

Improvement Of Watermarking Quality Using The Least Significant Bit Method With Reed Solomon Code

Muhammad Khozin¹, M. Arief Soeleman²

¹(Faculty Of Computer Science, Dian Nuswantoro University, Indonesia)

²(Faculty Of Computer Science, Dian Nuswantoro University, Indonesia)

Abstract:

Watermarking is a technique used to protect the authenticity and integrity of digital data. One method commonly used in watermarking is the Least Significant Bit (LSB) method, which utilizes the last bit of digital data to insert a watermark. However, this method is vulnerable to attacks and loss of information during data compression or transformation. In order to increase robustness and ease watermarking, in this study it is proposed to use the LSB combination method with the Reed-Solomon Code. The Reed-Solomon Code is an error correcting code capable of detecting and repairing defects in digital data. By combining the LSB method and the Reed-Solomon Code, watermarking can be obtained that is more resilient and can withstand attacks or disturbances that may occur. In the experiment, the image dataset was tested using the usual LSB method and the LSB combination method with the Reed-Solomon Code. The evaluation results show that the combination method is able to provide a better level of softness and durability compared to the usual LSB method. This is indicated by the results of an average PSNR (Peak Signal-to-Noise Ratio) value in the range of 78-79 dB and an average MSE (Mean Squared Error) value ranging from 0.0008-0.001.

Key Word: Watermarking, Least Significant Bit, Reed Solomon Code

Date of Submission: 09-02-2024

Date of Acceptance: 19-02-2024

I. Introduction

The rapid growth of internet technology has made issues such as illegal copying, data file transmission, storage, and distribution of digital multimedia crucial security concerns [1]. The dissemination of digital multimedia information has created a major problem, namely copyright infringement, which needs to be addressed worldwide. Copyright protection is necessary for various forms of multimedia information, including text, images, audio, video, and software [2],[3],[4]. One solution is the use of watermarks, which require less transparent images or text to be inserted into paper or images to enhance security, reinforce intellectual property rights for authentication and copyright protection, broadcast monitoring, authentication, and ownership data hiding, prevention of copying, and authentication. This solution will prevent illegal duplication and prove the credibility or integrity of watermarked images to determine the original owner's identity[5],[6],[7] is part of security methods.

Digital watermarking is a technique of embedding or hiding information called a watermark (also known as a tag or digital label) within a digital file without altering the file itself, [8] Digital watermarking provides intellectual property rights and detects damaged data. The proposed method uses Reed-Solomon code to conceal secret messages in medical images, enhancing resistance to salt and pepper noise. This method encodes the message, hides it within the image, and then extracts it using error correction techniques.

This research will focus on the use of watermarking techniques implemented with the least significant bit (LSB) method, this method involves the insertion of a unique code into the image to be protected. The least significant bit operates by embedding secret data in the form of bits in the smallest or rightmost bit positions of the pixel data when composing the original image document. This process will not visibly alter the image but can still be recognized by the computer. By combining LSB with Reed-Solomon code, it is possible to detect and correct errors that occur during the watermark insertion and extraction processes. This means that Reed-Solomon code can identify damage or changes to the watermarked image and rectify them, ensuring that the watermark can still be extracted with high accuracy.

II. Material and Methods

This research utilizes the Systematic Literature Review (SLR) method, which is employed for the identification, analysis, and interpretation of research stages in accordance with the questions posed in the study.

The method is popularized by Kitchenham and Charters [17]. The findings obtained from this study include:

1. Modified LSB Watermarking for Image Authentication [18]

The study by R. Aarathi et al. [18] in 2015 proposed a modified LSB embedding technique. This technique fulfills the feature of reversibility not supported by simple LSB techniques. In the third and fourth least significant bits, these are used to embed data, and a matrix is created with the same dimensions as the watermark image. The values in this matrix are obtained by XOR-ing each pixel from the original image with the watermark image. This matrix is used during the digital watermark extraction process. The results of this paper indicate that the proposed algorithm can enhance the capacity of the scheme and provide reversibility and fragility for transmitting secret data. They also demonstrate that the proposed scheme achieves better imperceptibility and reversibility compared to traditional LSB schemes. Quantitative analysis of the algorithm also shows improvements in the embedding rate and reversibility. Additionally, imperceptibility and fragility are analyzed using PSNR values and attack percentages.

2. Analysis of Image Watermarking Using Least Significant Bit Algorithm [8]

The research by Puneet Kr Sharma et al. [8] in 2012 proposed a least significant bit algorithm where the embedded watermark is spread across the entire image to avoid watermark damage by attackers. They explored the influence and impact of using different bit positions in the LSB algorithm. For example, they tested and analyzed the performance of watermarking using a single LSB bit, LSB bits in each color component (RGB), or sequential LSB bits in multiple pixels.

They evaluated the quality and clarity of the watermark generated by the LSB algorithm. The methods used in the experiments, including the selection of test image datasets and relevant parameter settings, were described. The experimental steps taken to analyze and evaluate the performance of the LSB algorithm were outlined. The experimental results and analysis demonstrated the effectiveness and quality of watermarking using the LSB algorithm. The paper discusses the use of image watermarking using the Least Significant Bit (LSB) algorithm to embed messages or logos into images. Additionally, it explores security issues and challenges related to digital watermarking. The paper outlines the watermarking process, the concept of modifying the least significant bit, and the results of watermark embedding using various bit substitution methods. The conclusion highlights the effectiveness of LSB-based digital watermarking and provides references for further reading.

3. Digital Image Watermarking Using LSB Technique [19]

The research by Anum Javeed Zargar in 2015 [19] proposed a technique in which the least significant bit of grayscale image pixels is replaced with the most significant bit of the watermark image. Before embedding the watermark, the original image and watermark are cropped according to the desired pixels. The strength and robustness of the resulting watermark using the LSB technique are evaluated. This may include testing to assess the extent to which the watermark can be recovered from images that have undergone attacks or manipulations. The methods used in the experiments, including the selection of test image datasets and relevant parameter settings, are described. The steps of the experiments conducted to analyze and evaluate the performance of the LSB technique in image watermarking are outlined.

The paper's results discuss a technique for digital image watermarking using the least significant bit (LSB) method. The paper explains the importance of watermarking for confidentiality, authentication, and copyright protection. The proposed algorithm uses the LSB of the original image and performs an '&&' operation with the most significant bit (MSB) of the watermark image. The paper also covers the embedding and extraction algorithms, as well as experimental results. The conclusion suggests that the proposed technique is a desirable approach and may be resistant to various attacks in the future.

4. Detection of Tampering in Image Using Watermarking [20]

The research by Manoj Nagar et al. in 2015 [20] proposed a digital watermarking technique to detect tampering in color images. According to this technique, the watermark is generated with the help of Discrete Cosine Transform (DCT) or Discrete Fourier Transform (DFT) coefficients, and then the generated watermark is embedded in the least significant bits of the image pixels.

Based on the provided description, the research paper presents a method for detecting tampering in color images using digital watermarking. The algorithm involves two stages: embedding and authentication/localization. Experimental results show the efficiency of the proposed algorithm in detecting and localizing areas that are corrupted in images affected by various types of attacks. Additionally, the paper includes a literature survey on tamper detection techniques and references for further reading.

5. Least Significant Bit Hash Algorithm for Digital Image Watermarking Authentication [4]

The research by S. Muyco et al. in 2019 [4] proposed digital watermarking using the least significant bit (LSB) algorithm for the embedding and extraction processes. This algorithm is significant in the embedding and extracting processes, capable of extracting the embedded hash code from the protected file to produce an output file identical to the original one. The study involved data capacity analysis, histogram analysis, and the same Hamming distance. It presented a digital watermarking technique using the Least Significant Bit (LSB)

algorithm for embedding and extraction. The results demonstrated the algorithm's ability to extract the embedded hash code from the protected file, producing an output file identical to the original. Furthermore, the research showed that the watermarked image is not visible and effectively embedded in the original file. The study was supported by the Commission on Higher Education (CHED), and it suggests further research to compare and simulate different image variations in terms of security. The paper includes a literature review, proposed methods, and experimental results, including data capacity analysis and histogram analysis, demonstrating the success of watermark embedding and extraction.

6. Digital Image Watermarking Using Least Significant Bit Technique in Different Bit Positions [21]

The research by Bansal et al. in 2014 [21] presents and compares the LSBW method using different bit positions. The comparison for these bit positions is conducted based on various parameters such as Mean Square Error, Peak Signal to Noise Ratio, and Normalized Cross Correlation. These parameters are evaluated for various attacks such as Gaussian Noise, Poisson Noise, Salt & Pepper Noise, and Speckle Noise. The explanation of the methods used in this research, including the selection of test images, parameter settings, and experimental procedures, is provided.

The results of this paper indicate that the digital image watermarking technique using the Least Significant Bit (LSB) method at different bit positions has been compared. The authors compared the results for various parameters such as Mean Square Error, Peak Signal to Noise Ratio, and Normalized Cross Correlation for different bit positions. Simulation results show that embedding the watermark in the 8th bit position produces the best results. The paper concludes that the proposed algorithm can maintain image quality after the watermarking process and suggests using larger-sized images as watermarks for future research.

7. Reed Solomon Coding-Based Medical Image Data Hiding Method against Salt and Pepper Noise [16]

The research by Mehmet Zeki Konyar and Sitki Öztürk in 2020 [16] proposes a Reed Solomon coding-based method to conceal a secret logo in medical images. The aim is to safeguard patient privacy and ensure the security and authenticity of medical images. This method was tested with various types of medical images and noise densities, demonstrating the extraction of hidden messages with almost error-free results even at a noise density of 10%. The method also outperforms existing methods in terms of Bit Error Rate (BER) and Structural Similarity Index (SSIM).

Digital Watermarking

Digital watermarking is a technique of embedding or hiding information called a watermark (also known as a digital tag or label) within a digital file without altering the file itself, [8] Digital watermarking provides intellectual property rights and detects damaged data. Watermarks themselves are divided into two types: visible watermarks and invisible watermarks. Visible watermarks are sub-images that are blurry or semi-transparent and placed on top of the original image, such as logos used by various companies and television channels.

Least Significant Bit (LSB)

The simplest algorithm is the Least Significant Bit (LSB), which adds a watermark to each least significant bit of an 8-bit pixel. The capacity of using high-channel covers for transmission is high, and the object insertion takes place multiple times. In digital images, information can be embedded in busier areas of an image, calculated to conceal a message in a specific part of the image, or it can be directly inserted into each bit of image information that is less visible.

The algorithm proposed by Kurah and McHughes [22] is intended to be embedded in the LSB and is known as image downgrading [23]. An example that is less noticeable or less predictable is the Least Significant Bit Embedding. This explains how it works for an 8-bit grayscale image and the potential effects of altering such an image. The embedding principle is effective and quite simple. In a grayscale image, each pixel consists of 8 bits represented by 1 byte, which can represent 256 shades of gray between black (0) and white (255).

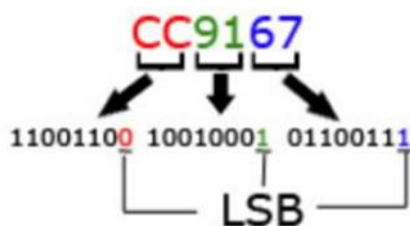


Figure 1 Least Significant Bit (LSB) [25]

Figure 1, the least significant bit (LSB) is visible in one color pixel, information embedding can be performed in this bit, for example:

The initial data, three pixels from a 24-bit image.

(00100111 11101001 11001000)
 (00100111 11001000 11101001)
 (11001000 00100111 11101001)
 binary value of the character 'A'
 10000011.

Data after planting the character 'A'
 (00100111 11101000 11001000) → 100
 (00100110 11001000 11101000) → 000
 (11001001 00100111 11101001) → 11

Only the underlined bits change

Bit or Binary digits are the basic units of computer data storage; the data bit values are 0 (zero) or 1 (one). All information in a computer is stored in bits, including images, audio, and video. Image color formats such as monochrome, grayscale, RGB, CMYK also utilize bit units within their storage space. For example, monochrome bitmap coloring (using 1 bit for each pixel), RGB - 24 bits (8 bits for red, 8 bits for green, 8 bits for blue), grayscale uses 8 bits to determine the black level of a pixel.

Pengolahan Citra Digital

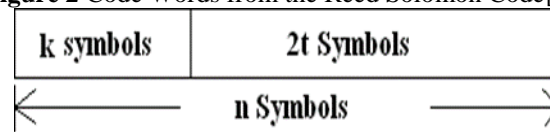
Five human senses that are most effective are the eyes, thus the image plays a crucial role from the human perspective. However, the human eyes have limitations in capturing images in the form of electromagnetic signals. Unlike computers or other imaging devices, they can capture electromagnetic signals ranging from gamma rays to radio waves. Imaging devices can capture signals that are not visible, not consistent with their source, or not visible to the human eye.

These issues mean that digital image processing plays a crucial role in various applications. Image processing technology can be used in many disciplines such as medicine, industry, agriculture, geology, marine industry, etc. The development of image processing technology offers significant advancements in this field. In the future, the application of digital imaging technology will continue to expand and evolve in such a way that it presents a unique challenge for researchers in the field of digital imaging.

Reed Solomon Code

Reed Solomon Code is a forward error-correcting code that can be specified as RS (n, k), where n is the size of the code word produced by the RS encoder, and k is the size of the input data to the RS encoder. The difference between the number of symbols output by the RS encoder and the number of symbols input to the RS encoder is called the parity symbol 2t. Each symbol is formed from m bits. Figure 2 below shows the code word of the Reed Solomon Code k: Input symbol to the RS encoder; n: Output symbol from the RS encoder (n = 2m - 1); 2t: parity symbols = n - k; m: Size of each symbol.

Figure 2 Code Words from the Reed Solomon Code[27]



Bit data stream is divided into k symbols, each of length m. 2t parity symbols are added to each of the k symbols to produce n RS code symbols.

Peak Signal to Noise Ratio (PSNR) dan Mean Square Error (MSE)

PSNR is the comparison between the original image and the compressed image. PSNR can be calculated using equation (6). Before calculating PSNR, MSE (Mean Square Error) is the mean square error value between the original image and the compressed image [28]. MSE can be calculated using equation (6).

$$MSE = \frac{\sum_{x=1}^M \sum_{y=1}^N (g(x,y) - f(x,y))^2}{M \times N}$$

$$PSNR = 20 \times \log_{10} \frac{\max |g(x,y)|}{\sum_{x=1}^M \sum_{y=1}^N (g(x,y) - f(x,y))^2} \dots \dots \dots (6)$$

Information:

- M : image width
- N : image length
- f(x,y) : pixel intensity of the original image at coordinates (x,y)

$g(x,y)$: pixel intensity of the compressed image at coordinates (x,y)

Results of MSE and PSNR calculations can be interpreted in such a way that the higher the MSE value, the more pixels differ between the input image and the output image. Conversely, the higher the PSNR value, the more similar the quality of the output image is to the input image. The PSNR value for images with good visual quality and lossless compression is typically around 30-50 dB [28].

III. Research Methodology

Dataset

Research utilizes a grayscale image dataset consisting of six images, namely cameraman.png, fruit.png, house.png, peppers.png, lena.png, and baboon.png. The research dataset comprises images commonly used in image processing studies, downloaded from the SIPI image database website. Each image container in the dataset has an 8-bit depth specification (gray scale).

Proposed Method

Research will propose a watermarking technique implemented using the least significant bit (LSB) method. This method involves embedding a unique code into the image to be protected. The least significant bit operates by inserting secret data into the least significant bits, specifically the rightmost bits, of pixel data when composing the original image document. This process will not visibly alter the image to the human eye, but it can still be recognized by a computer. The Proposed Method is illustrated in **Figure 3**:

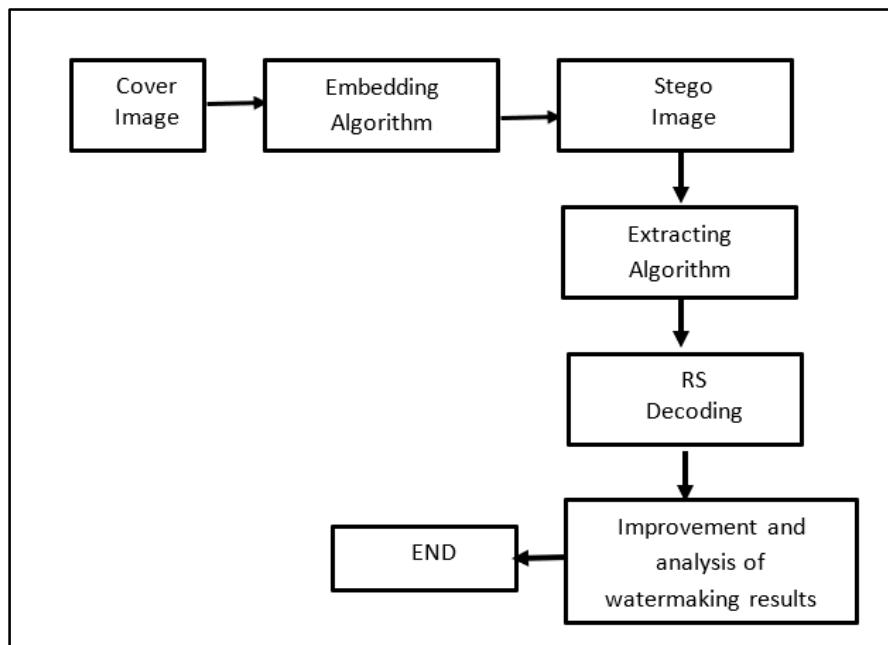


Figure 3 Proposed Method

Testing Experiment

The stages of experimentation and testing of the method were carried out on a computer with an Intel Core i5 1.60 GHz processor, 12 GB RAM, and a 512 GB SSD hard disk. It utilized the Windows 10 64-bit operating system. The method was tested using the Python programming language for watermarking.

IV. Results and Discussion

This research applies Reed-Solomon code optimization to the least significant bit (LSB) steganography technique. It enhances the efficiency and reliability of hiding secret data in images using the LSB method by combining the advantages of Reed-Solomon code in error detection and correction with the information hiding capabilities provided by LSB. This experiment employs various parameters and settings to achieve optimal results in terms of the capacity and reliability of data hiding.

Results

Image materials used are divided into two groups, with 6 images as research material and 30 images as t-test material in the proposed procedure. The images used as the research dataset consist of 6 files. The image dataset used in this research can be displayed as shown in **Figure 4** below:



Figure 4 Image Dataset

This research utilizes a grayscale image dataset consisting of six images, namely cameraman.png, fruit.png, house.png, peppers.png, lena.png, and baboon.png. The research dataset comprises images commonly used in image processing studies, and it was downloaded from the SIPI image database website. Each image container in the dataset has an 8-bit depth specification (gray scale).

Discussion

Images in the dataset are preprocessed using watermarking techniques employing the Least Significant Bit (LSB) method. The watermarking technique is implemented using the Python programming language, programmed according to techniques with equations from previous research. All images undergo the insertion process of the Least Significant Bit (LSB) in the embed_message function, where the message encoded with Reed-Solomon code is added to the last bit (LSB) of each pixel in the image. Then, the extract_message function is used to extract the embedded message from the steganography image using LSB. The image to be watermarked is converted into binary/bitstream format, and the bitstream message is divided into exact-sized blocks. Reed Solomon encoding of each bitstream message block is encrypted with Reed Solomon code, used to provide redundancy and correct errors during the sampling process.

Embedding the watermark involves transforming the image to be watermarked into a pixelated image. Each block of pixels in the image is captured, and the Least Significant Bit (LSB) of each color channel (e.g., RGB) is used to add bits from the encrypted watermark message with Reed Solomon code. During this process, attention is given to optical tolerance to make the changes less noticeable. The watermark image, which already contains the watermark message, is displayed or saved as a watermark image.

Next stage involves extracting the watermark, where the received watermark image is transformed into a pixelated image. Each pixel block of the watermark image is taken, and the least significant bit (LSB) from each color channel is extracted to obtain the watermark message bits. The removed pieces are then combined and divided into message bitstream blocks.

Decoding Reed-Solomon is applied to each message bitstream block that has been decrypted and encrypted with Reed-Solomon code. This is used to detect and correct errors that occur during the embedding and extraction processes. The reconstructed message for each decrypted bitstream block is combined into a complete message bitstream. The message bitstream is then converted to the original watermark message format. This flow allows the watermark message to be embedded in the image using the LSB input, utilizing Reed-Solomon code for error detection and correction.

Results of Embedding LSB and Reed Solomon Code

Stages of evaluating embeddings using Peak Signal-to-Noise Ratio (PSNR) is one of the most commonly used methods to measure the quality of watermarked images. PSNR calculates the relationship between the signal strength of the original image and the noise or distortion generated by the watermarking process.

Table 1 Dataset Embedding Results

Image	Original Image (kB)	Embedded Image (kB)	PSNR (dB)	MSE (dB)
Cameraman.png	92 kB	114 kB	47.96	0.925
Fruit.png	91 kB	113 kB	47.83	0.955
House.png	117 kB	217 kB	48.34	0.976
Peppers.png	180 kB	242 kB	48.99	0.980
Lena.png	257 kB	401 kB	50.84	0.993
Baboon.png	257 kB	401 kB	50.84	0.993

Table 1 shows the average performance values of all images for different capacity sizes. A PSNR value above 35 dB indicates that the visual quality does not change significantly after the embedding process. Image

size exhibits differences between the original image and the embedded image. The embedded image has a larger size than the original image in each case, indicating that the watermark embedding process has added additional information to the image.

A high Peak Signal-to-Noise Ratio (PSNR) value indicates good watermarking results. The higher the PSNR value, the lower the level of distortion between the original image and the embedded image. All PSNR values provided in the table are sufficiently high, indicating good-quality watermarking results. A low Mean Squared Error (MSE) value also indicates a high level of conformity between the original image and the embedded image. The lower the MSE value, the closer the embedded image is to the original image. The MSE values given in the table are quite low, indicating good watermarking results.

High PSNR and MSE-based Watermark compatibility suggests that the watermark embedding process in these images is effective and produces embedded images that closely match the original images.

The conclusion from **Table 1** is that the watermark embedding process in these images produces high-quality watermarking results, with low distortion levels and a high level of conformity between the original images and the embedded images. The following are the results after the image embedding process:



Original Embedding
Figure 5 (a) Original Image (b) Image Embedding

Based on **Figure 5**, hiding the watermark without visually damaging the original image. In this context, the watermark canvas image maintains quality and visual similarity with the original image, yet the watermark remains concealed and can be detected during the verification or authenticity search process. In conclusion, after adding the watermark, the image visually resembles the original image, and no significant changes are noticeable in the picture.

Results of Extracting LSB and Reed Solomon Code

Process of extracting the Least Significant Bit (LSB) with Reed-Solomon Code is used to recover the embedded watermark in a modified image. The evaluation of extracting the watermark using Normalized Cross Correlation (NCC) is one method to measure how well the watermark message can be retrieved from the watermark image. NCC calculates how well the extracted watermark matches the known original watermark. **Table 2** below shows the results of extracting the dataset as follows:

Table 2 Results of Extracting Dataset



Image	Embedding Image (kB)	Extracting Image (kB)	Normalized Cross Correlation (NCC)
 Cameraman.png	114 kB	114 kB	1
 Fruit.png	113 kB	113 kB	0.99




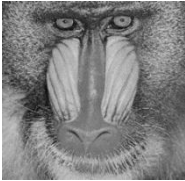
Image	Embedding Image (kB)	Extracting Image (kB)	Normalized Cross Correlation (NCC)
 House.png	217 kB	217 kB	1
 Peppers.png	242 kB	242 kB	0.99
 Lena.png	401 kB	401 kB	1
 Baboon.png	401 kB	401 kB	1

Table 2 shows the images of the embedding results and the images of the extracting results. In all cases, the images of the embedding results and the images of the extracting results have the same size. This indicates that the watermark embedding and extraction processes are carried out successfully without any loss or alteration of data in the images.

Normalized Cross Correlation (NCC) values are provided, and they are 1 or close to 1 in all cases. This indicates that the images of the extracting results are highly correlated or very similar to the original images (watermark images). The higher the NCC value approaching 1, the higher the level of similarity between the original image and the image of the extracting result. The high NCC values indicate that the watermark embedding and extraction processes for these images are successful. The watermark is successfully embedded and extracted without significant loss or changes in the images. There is variation in the image sizes for each image. However, the sizes of the embedded and extracted images (expressed in kilobytes/kB) are the same for each image, indicating that the watermarking process does not affect the file size of the images.

The main conclusion from **Table 2** is that the embedding and watermark extraction processes performed on these images yield good results, with high NCC values indicating a high level of match between the original image and the extracted image. **Figure 6** below illustrates the results of the watermark extraction:

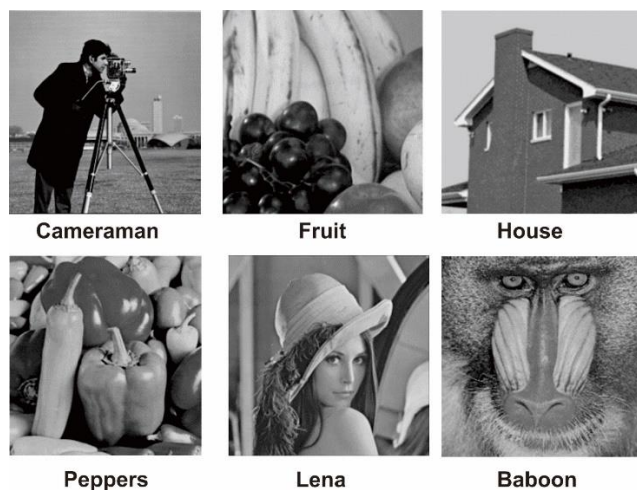


Figure 6 Dataset Extraction Results

Results of Improved Watermarking Using LSB with Reed Solomon Code

Combination of the Least Significant Bit (LSB) method and Reed-Solomon code is chosen in watermarking to achieve the goal of enhancing the security and reliability of watermarking. The LSB method is used to embed watermark information into an image by manipulating the least significant bit (LSB) of each pixel. In this method, the LSB value of each pixel is altered to reflect the watermark message bit to be embedded. LSB is chosen because changes in the least significant bit do not significantly disturb the visual appearance of the image, making it difficult to be visually detected.

Reed-Solomon code is used as an error correction mechanism that can detect and correct errors that may occur in the embedded watermark message. The Reed-Solomon code is capable of detecting and correcting errors in data transmission, thereby improving the reliability of watermark extraction. By employing the Reed-Solomon Code, the watermark message can be divided into smaller data blocks, encoded with additional redundancy, and then embedded into the image using the Least Significant Bit (LSB) technique.

During extraction, if there are errors or modifications in the extracted message, the Reed-Solomon code can correct errors and recover the original message with high accuracy. By combining the LSB method and Reed-Solomon code, the security and reliability of watermarking can be enhanced. Regarding security, the LSB method generates an embedding technique that is not visually noticeable, making it difficult to be detected by the human eye. The Reed-Solomon code provides error correction mechanisms that can detect modifications or attacks on the embedded watermark message. If there are changes to the message, the Reed-Solomon code can detect and correct errors, allowing the original message to be restored.

Reed-Solomon code enhances the reliability of watermark extraction by detecting and correcting errors that occur in the extracted message. This ensures that the watermark message can be retrieved with a high success rate, even in the presence of disturbances in the image or attacks. The use of additional redundancy in the Reed-Solomon code helps improve resilience against disturbances and noise that may affect the image. Thus, the combination of LSB and Reed-Solomon code in watermarking collaborates to embed the watermark message invisibly and enhance the security and reliability of watermark extraction. **Table 3** below shows the results of implementing watermarking improvement using LSB with Reed Solomon Code:

Table 3 Results of LSB Improvement with Reed Solomon Code

Stego Image	No LSB+RSC		Proposed Method	
	PSNR	MSE	PSNR	MSE
Cameraman.png	76.24	0.0248	78.324253	0.0956441
Fruit.png	76.47	0.0256	78.926376	0.0832612
House.png	77.32	0.0346	79.164177	0.0788247
Peppers.png	76.12	0.0175	78.259054	0.0970901
Lena.png	76.32	0.0251	78.701237	0.0876913
Baboon.png	76.26	0.0232	78.548425	0.0908318

Based on **Table 3** compared to the previous method, the proposed method produces better imperceptibility quality for each combination of image Peak Signal-to-Noise Ratio (PSNR). The average PSNR for all images is in the range of 78-79 dB. PSNR is used to measure the quality of image restoration, and the higher its value, the better the quality of the generated image. Therefore, it can be concluded that the image restoration quality for all images (Cameraman.png, Fruit.png, House.png, Peppers.png, Lena.png, Baboon.png) is quite good with a high average PSNR.

The Mean Squared Error (MSE) for all images is in the range of 0.0008-0.001. MSE is used to measure the error between the original image and the restored image. The lower the MSE value, the better the image restoration. In this case, it can be concluded that the image restoration for all images has a low error rate with a small average MSE. Thus, based on the table, it can be inferred that the image restoration method used successfully produces high-quality images with a low error rate. This indicates that the LSB+RS method is capable of improving the quality of stego images by reducing the generated distortion. **Figure 7** below shows the results of the improvement of the LSB and RS code:



Figure 7 LSB Image Results and RS Code

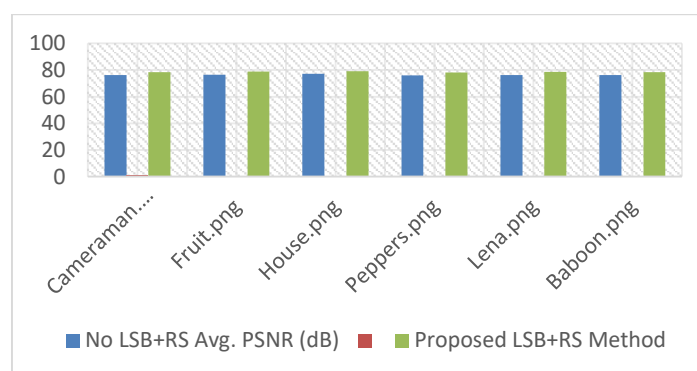


Figure 8 Comparison of Peak Signal to Noise Ratio (PSNR)

Based on **Figure 8**, the average Peak Signal-to-Noise Ratio (PSNR) for all image ranges from 76.12 to 77.32. PSNR is used to measure the quality of image restoration, and the higher the PSNR value, the better the image quality. The average PSNR for each image falls within the range of 78.3242 to 79.164177 dB, indicating that all images have good restoration quality with high PSNR values. There is a small variation in the average PSNR for each image, with a maximum difference of around 1.84 dB. The average PSNR for House.png has the highest value among all evaluated images, while Peppers.png has the lowest. This indicates that House.png has better restoration quality compared to the other images. In terms of PSNR values, all evaluated images exhibit high restoration quality and closely approach the original images.

V. Conclusion and Suggestions

Conclusion

This research provides novelty that the improvement of watermarking using Least Significant Bit with Reed-Solomon algorithm can enhance the watermarking technique to detect damage or changes in watermarked images and rectify them, ensuring that the watermark can still be extracted with average MSE and PSNR indicating high accuracy. The message was successfully embedded into the image using the Least Significant Bit (LSB) method with the Reed-Solomon algorithm for message encoding and decoding. The resulting embedded and extracted images were successfully displayed, and metrics such as MSE and PSNR were used to measure the quality of the embedded images. Improvement in imperceptibility and system robustness was achieved.

The performance evaluation of this proposed method measures two factors: PSNR and MSE. The average PSNR (Peak Signal-to-Noise Ratio) for all image ranges from 76.12 to 77.32. The improvement of watermarking with LSB and RS in the stego image system offers well-extracted images that can be used to measure the quality of image restoration.

Suggestions

The following are suggestions for future research related to the improvement of watermarking, including the following:

1. **Application to Other Domains:** In addition to images, explore the application of this method in other domains such as video, audio, or text documents. Investigate the challenges and opportunities that arise in applying this watermarking method to those domains.
2. **Optimization of Embedding Techniques:** Examine more sophisticated LSB embedding techniques. You can explore pixel grouping methods or the use of adaptive filters to enhance the security and robustness of watermarking.
3. **Subjective Evaluation:** In addition to objective metrics such as MSE and PSNR, also conduct a subjective evaluation of the watermarked images. Obtain feedback from users or expert panels to understand how this watermarking affects visual perception.
4. **Performance Evaluation:** Compare this method with other watermarking methods in terms of quality, robustness, and efficiency. Perform a comprehensive performance evaluation to demonstrate the superiority and benefits of this method compared to other approaches.

The above suggestions can provide direction for further research in the development of watermarking using LSB with Reed-Solomon Code. Also, consider recent literature and related research in this domain to gain deeper insights.

References

- [1] R. S. C. P. Singh, P. Singh, And R. S. Chadha, "A Survey Of Digital Watermarking Techniques, Applications And Attacks," *Int. J. Eng. Innov. Technol.*, Vol. 2, No. 9, Pp. 165–175, 2013.
- [2] A. Arya And S. Soni, "A Literature Review On Various Recent Steganography Techniques," *Int. J. Comput. Technol. Appl.*, Vol. 4, No. 1, Pp. 143–149, 2018.
- [3] T. K. Hazra, M. Haldar, M. Mukherjee, And A. K. Chakraborty, "A Survey On Different Techniques For Covert Communication Using Steganography," *Iosr J. Comput. Eng.*, Vol. 20, No. 2, Pp. 42–52, 2018, Doi: 10.9790/0661-2002024252.
- [4] S. D. Muyco And A. A. Hernandez, "Least Significant Bit Hash Algorithm For Digital Image Watermarking Authentication," *Acm Int. Conf. Proceeding Ser.*, Pp. 150–154, 2019, Doi: 10.1145/3330482.3330523.
- [5] F. Hartung, "Digital Watermarking Of Keynote Speech Iii Digital Watermarking," No. June 2002, Pp. 2–4, 2015.
- [6] R. Jaiswal And S. Ravi, "Robust Imperceptible Digital Image Watermarking Based On Discrete Wavelet & Cosine Transforms Original Image," Vol. 7, No. 2, Pp. 204–213, 2018.
- [7] H. Tao, L. Chongmin, J. M. Zain, And A. N. Abdalla, "Robust Image Watermarking Theories And Techniques: A Review," *J. Appl. Res. Technol.*, Vol. 12, No. 1, Pp. 122–138, 2014, Doi: 10.1016/S1665-6423(14)71612-8.
- [8] P. K. Sharma, "Analysis Of Image Watermarking Using Least Significant Bit Algorithm," *Int. J. Inf. Sci. Tech.*, Vol. 2, No. 4, Pp. 95–101, 2012, Doi: 10.5121/Ijst.2012.2409.
- [9] M. Durvey And D. Satyarthi, "A Review Paper On Digital Watermarking," *Int. J. Emerg. Trends Technol. Comput. Sci.*, Vol. 3, No. 4, Pp. 99–105, 2014.
- [10] B. Goel And C. Agarwal, "An Optimized Un-Compressed Video Watermarking Scheme Based On Svd And Dwt," 2013 6th Int. Conf. Contemp. Comput. Ic3 2013, Vol. 1, No. 4, Pp. 307–312, 2013, Doi: 10.1109/Ic3.2013.6612210.
- [11] Y. S. Singh, B. P. Devi, K. M. Singh, B. Pushpa Devi, And K. M. Singh, "A Review Of Different Techniques On Digital Image Watermarking Scheme," *Int. J. Eng. Res.*, Vol. 199, No. 2, Pp. 193–199, 2013.
- [12] M. Cedillo-Hernández, F. García-Ugalde, M. Nakano-Miyatake, And H. M. Pérez-Meana, "Robust Hybrid Color Image Watermarking Method Based On Dft Domain And 2d Histogram Modification," *Signal, Image Video Process.*, Vol. 8, No. 1, Pp. 49–63, 2014, Doi: 10.1007/S11760-013-0459-9.
- [13] A. N. Senarathne And K. De Zoysa, "Llsb: Indexing With Least Significant Bit Algorithm For Effective Data Hiding," *Int. J. Comput. Appl.*, Vol. 161, No. 5, Pp. 975–8887, 2017, [Online]. Available: [Http://www.ijcaonline.org/Archives/Volume161/Number5/Senarathne-2017-Ijca-913201.Pdf](http://www.ijcaonline.org/Archives/Volume161/Number5/Senarathne-2017-Ijca-913201.Pdf)
- [14] A. K. Singh, M. Dave, And A. Mohan, "Wavelet Based Image Watermarking: Futuristic Concepts In Information Security," *Proc. Natl. Acad. Sci. India Sect. A - Phys. Sci.*, Vol. 84, No. 3, Pp. 345–359, 2014, Doi: 10.1007/S40010-014-0140-X.
- [15] R. Sharma And J. Singh, "Image Authentication Technique Based On Digital Watermarking Using Clustering," *Int. J. Adv. Res. Comput. Sci.*, Vol. 8, No. 5, Pp. 1466–1475, 2017.
- [16] M. Z. Konyar And S. Öztürk, "Reed Solomon Coding-Based Medical Image Data Hiding Method Against Salt And Pepper Noise," *Symmetry (Basel)*, Vol. 12, No. 6, Pp. 1–16, 2020, Doi: 10.3390/Sym12060899.
- [17] B. Kitchenham, "Guidelines For Performing Systematic Literature Reviews In Software Engineering (Software Engineering Group, Department Of Computer Science, Keele ...)," No. October 2021, 2007.
- [18] R. Aarthi, V. Jaganya, And S. Poonkuntran, "Modified Lsb Watermarking For Image Authentication," *Int. J. Comput. Commun. Technol.*, Vol. 6, No. 1, Pp. 5–8, 2015, Doi: 10.47893/Ijcc.2015.1264.
- [19] P. Gaur And N. Manglani, "Image Watermarking Using Lsb Technique," Vol. 3, No. 3, Pp. 1424–1433, 2015.
- [20] N. Patel And N. Limbad, "Detection Of Tampering In Image Using Watermarking," Vol. 2, No. August, P. 2016, 2021, [Online]. Available: www.ijariie.com/840
- [21] N. Bansal, V. K. Deolia, A. Bansal, And P. Pathak, "Digital Image Watermarking Using Least Significant Bit Technique In Different Bit Positions," *Proc. - 2014 6th Int. Conf. Comput. Intell. Commun. Networks, Cicin 2014*, Pp. 813–818, 2014, Doi: 10.1109/Cicin.2014.174.
- [22] D. Chopra, "Lsb Based Digital Image Watermarking For Gray Scale Image," *Iosr J. Comput. Eng.*, Vol. 6, No. 1, Pp. 36–41, 2012, Doi: 10.9790/0661-0613641.
- [23] Y. K. Lee, G. Bell, S. Y. Huang, R. Z. Wang, And S. J. Shyu, "An Advanced Least-Significant-Bit Embedding Scheme For Steganographic Encoding," *Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, Vol. 5414 Lncs, Pp. 349–360, 2009, Doi: 10.1007/978-3-540-92957-4_31.
- [24] A. Muzakir And M. Habibi, "Watermarking Techniques Using Least Significant Bit Algorithm For Digital Image Security Standard

- Solution- Based Android,” *Sci. J. Informatics*, Vol. 4, No. 1, Pp. 20–26, 2017, Doi: 10.15294/Sji.V4i1.7290.
- [25] N. F. Johnson And G. Mason, “See The Unseeing 1998.Pdf,” *Ieee Trans. Image Process.*, P. 26, 1998.
- [26] Fabiana Meijon Fadul, “~~濟無~~no Title No Title No Title,” Vol. 5, No. September, Pp. 1–17, 2019.
- [27] A. Singh And M. Kaur, “Design And Implementation Of Reed Solomon Encoder On Fpga,” Vol. 7, No. 9, Pp. 604–606, 2013.
- [28] N. Laila And A. S. R. Sinaga, “Implementasi Steganografi Lsb Dengan Enkripsi Vigenere Cipher Pada Citra,” *Sci. Comput. Sci. Informatics J.*, Vol. 1, No. 2, P. 47, 2019, Doi: 10.22487/J26204118.2018.V1.I2.11221.
- [29] S. Andi Nurul Utami Husain, Gamantyo Hendrantoro, “Pendekodean Kanal Reed Solomon Berbasis Fpga Untuk Transmisi Citra Pada Sistem Komunikasi Satelit Nano,” *J. Tek. Pomits*, Vol. 2, No. 1, Pp. 33–38, 2013.
- [30] H. A. Jassim, Z. K. Taha, M. A. Alsaedi, And B. M. Albaker, “Enhancing Data Transfer Architecture Using Lsb Steganography Combined With Reed Solomon Code,” *Int. J. Eng. Technol.*, Vol. 7, No. 2, Pp. 24–26, 2018, Doi: 10.14419/Ijet.V7i2.29.13119.