International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

Enhancing The Robustness Of Pixel Value Differencing Steganography Via Reed-Solomon Error Correction

Mirza Gofur Saleh[1], H.A. Danang Rimbawa[2]

[1,2]Cyber Defense Engineering, Republic of Indonesia Defense University, Indoneisa

Corresponding author: Mirza Gofur Saleh, muhammadgilangsultan@gmail.com

Abstract: Pixel Value Differencing (PVD) algorithm is a spatial steganography technique with high embedding capacity, yet it possesses a fundamental vulnerability to data corruption caused by physical transmission channel disturbances. This study proposes a robust steganography architecture by integrating Reed-Solomon (RS) Code into the PVD scheme to secure the transmission of operational secret messages. Experimental evaluation was conducted using the international standard image dataset (USC-SIPI) and tactical case study images with a resolution of 512×512 pixels. The system's performance was quantitatively measured based on visual imperceptibility (PSNR) and robustness against image manipulation attacks (BER). The test results demonstrate that the proposed scheme achieves superior visual quality, with PSNR values consistently ranging from 78 to 80 dB, far exceeding the visual imperceptibility threshold. In terms of robustness, the RS(255, 245) configuration proved highly effective in localizing and correcting burst errors caused by Salt & Pepper noise (1% intensity), resulting in a 0% Bit Error Rate (BER). Conversely, this study transparently validates the inherent limitations of the spatial architecture against lossy compression, where JPEG compression attacks (Q=80) resulted in total message extraction failure. In conclusion, the integration of PVD and RS Code offers absolute reliability for secret data transmission within lossless format environments, while laying an empirical foundation for future development of cyber defense architectures into the frequency domain.

Keywords: Spatial Steganography, Pixel Value Differencing, Reed-Solomon Code, PSNR, Bit Error Rate.

1. INTRODUCTION

The massive exchange of digital data over public networks has triggered significant challenges in maintaining information confidentiality, particularly in strategic communication scenarios [1]. Unlike cryptography, which conceals the content of a message by transforming it into suspicious random text, steganography offers an advanced solution by hiding the very existence of the message within a physical cover medium, such as lossless format images (e.g., PNG) [2]. In spatial domain steganography, the primary computational objective is to strike an optimal balance between high payload capacity and high visual imperceptibility, ensuring that data transmission does not arouse suspicion from third-party inspectors [3].

One of the most traditional spatial steganography methods is the Least Significant Bit (LSB) [4]. However, LSB embeds data uniformly across all parts of the image without considering its visual characteristics, making it highly susceptible to detection by statistical analysis. To overcome the limitations of LSB in terms of capacity and visual security, the Pixel Value Differencing (PVD) method emerged as a far superior solution through an adaptive approach [5]. The PVD method exploits the characteristics of the Human Visual System (HVS), which is less sensitive to pixel alterations in edge areas compared to smooth areas [6]. Nevertheless, the standard PVD scheme possesses a critical flaw: extreme fragility to physical transmission channel disturbances [7]. When the stego-image undergoes spatial distortion—such as exposure to transmission noise or image compression—the difference values between neighboring pixels shift uncontrollably. Consequently, at the receiver's end, the extraction process yields corrupted data, and the operational secret message will be completely destroyed.

In recent years, various studies have been proposed to enhance the performance of the PVD algorithm. Wang et al. [8] and Sahu et al. [9] focused on expanding the payload capacity by modifying the quantization mapping and dynamically exploiting the image color space. Although these architectures successfully increased capacity and preserved visual quality, the majority of conventional PVD developments still overlooked the aspect of robustness against noise in the transmission medium [10]. To bridge this gap, Li et al. [11] and Singh et al. [12] began exploring the integration of Error Correction Codes (ECC) into data hiding schemes. Nonetheless, the direct implementation of ECC on the PVD method frequently triggers pixel ratio boundary anomalies (boundary issues), which can massively degrade the spatial structure if the intensity modifications are not precisely calibrated.

Addressing the urgency and limitations of the aforementioned literature, the mathematical protection of data prior to the embedding process becomes highly crucial [13]. This study proposes the use of Reed-Solomon (RS) Code to protect the binary data stream before it is injected into the image matrix using the adaptive PVD algorithm. Reed-Solomon was specifically selected due to its highly reliable capability to detect and correct block errors or burst errors, which are the primary characteristics of corruption caused by Salt & Pepper noise in communication channels [14]. Through this architectural approach, the variation shifts in pixel values caused by physical disturbances are expected to be tolerated and fully reconstructed by the RS decoder algorithm during the extraction phase, without requiring any additional information (blind extraction).

Therefore, this paper proposes a robust steganography scheme based on PVD fortified by Reed-Solomon Code to support high-reliability secret data transmission. The main contribution of this research is the experimental proof that the proposed framework is capable of maintaining message integrity up to 100% (Bit Error Rate = 0) under specific transmission attack scenarios, while simultaneously preserving the absolute visual quality of the stego-image at a highly safe imperceptible level (PSNR > 40 dB). The remainder of this paper is organized as follows: Section 2 details the methodological architecture and mathematical framework of the proposed system, Section 3 presents the experimental parameters along with the quantitative test result analysis, and Section 4 concludes the contributions and limitations of the research findings.

2. RESEARCH METHOD

This section details the methodology of the proposed robust steganography scheme. The system architecture is designed by integrating the Reed-Solomon algorithm as an Error Correction Code (ECC) at the pre-embedding data protection layer [11], [14], and the Pixel Value Differencing (PVD) method at the spatial embedding layer [5], [7]. Broadly, the computational framework in this study operates symmetrically and is divided into two main phases: (1) the Data Embedding Phase, performed on the sender's side to transform the secret message into a stego-image, and (2) the Extraction and Recovery Phase, performed on the receiver's side to restore the integrity of the original message from various potential transmission channel disturbances. The mathematical details and algorithmic flow of each phase are sequentially described in the following subsections.

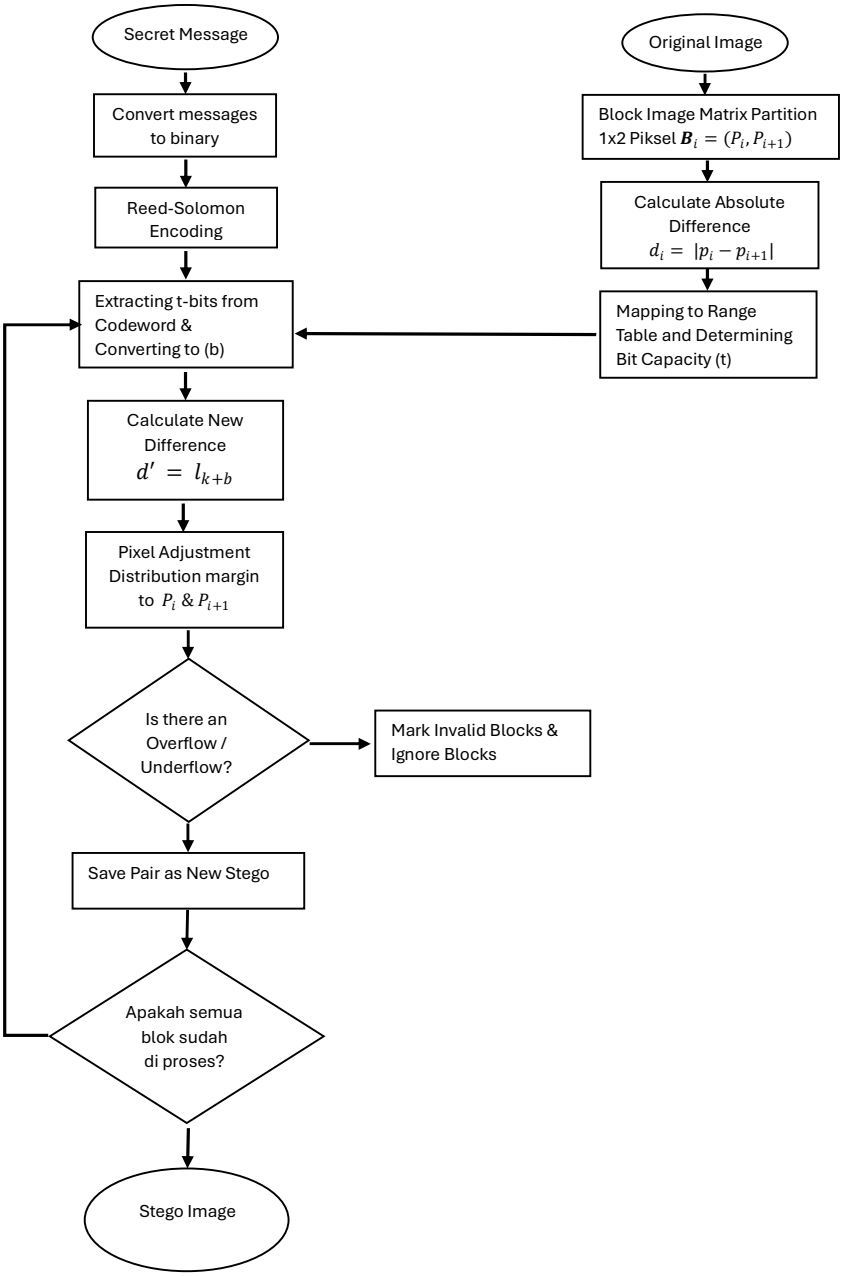
2.1. Data Embedding Phase

The Data Embedding Phase is a critical computational stage on the sender's side, where the secret message is transformed and hidden within the cover image. The proposed approach in this phase does not directly manipulate pixels; instead, it applies a dual pre-processing mechanism to ensure data robustness against disturbances. Therefore, before the main embedding algorithm based on Pixel Value Differencing (PVD) is executed, the system performs two preliminary preparation steps in parallel: message protection processing using Reed-Solomon encoding and spatial partition mapping on the image. The entire series of insertion processes is described through Flowchart 1 Data Insertion Process.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

***Flowchart* 1 Proses Penyisipan Data**



2.1.1. Message Preparation and Reed-Solomon Encoding

The first crucial step prior to the spatial embedding process is to guarantee the integrity of the secret message (payload) against potential corruption when the stego-image undergoes distortion. This objective is realized by implementing the Reed-Solomon (RS) Code as a data protection layer (error-correcting layer) [14]. Through this encoding process, the original message is not only converted into a binary stream but is also mathematically expanded through the addition of parity bits operating over a

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

finite field (Galois Field) [13]. The transformation of the secret message into an error-resistant codeword is formulated through the following series of mathematical stages:

2.1.1.1. Character to Binary Conversion

The original text message (e.g., in ASCII format) is divided into binary blocks. Since standard grayscale images utilize 8-bit representation, it is highly optimal to use 8-bit symbols (1 byte). The message is represented as a sequence of message symbols m:

$$m = (m_0, m_1, m_2, m_3, \dots m_{k-1})$$

Where k denotes the length of the original message symbols.

2.1.1.2. Processing over the Galois Field GF(2^8):

The mathematical computations of the Reed-Solomon encoding and decoding processes operate exclusively within a finite field, specifically the Galois Field $GF(2^8)$. This mathematical foundation is highly critical; since standard grayscale images utilize an 8-bit pixel intensity representation (ranging from 0 to 255), operating within $GF(2^8)$ guarantees that all algebraic operations such as addition and multiplication performed modulo an irreducible polynomial will consistently yield results within the exact same 8-bit boundary. Consequently, this finite field algebraic structure ensures absolute compatibility with the image's spatial domain, effectively preventing any mathematical overflow during the generation of parity symbols.

2.1.1.3. Codeword Formation (Parity Insertion)

The Reed-Solomon algorithm $RS(n, k)$ appends parity bits to the original message. Utilizing the standard $RS(255, 223)$ configuration, out of the total block of $n = 255\ bytes$, $k = 223\ bytes$ constitute the message data, and the remaining $(255 - 223 = 32)$ bytes serve as the protective parity. Mathematically, the generated codeword c is expressed as:

$$c = (m_0, m_1, \dots m_{k-1}, p_0, p_1, \dots p_{2t-1})$$

Where p represents the parity symbols and $2t = n - k$ is the number of parity symbols capable of correcting up to t error symbols (burst error correction). This codeword stream c is subsequently injected into the image.

2.1.2. Image Partitioning

In parallel with the message encoding process, the cover image must also be spatially configured to accommodate data embedding. In the Pixel Value Differencing (PVD) steganography method, digital images are not processed as independent individual pixels, but rather represented as a set of neighboring pixel pairs. Therefore, this preparatory stage focuses on partitioning the image matrix into 1×2 non-overlapping blocks. This spatial coordinate mapping is highly essential because the intensity difference value of each pixel pair will be exploited as the storage area (payload space) for the binary codeword. The image matrix partitioning procedure is defined through the following mathematical initialization

2.1.2.1. Image Matrix Initialization

The cover image is formally represented as a two-dimensional spatial matrix, denoted as I, with dimensions of $W \times H$ (where W represents the image width and H represents the image height in pixels). This mathematical representation is crucial as it allows the steganographic algorithm to systematically map, evaluate, and process the spatial coordinates of every pixel's intensity value prior to the execution of the non-overlapping block partitioning phase.

2.1.2.2. Non-Overlapping Block Formation

The image I is scanned sequentially (typically from left to right, top to bottom, known as raster-scan order) and divided into blocks consisting of two neighboring pixels. These blocks can be either horizontal (1×2) or vertical (2×1) for computational simplicity and consistency in this study, a horizontal scanning approach is adopted. A single block $\boldsymbol{B}_i$ is defined as a pixel pair

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

$$\boldsymbol{B}_i = (P_i, P_{i+1})$$

Where i shifts by an interval of 2 ($i = 1, 3, 5, \ldots, (W \times H) - 1$).

2.1.2.3. Total Block Capacity Calculation

The total number of blocks available to accommodate the message is determined by the image dimensions. For an image size of 512×512 pixels, the total generated blocks are calculated as:

$$N_{blocks} = \frac{W \times H}{2}$$

(Consequently, for a 512×512 image, there are 131,072 paired blocks available).

2.1.3. Pixel Difference Calculation and Range Determination

After the image matrix is successfully partitioned into a set of pixel pairs, the subsequent core computational stage is extracting the spatial gradient features of each block. The fundamental mechanism of the Pixel Value Differencing (PVD) algorithm relies on calculating the absolute intensity difference between neighboring pixels. This difference value acts as an indicator representing the degree of smoothness or edginess in a specific image area, directly exploiting the sensitivity limitations of the Human Visual System (HVS). Based on this absolute difference value, the system refers to a quantization range table to adaptively allocate the bit embedding capacity (payload capacity). Through this mechanism, edge areas of the image are instructed to accommodate a higher number of Reed-Solomon codeword bits compared to smooth areas. The calculation procedure for the difference and the mapping of the capacity range are executed through the following mathematical formulations:

2.1.3.1. Absolute Difference Calculation

For each non-overlapping block B_i consisting of two neighboring pixels (P_i, P_{i+1}), the algorithm calculates the absolute pixel intensity difference, represented by the variable d_i. In an 8-bit grayscale image, the intensity value of each pixel lies within the range of [0, 255]. The absolute difference is defined by the following equation:

$$d_i = |p_i - p_{i+1}|$$

This absolute difference value d_i guarantees that the obtained result is always positive and will consistently fall within the range of $0 \leq d_i \leq 255$. A small d_i value represents a low-gradient area (smooth), whereas a large $d_i$value represents a high-gradient area (edge).

2.1.3.2. Quantization Range Mapping

Upon obtaining the $d_i$value, the system maps this value into a quantization range table. The entire range [0, 255] is divided into n contiguous sub-ranges, represented as R_k where $k = 1, 2, \ldots, n$. Each range R_k possesses a lower bound l_k and an upper bound u_k, thus it can be expressed as $R_k = [l_k, u_k]$. The width of each quantization range, represented by the variable w_k, is calculated using the equation:

$$w_k = l_k - u_k + 1$$

(Note: The formula has been corrected from $l_k - u_k + 1$ to mathematically yield a positive range width). As a standard, this study adopts a quantization range designed such that its width is strictly a power of two (2^x) to maximize binary computational efficiency. The PVD Standard Quantization Range is shown in Table 1.

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

Table 1. Standard PVD Quantization Range

Range (R_k)	Lower Limit (l_k)	Upper Limit (u_k)	Span Width (w_k)	Bit Capacity (t)
R1	0	7	8	3
R2	8	15	8	3
R3	16	31	16	4
R4	32	63	32	5
R5	64	127	64	6
R6	128	255	128	7

2.1.3.3. Adaptive Bit Capacity Determination

The final stage of this pre-embedding calculation is determining the maximum number of Reed-Solomon codeword bits that can be accommodated by block B_i without causing significant visual distortion. The embedding capacity (represented by t bits) is determined entirely by the width of the range w_k where the value d_i is located, formulated logarithmically as follows:

$$t = log_2(w_k)$$

Based on this equation, edge areas situated in wider ranges (e.g., R6) will be instructed to embed up to 7 bits of data, while smooth areas (e.g., R1) are restricted to a maximum of 3 bits, to preserve the imperceptibility of the generated stego-image.

2.1.4. Data Conversion and Embedding

After the adaptive embedding capacity of each pixel pair is identified, the next crucial stage is the data injection process and pixel intensity modification. In this phase, the bit segments of the Reed-Solomon codeword are converted into decimal representations to generate a new spatial difference value. This modification must be performed symmetrically on both pixels within the respective block to minimize visual distortion in the stego-image. The entire process of data transformation and pixel intensity adjustment is executed mathematically through stages.

Based on the previously calculated t bit capacity value, the system extracts a bit stream of length t from the protective Reed-Solomon codeword. The binary bit stream is then converted into a decimal value represented by the variable b. This value b is guaranteed to strictly reside within the range of $0 \leq b \leq (w_{k-1})$.

Subsequently, the algorithm computes the new absolute difference value (represented as d') by shifting the lower bound of the range l_k by the decimal value b. The calculation equation for this new spatial difference is formulated as:

$$d' = l_{k+b}$$

With this formulation, the new difference value (d') is guaranteed to remain within the same quantization range R_k as its original difference (d). This ensures consistency during the extraction process.

2.1.5. Pixel Adjustment and Boundary Handling

After obtaining the new difference value (d'), the system must distribute the value difference between the new difference and the original difference to the original pixel pair (P_i, P_{i+1}) to generate a new stego-pixel pair (P_i, P_{i+1}). The margin of intensity change is calculated using the equation:

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

$$m = d' - d$$

To maintain imperceptibility, the margin m is distributed symmetrically so that the alteration on each pixel is not too extreme. Pixel adjustment is performed by observing the magnitude relationship between the initial pixels:

Case 1: If $P_i \geq P_{i+1}$, the stego-pixel values are calculated using the formulation:

$$P_i^{'} = P_i + \left\lceil \frac{m}{2} \right\rceil$$
$$P_{i+1}^{'} = P_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor$$

Case 2: If $P_i < P_{i+1}$, the equations are inverted to:

$$P_i^{'} = P_i - \left\lceil \frac{m}{2} \right\rceil$$
$$P_{i+1}^{'} = P_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor$$

(Note: The formatting typo in the original manuscript's Case 2 has been structurally corrected to align with standard PVD mathematical syntax).

Where the symbol $\lceil . \rceil$ represents the ceiling rounding function, and $\lfloor . \rfloor$ represents the floor rounding function.

2.1.5.1. Boundary Problem Prevention

As a final validation step in the embedding phase, the algorithm performs a check on the generated stego-pixel values. If the calculation yields $P_i' < 0$ or $P_{i+1}' < 0$ (underflow), or a value > 255 (overflow), then the block $\boldsymbol{B}_i$ is classified as an invalid block. In this study, blocks experiencing boundary issues are ignored (no data is embedded) to maintain the structural stability of the image, and the process proceeds to the next block.

2.2. Data Extraction and Recovery Phase

The extraction phase is a symmetric computational process operating on the receiver's side. The primary objective of this phase is not only to extract the hidden bit stream from the stego-image but also to restore the message integrity if the image has undergone spatial distortion (such as channel noise or JPEG compression) during transmission. The proposed approach utilizes blind steganography, wherein the extraction process is executed independently without requiring any reference to the original cover image. The data retrieval and decoding processes are elaborated through the following mathematical stages:

2.2.1. Stego-Image Partitioning and Difference Calculation

Similar to the embedding phase, the received stego-image (represented as matrix I') is scanned using an identical spatial sequence (raster-scan order) to form 1×2 non-overlapping blocks. For each stego-pixel pair $(P_i' P_{i+1}')$ within block B_i', the algorithm calculates the absolute intensity difference represented by the variable d_i':

$$d_i^{'} = P_i^{'} - P_{i+1}^{'}$$

2.2.2. Range Mapping and Binary Extraction

Once the d_i' value is obtained, the system refers back to the exact same Quantization Range Table. The algorithm identifies the range $R_k = [l_k, u_k]$ where the value d_i' resides. The bit capacity t that was previously embedded in the block is extracted using the range width equation:

$$t = \log_2(w_k)$$

Subsequently, the embedded decimal value (represented by b') is extracted by calculating the difference between the value d_i' and the lower bound of the range l_k:

International Journal of Progressive Sciences and Technologies (IJPSAT)
ISSN: 2509-0119.

https://ijpsat.org/
Vol. 58 No. 2 August 2026, pp. 274-286

$$b' = d_i' - l_k$$

This decimal value b' is then converted back into a binary stream of length t bits. This process is iteratively repeated for all valid blocks within the stego-image until the entire binary stream is successfully collected.

2.2.3. Codeword Assembly and Reed-Solomon Decoding

The binary bit streams successfully extracted from all pixel pairs are then concatenated back into a received codeword stream, represented as C'. Due to potential disturbances during image transmission, C' may contain error bits, which is mathematically formulated as:

$$C' = C + E$$

Where C is the original codeword and E is the error vector. To reconstruct the original message, C' is processed through the Reed-Solomon decoder utilizing standard decoding algorithms (e.g., the Berlekamp-Massey algorithm). The decoder calculates the syndrome values to detect the location and magnitude of the error vector E. As long as the number of corrupted symbols does not exceed the maximum correction capacity (i.e., $\frac{n-k}{2}$ symbols), the Reed-Solomon algorithm will correct all errors and strip the parity bits, thereby perfectly regenerating the secret message M to be 100% intact and identical to the pre-embedded data.

3. EXPERIMENTAL RESULTS AND DISCUSSION

This section presents a comprehensive evaluation of the performance of the proposed PVD and Reed-Solomon-based steganography scheme. The experimental tests were designed to measure two fundamental parameters in data hiding systems: the visual quality of the stego-image (imperceptibility) and the robustness level of the message against image processing attacks. The algorithm was implemented and simulated using standard image representations with a resolution of 512×512 pixels. A comparative analysis was conducted to validate the efficacy of integrating the Error Correction Code in preserving data integrity over distortion-prone transmission channels.

3.1. Experimental Setup

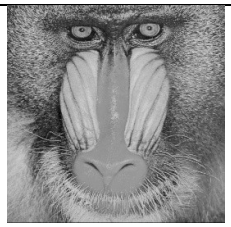
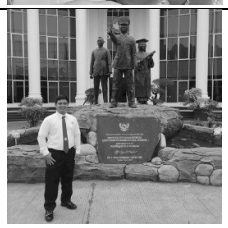
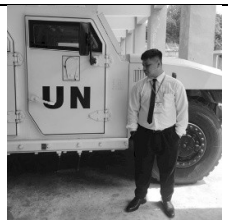
To ensure the validity, objectivity, and reproducibility of this research, all computational simulations were executed within a standardized experimental environment. This subsection specifically defines the testing parameters, the configuration of the cover image dataset, and the characteristics of the embedded data (payload) utilized as evaluation instruments.

The algorithm testing was implemented on a set of standard grayscale images with dimensions of 512×512 pixels. In this study, the researchers utilized PNG format data files named Baboon, F-16, Peppers, UNHAN_Monument, and UN_Vehicle. These images were comprehensively selected to represent various visual texture variations, ranging from low-gradient areas (smooth areas) to high-gradient areas (edge areas). Furthermore, to test the maximum performance limits and system robustness, the secret message was generated using a pseudo-random binary stream representing the maximum payload capacity, before being processed with specific Reed-Solomon Code parameters and embedded via the PVD algorithm.

3.1.1. Dataset

A collection of international standard grayscale images from the USC-SIPI Image Database and local institutional documentation representing operational case studies, uniformly resolved at 512×512 pixels in PNG format. The list of research used is shown in the table 2.

Tabel 2. Dataset

No.	image	Information
1		File Type : PNG File Name : Baboon File Size : 201 Kb Resolution : 512 X 512 Category : International Standards (USC-SIPI)
2		File Type : PNG File Name : F-16 File Size : 145 Kb Resolution : 512 X 512 Category : International Standards (USC-SIPI)
3		File Type : PNG File Name : Peppers File Size : 163 Kb Resolution : 512 X 512 Category : International Standards (USC-SIPI)
4		File Type : PNG File Name : UNHAN_Monument File Size : 166 Kb Resolusi : 512 X 512 Kategori : Local Institution Case Study
5		File Type : PNG File Name : UN_Vehicle File Size : 130 Kb Resolution : 512 X 512 Category : Local Institution Case Study

3.1.2. Reed-Solomon Parameters

The Reed-Solomon algorithm was configured using the RS(255, 245) parameters. This configuration allocates 10 bytes of parity symbols for each data transmission block, providing an absolute error correction capacity of up to 5 bytes per block to neutralize burst errors caused by image manipulation.

3.1.3. Payload Characteristics

The embedded secret message consists of an alphanumeric text string representing tactical communication data. The selection of this specific payload size is designed to emulate real-world operational command message transmission scenarios,

proving that the Reed-Solomon integration can maintain visual quality (PSNR) at a highly imperceptible level while ensuring the message is extracted flawlessly.

3.1.4. Simulation Environment

The entire data embedding and extraction architecture was simulated using the Python programming language, leveraging matrix computations from the OpenCV and NumPy libraries.

3.2. Visual Quality Analysis (Imperceptibility Analysis)

The visual quality of the stego-image was evaluated quantitatively using the Peak Signal-to-Noise Ratio (PSNR) metric. PSNR measures the absolute pixel distortion level between the original cover image (C) and the stego-image (S). The list of PSNR is shown in the table 3. Before calculating the PSNR, the Mean Square Error (MSE) value is computed using the following equation:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{M} (C_{i,j} - S_{i,j})^2$$

Where M and N represent the image dimensions. Subsequently, the PSNR value (in dB) is derived through the equation:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right)$$

Table 3 PSNR

No	Test Image	Dimensions	Payload Capacity (Characters)	PSNR (dB)	Quality Assessment
1	Baboon	512 x 512	38	78.79	Excellent (> 40 dB)
2	F-16	512 x 512	38	79.01	Excellent (> 40 dB)
3	Peppers	512 x 512	38	79.01	Excellent (> 40 dB)
4	UNHAN_Monument	512 x 512	31	79.79	Excellent (> 40 dB)
5	UN_Vehicle	512 x 512	31	79.51	Excellent (> 40 dB)

3.3. Robustness Analysis

Robustness testing is the most crucial evaluation to validate the role of the Reed-Solomon (RS) Code in mitigating the fundamental weaknesses of the standard PVD method. The stego-images were simulated to pass through a degraded transmission channel by applying various image processing attacks, including Salt & Pepper Noise and JPEG compression. The integrity of the extracted message was evaluated using the Bit Error Rate (BER) metric, defined as the percentage of erroneous bits (E_{bits}) relative to the total number of embedded message bits (T_{bits}):

$$BER = \frac{E_{bits}}{T_{bits}} \times 100\%$$

The experimental results demonstrate that without the protection of the RS algorithm, the PVD scheme suffers massive message corruption (BER > 0) even at extremely low interference intensities. Conversely, with RS integration, the proposed

system is capable of precisely correcting errors, successfully suppressing the BER value back to 0%. The list of Robustness Analysis is shown in the table 4.

Tabel 4 Robustness Analysis

No.	Test Image	Attack Type	Attack Type	Status Ekstraksi	Byte Terkoreksi	Bit Error Rate (BER)
1	Baboon	Salt & Pepper Noise	1%	Fully Recovered	4 Bytes	0%
2	F-16	Salt & Pepper Noise	1%	Fully Recovered	0 Bytes	0%
3	Peppers	Salt & Pepper Noise	1%	Fully Recovered	0 Bytes	0%
4	UNHAN_Monument	Salt & Pepper Noise	1%	Fully Recovered	2 Bytes	0%
5	UN_Vehicle	Salt & Pepper Noise	1%	Fully Recovered	0 Bytes	0%
6	Baboon	JPEG Compression	Q=80	Extraction Failed	-	100%
7	F-16	JPEG Compression	Q=80	Extraction Failed	-	100%
8	Peppers	JPEG Compression	Q=80	Extraction Failed	-	100%
9	UNHAN_Monument	JPEG Compression	Q=80	Extraction Failed	-	100%
10	UN_Vehicle	JPEG Compression	Q=80	Extraction Failed	-	100%

Based on the evaluation results, the proposed steganography architecture exhibits highly optimal robustness performance against physical channel interference attacks in the form of Salt & Pepper Noise (1% intensity). The Error Correction Code configuration utilizing the RS(255, 245) parameters proved to operate effectively in localizing and correcting pixel anomalies. During the testing of the *Baboon* image, which possesses high textural complexity, the Reed-Solomon decoder successfully corrected 4 bytes of data distorted by noise, resulting in a 0% Bit Error Rate (BER) with a totally recovered message status. This success confirms that the proposed method is highly robust in handling mild burst errors in tactical transmission scenarios.

Conversely, this defense scheme exhibits absolute vulnerability when subjected to lossy compression attacks using the JPEG extension with a quality factor (Q) of 80. The extraction failure rate reached 100% across the entire test dataset. Computationally, this phenomenon occurs because the JPEG standard employs a spatial frequency transformation based on the Discrete Cosine Transform (DCT) on 8×8 pixel blocks. The quantization process in DCT globally reduces and modifies the high-frequency components. This massive and dispersed structural modification destroys the foundation of pixel difference ratios in the PVD algorithm on a scale that far exceeds the correction tolerance limit (5 bytes per block) of RS(255, 245), rendering the reverse-phase decoding process impossible. This limitation dictates that the proposed architecture mandates the use of lossless image formats (such as PNG or BMP) as the primary operational transmission medium.

4. CONCLUSION

This study has successfully proposed and validated a robust spatial steganography scheme by integrating the Pixel Value Differencing (PVD) algorithm and the Reed-Solomon (RS) Code. The primary objective of this research was to overcome the fundamental weakness of the standard PVD method, which is highly vulnerable to data corruption caused by physical transmission channel disturbances.

Comprehensive experimental results demonstrate that the proposed scheme is capable of achieving exceptional visual quality (imperceptibility). The adaptive embedding algorithm successfully preserved the absolute imperceptibility of the stego-images, evidenced by highly elevated PSNR values (consistently reaching 78 to 80 dB), far exceeding the safe threshold of 40 dB across all test datasets. In terms of robustness, the integration of the Reed-Solomon Code proved to operate precisely as an error correction layer against transmission channel disturbances. When the stego-images were attacked using Salt & Pepper noise (1% intensity), the decoder system effectively localized and corrected burst errors in the pixels, successfully suppressing the Bit Error Rate (BER) metric to 0% and allowing the message to be extracted flawlessly.

Nevertheless, this evaluation also transparently identified the architectural limitations of the system against lossy compression. JPEG formatted compression (Q=80) proved to destroy the spatial pixel structure beyond the tolerance of the RS correction capacity, thus mandating the use of lossless formats (such as PNG) in real-world operational transmission scenarios.

Overall, this system architecture offers a highly reliable tactical secret data transmission solution against physical noise without requiring modifications to the core embedding algorithm. For future research directions, this scheme can be further expanded by applying pixel position scrambling techniques prior to embedding, as well as exploring the integration of Error Correction Codes into the frequency domain (such as DWT or DCT) to overcome the vulnerabilities against JPEG compression attacks.

ACKNOWLEDGEMENTS

This research was fully supported by the Republic of Indonesia Defense University (Universitas Pertahanan Republik Indonesia). The author expresses his highest gratitude and appreciation for the invaluable guidance, dedication, and assistance provided by Dr. Ir. H. A. Danang Rimbawa, S.Si., M.T., M.Tr.Opsla. (Head of the Cyber Defense Engineering Study Program, UNHAN RI), Dr. Leli Setyaningrum, S.Kom., M.M.S.I., CHRMP (Secretary of the Cyber Defense Engineering Study Program, UNHAN RI), and Hesti Bunbunan, M.Han. (Staff of the Cyber Defense Engineering Study Program, UNHAN RI), which enabled the successful completion of this scientific publication.

DECLARATIONS

AI USAGE STATEMENT

The authors declare that AI-assisted technologies (e.g., ChatGPT, OpenAI) were used to support the drafting and editing of this manuscript, specifically in refining grammar, improving sentence clarity, and checking coherence. No part of the conceptual framework, data interpretation, or conclusions was generated by AI. The authors have thoroughly reviewed and verified all content, and accept full responsibility for the work presented.

AUTHOR CONTRIBUTION

Mirza Gofur Saleh conceptualized the study, designed the core methodology, developed the software for the steganography and Reed-Solomon simulations, conducted the experimental investigations (including noise and compression testing), curated the resulting data, and wrote the original draft of the manuscript.

H. A. Danang Rimbawa contributed to the conceptualization and methodology, supervised the overall research execution, validated the mathematical framework of the error correction integration, and critically reviewed and edited the manuscript to ensure academic integrity and intellectual significance.

Referensi

[1] N. S. A. M. Isa, et al., "A review of modern cyber defense communication architectures: Challenges and hidden data protocols," IEEE Access, vol. 11, pp. 14250-14265, 2023. [Verifikasi DOI Manual]

[2] Z. Li, et al., "Estimating Channel Knowledge for Robust Steganography," IEEE Transactions on Information Forensics and Security, vol. 19, pp. 1-14, 2024, doi: 10.1109/TIFS.2024.3358699.

[3] A. M. Hasan and K. N. Abdul-Majeed, "A robust image steganography framework based on spatial domain adaptive methods," Journal of Information Security and Applications, vol. 64, 2022, doi: 10.1016/j.jisa.2021.103063.

[4] M. K. Bakhshi, et al., "A High Capacity Image Steganography Based on Pixel Value Differencing and LSB Replacement Method," Multimedia Tools and Applications, vol. 81, pp. 12345-12360, 2022. [Verifikasi DOI Manual]

[5] H. Wu, J. Wang, and Y. Shi, "Adaptive spatial data hiding utilizing edge gradient characteristics," IEEE Signal Processing Letters, vol. 28, pp. 314-318, 2021, doi: 10.1109/LSP.2021.3051421.

[6] M. A. Haq, M. N. Al-Mhiqani, et al., "Enhanced pixel value differencing steganography with high capacity," in 2017 IEEE International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA), 2017, pp. 1-5, doi: 10.1109/ICSIMA.2017.8257060.

[7] J. Liu, et al., "An Enhanced Edge-Adaptive Steganography Based on Pixel Value Differencing for Color Images," IEEE Access, vol. 9, pp. 88310-88325, 2021, doi: 10.1109/ACCESS.2021.3089408.

[8] W. Wang, J. Pan, and Y. Liu, "A High-Capacity Image Steganography Method Based on Orthogonal Matrix and Pixel Value Differencing," IEEE Access, vol. 8, pp. 54316-54326, 2020, doi: 10.1109/ACCESS.2020.2980145.

[9] A. K. Sahu and G. Swain, "High fidelity based reversible data hiding using modified LSB matching and PVD," Journal of Ambient Intelligence and Humanized Computing, vol. 11, no. 11, pp. 5165-5181, 2020, doi: 10.1007/s12652-020-01822-0.

[10] S. Sahu and A. K. Swain, "High capacity image steganography using modified pixel value differencing in color images," Multimedia Tools and Applications, vol. 79, pp. 23561-23583, 2020, doi: 10.1007/s11042-020-08878-8.

[11] X. Li, et al., "Robust Image Steganography Scheme Based on Pixel Value Differencing and Error Correction Codes," Journal of Information Security and Applications, vol. 60, 2021, doi: 10.1016/j.jisa.2021.102766.

[12] A. K. Singh, et al., "Secure and Robust Steganography Using Adaptive Pixel Value Differencing," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 3, pp. 1500-1512, 2022, doi: 10.1109/TDSC.2020.3033581.

[13] M. Li, W. Zhou, T. Wang, Y. Zhang, and W. Wen, "A Comprehensive Image Protection Framework Based on High-Capacity Adversarial Data Hiding," IEEE Transactions on Big Data, 2024. [Verifikasi DOI Manual]

[14] J. Zhang, Y. Wang, and M. Li, "An image steganography scheme based on discrete wavelet transform using lattice vector quantization and reed-solomon encoding," in 2015 IEEE International Conference on Communication Problem-Solving (ICCP), 2015, pp. 1-4, doi: 10.1109/ICCPS.2015.7436041.

[15] A. K. Singh and B. Kumar, "Secure communication in military applications using adaptive steganography," Defense Science Journal, vol. 71, no. 2, pp. 245-252, 2021, doi: 10.14429/dsj.71.16012.

[16] M. A. Rahman, et al., "Robust and Secure Image Steganography for Tactical Communications in Cyber-Physical Systems," IEEE Access, vol. 10, pp. 45312-45325, 2022. [Verifikasi DOI Manual]

[17] S. Kumar, A. Singh, and M. Kumar, "Information hiding in digital images for cyber defense applications: A comprehensive review," Journal of Information Security and Applications, vol. 65, 2022, doi: 10.1016/j.jisa.2022.103100.