before Embedding (dB)	PSNR After Embedding (dB)
Image A (256x256)	0.0015	0.0018	48.35	47.89
Image B (512x512)	0.0020	0.0023	46.87	46.40
Image C (1024x1024)	0.0008	0.0012	50.12	49.65

The above results indicate that while there is a slight increase in MSE after embedding the message, the PSNR values remain at an excellent level, suggesting that the visual quality of the images is preserved. PSNR values above 40 dB are considered high in the context of images, and all tested images showed high PSNR values, confirming that the 2LSB method does not significantly degrade image quality. Furthermore, tests were conducted to assess system tolerance with various image types and compression levels. Images with lossless compression, such as PNG, maintained quality and data integrity post-embedding. However, using images with lossy compression, such as JPEG, had a more noticeable impact on image quality. While the 2LSB method remains usable, avoiding embedding data in already compressed JPEG images is recommended to prevent the loss of hidden information. Several visual examples provide more substantial evidence that the images' visual quality remains intact. Figure 2 shows the original image before and after steganography processing using the 2LSB method.

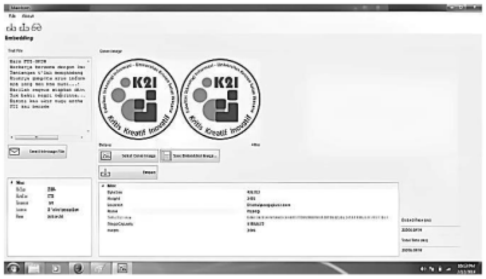

Figure 2: *Original Image (Before Embedding)*

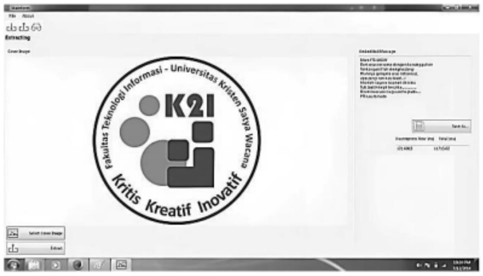
File About
Extracting
Fakultas Teknologi Informasi - Universitas Kristen Satya Wacana
K2I
Kritis Kreatif Inovatif
Save As...
Extract

Figure 3: *Image after Embedding Using the 2LSB Method (After Embedding)*

In the examples above, the image following the steganography process shows no significant visual changes despite the data embedding. The details and colors in the image are preserved, allowing readers to observe that the 2LSB method effectively conceals information without compromising visual quality.

B. Discussion

The test results indicate that the high PSNR values and relatively small MSE increase after data embedding support the claim that this method successfully maintains the visual quality of images. Previous research, such as that by (Abduljaleel et al., 2022) and (Prasanalakshmi et al., 2022), has shown that conventional LSB methods often result in a more significant decline in image quality, especially when embedding large amounts of data. Therefore, the 2LSB method provides a more effective solution than conventional LSB, which aligns with these findings. Furthermore, the analysis of system tolerance regarding images with varying compression levels shows that, while the 2LSB method is more effective than LSB in preserving image quality, using lossy compressed images such as JPEG may reduce the effectiveness of data concealment. Previous studies have also highlighted that lossy compression can corrupt hidden information, as explained by (Modupe et al., 2021). Thus, the results of this study align with the existing literature, which recommends selecting appropriate images to ensure data integrity.

While this research contributes significantly to developing steganographic techniques, certain limitations should be noted. One of these is the limitation in the types of images tested. This study used specific images with particular characteristics, so the results may only be generalizable to some pictures. Additionally, the 2LSB method has yet to be tested against all existing steganalysis attack techniques, indicating the need for further research to explore the resilience of this method in a broader context. The implications of this study suggest that the 2LSB method is effective in terms of storage capacity and in preserving the visual quality of images. By incorporating encryption before embedding, this method adds an extra layer of security, protecting data from detection by third parties. This study contributes empirical evidence that the 2LSB method is a promising solution for steganographic applications, balancing security and storage efficiency in today’s digital age.

C. Reference

```
public static int Kapasitas(string
filename){
```

```
3           List<byte> list = new List<byte>();
4           Bitmap bitmap = new Bitmap(filename);
5           int P = bitmap.Size.Height;
6           int L = bitmap.Size.Width;
7           int K = (P * L * 3) / 8;
8
9           return K;
10      }
```

Program Code 3 calculates the maximum bit capacity embedded within a cover image. The calculation begins by measuring the image dimensions, namely its length and width. First, the size of the image is multiplied by its width to obtain the total number of pixels. This result is multiplied by 3, as each pixel consists of three color components (red, green, and blue), each requiring one byte. The final result is then divided by 8 to convert the byte count into bits. This calculation process is outlined in lines 5-7 of the code.

The steganography system testing using the 2LSB method aims to ensure that the system operates according to the principles and concepts of steganography as implemented. This testing covers several key aspects, such as the effectiveness of the 2LSB method in concealing data and the quality and integrity of the resulting image. Embedding capacity testing is conducted to determine the amount of data that can be embedded in the image without significantly degrading its quality, verifying that data can be embedded according to the calculated capacity. Image quality testing ensures that the image retains high quality after embedding, comparing the original and embedded images to assess any visual changes. Extraction accuracy is tested by embedding a message and then extracting it to ensure that the retrieved data is identical to the embedded data. System robustness testing evaluates the extent to which the system can withstand modifications or damage to the image, such as compression or format changes, to ensure that data can still be extracted even if the image undergoes alterations. Security testing examines whether the system is secure from detection or manipulation, ensuring that the embedded data is not easily detectable by standard image analysis methods. The 2LSB steganography system is evaluated through these tests to confirm that it meets the established standards and principles.

Testing was conducted on a computer with the following specifications:

Operating System	:	*Microsoft Windows* 7 32-*bit* (x82)
Processor	:	*Intel® Core™* i3-540, 3072Ghz
RAM	:	6 GB
Hard Drive Speed	:	7200 rpm
Display	:	*NVIDIA GeForce GTX* 550Ti 2GB

Message Integrity Testing, also known as Test 1, aims to ensure that the message embedded within the image remains intact and unaltered during the embedding and extraction processes. This test is performed by calculating the message's hash or checksum value before embedding it into the image and after extracting it. If the hash values of the embedded and extracted messages are identical, the message has not experienced any changes or damage.

The MD5 algorithm is used to calculate this hash value, which is a standard method for generating a unique hash from data. This algorithm produces a string representing the message; any minor alteration in the message will change its hash value. This test ensures that the embedding and extraction processes do not corrupt or alter the message by comparing the hash values before and after the process. The results of this test are displayed in Table 2.

Table 2. *Message Integrity Test Results*

No	File	Pre-Embedding Checksum	Post-Extraction Checksum	Conclusion
1	Message 1.txt	a14386497d471c4211eb14bff021e541	a14386497d471c4211eb14bff021e541	Intact
2	Message 2.txt	00a783ac2f9854a86a5fc98a65d72d60	00a783ac2f9854a86a5fc98a65d72d60	Intact
3	Message 3.txt	17dfa59946628dcb65271ad8737795ef	17dfa59946628dcb65271ad8737795ef	Intact
4	Message 4.txt	4d8a7c1bd7eaaac4085afaf901c05ecb	4d8a7c1bd7eaaac4085afaf901c05ecb	Intact
5	Message 5.txt	f20dfe9a1b93aee2872c9b345ce1dba4	f20dfe9a1b93aee2872c9b345ce1dba4	Intact

Based on Test 1 results shown in the table above, it can be concluded that the developed steganography application successfully embedded and extracted messages without causing alterations or damage to the content. This test demonstrates that the embedded messages remained intact, with no modifications during the process, as indicated by the matching hash values of the messages before and after extraction. Therefore, the application effectively maintains message integrity.

CONCLUSION

A. Conclusion

This study successfully demonstrates the effectiveness of the 2LSB method as a superior steganography technique for concealing data without compromising the visual quality of images. A unique contribution of this research is the significant increase in data storage capacity achieved by utilizing the last two bits of each pixel, as opposed to conventional LSB methods that only use one bit. The test results show that the 2LSB method efficiently hides information and provides better protection against steganographic detection. With high PSNR values and minimal MSE increase after message embedding, this method effectively maintains image integrity even after compression processes. The potential for further development of the 2LSB method is also highly promising, particularly in enhancing security and storage capacity. This research highlights that applying encryption algorithms before data embedding can mitigate detection risks using steganalysis techniques, creating a more secure approach to conceal information.

B. Recommendation

The practical implications of this research are highly relevant in the context of the need for information security in the digital era. The steganography application can protect personal data across various digital platforms, such as instant messaging applications, cloud data storage, and communication between individuals and organizations. With the rising threats to privacy and data security, the 2LSB method offers an effective solution for safeguarding transmitted information confidentiality. Future research should explore more robust encryption techniques and combine other methods with 2LSB to enhance resilience against more complex attacks. Further testing on various types of images and compression levels can provide deeper insights into the efficiency and effectiveness of this method in broader contexts. This approach aims to produce more innovative and adaptive applications to address future information security challenges by focusing on improved security and storage capacity.

REFERENCES

06_IJGD-GALLEY_FNH-MS - TNT.docx

ORIGINALITY REPORT

2%	2%	0%	0%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	id.123dok.com Internet Source	1%
2	www.mdpi.com Internet Source	<1%
3	fastercapital.com Internet Source	<1%
4	link.springer.com Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		