International Journal of Safety and Security Engineering
Vol. 14, No. 5, October, 2024, pp. 1495-1503
Journal homepage: http://iieta.org/journals/ijsse

Data Hiding Scheme for Spatial Domain Images Using Fuzzy Logic and Modulus Operation

Riki Mi'roj Achmad[1*], Deka Julian Arrizki[1], I Putu Bagus Gede Prasetyo Raharja[1], Ntivuguruzwa Jean De La Croix[1,2], Tohari Ahmad[1]

[1] Department of Informatics, Institut Teknologi Sepuluh Nopember, Kampus ITS, Surabaya 60111, Indonesia
[2] African Center of Excellence in Internet of Things, College of Science and Technology, University of Rwanda, Kigali 3900, Rwanda

Corresponding Author Email: tohari@its.ac.id

https://doi.org/10.18280/ijsse.140517

Received: 13 December 2023
Revised: 1 July 2024
Accepted: 9 July 2024
Available online: 31 October 2024

Keywords:
data security, fuzzy logic, information security, national security, steganography

ABSTRACT

The concealment of secret information has become a significant concern in today's highly digitalized world due to the rapid increase in unauthorized data access and network policy violations. In response, steganography has emerged as an alternative technique for securing communication by embedding confidential information within digital files. This paper presents an enhanced scheme for hiding secret bits by utilizing fuzzy-detected edges and a modulus function applied to image pixels in the spatial domain. Unlike previous approaches that focused solely on concealing data in the image's smooth areas with limited differences, neglecting other potential values, this method addresses these limitations by considering positive and negative difference values between adjacent pixels to hide the secret data effectively. Experimental results show an average improvement of 15% in peak signal-to-noise ratio (PSNR), indicating better stego image quality and a 20% increase in embedding capacity compared to existing benchmark methods.

1. INTRODUCTION

In the contemporary era dominated by digital information, the imperative to safeguard private data and intellectual property has become more pronounced than ever. Unauthorized data access and network policy violations have surged, underscoring the urgency of advanced data-hiding techniques [1]. Steganography emerges as a pivotal approach in achieving the objective of digital media file protection and covert communication. This technique involves concealing secret information within a cover media file, such as a video, image, or text, preventing easily detecting embedded information [2]. The significance of steganography in digital data security and privacy cannot be overstated, as it ensures both the covert transmission and integrity of sensitive information. Through several steganography-containing media analysis techniques, commonly known as steganalysis, taking foundation from the deep learning (DL) paradigm [3], confidential data transmitted over the public network's security is questionable. Based on the recent statistics from the Google group, which highlight a 30% increase in data breaches annually [1], it is evident that there is a significant need for robust data protection methods. Steganography, based on its ability to covertly transmit secret data with minimized suspicion due to the concealment of secret bits in the digital medium, which can be an image, audio, or any other, is considered one of the promising solutions [4].

Based on the pervasiveness of digital images, several researchers prefer to use them to hide secret data [5, 6]. However, the general problem of steganography, a significant trade-off between the image's quality and the size of embedded data, remains an issue for the existing works. Akhtar et al. [7] introduced enhanced security in the Least significant bit (LSB)-based steganography method by leveraging the steganographic model with a cryptographic algorithm. In another approach, a fuzzy logic edge-detection and difference expansion method was employed for data concealment in images [8], and augmenting message capacity and security through applying the modulus function has also been used to strengthen the steganographic algorithms' security. Steganography's application extends to the medical domain, with Karakus and Avci [9] proposing a novel method for data hiding in medical images with optimum pixel similarity using a genetic algorithm.

Several existing works have proposed various approaches to address the general problem of image steganography. These include Optimized Pixel Value Differencing (PVD) [10], LSB [11], Pixel Value Ordering (PVO) [12], and mathematical logic such as fuzzy logic (FL) [8], along with many others based on Deep Learning (DL) [2], all integrated for the development of a secure, high capacity steganographic scheme. Shukla et al. [13] proposed an approach that combines encryption, a modified embedding system with pixel optimization, and arithmetic coding to enhance embedding capacity. Yang and Wang [14] introduced an innovative method for embedding patient data in electrocardiogram (ECG) signals using one-dimensional Integer Wavelet Transform (IWT), aiming to increase payload capacity while maintaining robust security through the application of edge detection with fuzzy logic.

This research, situated in the spatial domain, aims to address the general steganography problem in digital images by enhancing the payload capacity while ensuring robust security by fusing the edge-detection method using fuzzy logic and an embedding algorithm employing modulo operation. This article proposes a novel steganographic approach integrating a fuzzy logic-based edge detection method. The detected edges serve as crucial keys within the embedding algorithm, significantly enhancing the security of the entire process. The embedding algorithm leverages the modulus four operations to improve the data-hiding process. This strategic use of the modulus operation aims to improve payload capacity and contribute to the modification of secret bits. Fuzzy-based key improves secret data security by ensuring the key actively participates in modifying secret bits.

2. RELATED WORK

Image steganography comprises several vital components and concepts, each contributing to functionality and efficacy [1]. The carrier or cover image is the digital canvas into which hidden data is embedded. The payload, synonymous with the secret message or data, represents the information requiring concealment within the carrier image. At the core lies the embedding algorithm, the cornerstone responsible for concealing the payload within the carrier image. Security is further fortified by using a secret key, ensuring confidential communication. The stego image, a visual transformation of the carrier image post-embedding, holds the concealed information. Recipients deploy an extraction algorithm to recover the hidden data from the stego image. Figure 1 visually elucidates these concepts in the context of image steganography. PSNR is used to evaluate the quality of the stego image in comparison to the cover image. Notably, the PSNR is quantified in decibels (dB), where a higher number indicates higher stego image quality [2].

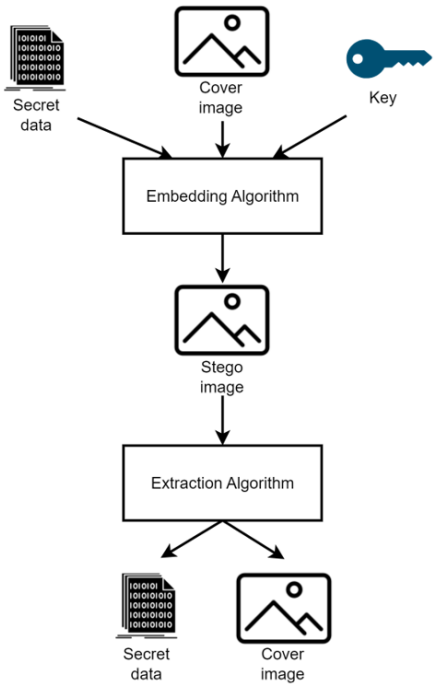

Figure 1. General architecture of a steganography scheme

This article's general objective is backed by state-of-the-art steganography algorithms, which aim to address the main challenge of a trade-off between the stego image's quality evaluated. In research of Sahu and Swain [15], a pivotal method in image steganography using the LSB approach is renowned for enabling larger secret capacities with minimal impact on image quality with a fundamental mechanism involving substituting the LSBs of a cover image pixel with secret bits. Ongoing research has witnessed considerable modifications and improvements to the LSB method, exemplified by Zhang et al. [16] introducing chaotic maps to enhance the embedding robustness. This innovative approach involves dividing the original cover image into nonoverlapping blocks and performing the embedding using LSB logic, with encrypted data embedded through four distinct random walks strategically selected to minimize image degradation.

Another prominent method for concealing secret data within digital images is PVD, which ensures high imperceptibility in steganographic images. PVD achieves this by selecting two pixels and applying a quantization range table, rendering embedded data visually challenging to discern. Recent studies [12, 17] focus on refining and modifying PVD in steganography. The method proposed in the study [17] consisted of applying the neighbouring pixels differencing approach to hide the secret data. The scheme proposed worked on the pixels grouped in triplets and performed the differencing using overlaps to improve the quality of the stego image. In addition to that, the method proposed in the study of Ren et al. [12] combines PVO and difference expansion (DE) to enhance a digital image's embedding capacity and the number of embeddable areas within its pixels. Their experimental results reveal a substantial improvement in embedding capacity and the maximum number of embeddable regions within the utilized images, underscoring the efficacy of this innovative approach. Unlike the previously proposed method, it is worth noting that this approach consisted of not using the neighbouring pixels in an image's initial setup but working on the pixels arranged in ascending order. The differencing operation has been performed on the successive pixels based on their magnitude. Though the previously proposed methods, in line with the PVD, achieved promising results, it is crucial to suggest that combining this with operations like the preprocessing of the pixels in one way or another may improve the results of this steganographic paradigm.

In line with addressing the general challenge of steganography in images, Grajeda-Marín et al. [18] proposed a tri-way Pixel-Value Differencing method, aiming to identify optimal pixel values for computed pixel blocks. This strategic approach ensures that the difference between pixel values accommodates the maximum input data without causing overflow or underflow, thereby improving the robustness and reliability of digital image steganography using Pixel-Value Differencing techniques. In the evolving landscape of steganography, edge-based techniques gain recognition for enhancing imperceptibility and minimizing visual distortion [19, 20]. The edge detection method identified in the study of Djemame and Fichouche [19] used the cellular automata (CA), which showed simplicity and outperformance over the previously proposed method based on the outer totalistic CA. Their results in edge detection have been benchmarked to state-of-the-art approaches such as Scaharr, Canny, Robert, and Sobel. Théophile et al. [20] introduced a novel algorithm to detect the edges of a digital image used for a steganographic

application utilizing fuzzy logic to identify the edge and background. The secret data have been embedded into pixels with low edge attachment values. Experimental results indicated that the suggested approach outperformed current schemes regarding PSNR and payload size, emphasizing the potential of fuzzy logic in efficient information concealment. It is crucial to note that edge detection has shown promising applicability in exploring the atomic components in digital images, as demonstrated in the literature [21, 22] for different steganalysis applications.

Moreover, exploring various steganography methods continues in pursuit of superior results. Models based on Generative Adversarial Networks (GANs), such as CycleGAN and DCGAN, have been investigated by Kuyoro et al. [23]. The researchers in this work have contrasted the performance of the steganographic models, with CycleGAN exhibiting superior results in terms of payload capacity quantified in the bit per pixel (BPP), the similarity between the cover and the stego image evaluated using the structural similarity index metric (SSIM), and quality of the stego image evaluated using the PSNR during the encoding stage. AbdAl-Hameed et al. [24] introduced a double-density dual-tree wavelet transform (DDDT-DWT) based method for a steganographic application. The experimental results of this work showcased improved PSNR for the stego image compared to conventional methods.

Drawing upon insights from established methodologies from state-of-the-art steganographic works, this research proposes an innovative scheme with significant advancements in the field. The proposed approach intricately involves the systematic use of fuzzy logic to identify the key for robust data concealment and the strategic utilization of difference expansion to embed confidential data discreetly. The motivation behind this work stems from the limitations observed in existing methods: constrained payload capacity and suboptimal quality of stego images when the payload is increased. This research addresses these shortcomings by improving the payload capacity, enhancing the structural similarity, and optimizing the peak signal-to-noise ratio of the stego images. The focal point of the proposed method is the substantial improvement of stego image quality when a payload is largely increased, elevating it beyond current standards. In essence, the proposed methodology builds upon the foundation laid by existing approaches and pioneers a fresh perspective that tackles shortcomings head-on. Through the amalgamation of images, edges are used for the security of confidential data, difference expansion, and customized concealment strategies; this work not only addresses deficiencies in prior works but also offers a robust framework with broadened capabilities for concealing substantial volumes of confidential information.

3. PROPOSED METHODOLOGY

This research proposes a steganographic scheme based on fuzzy logic and modulo operation. Referring to the work [25], the proposed method uses a fuzzy logic-based edge detection method within images from the common dataset used in steganographic applications known as SIPI [26]. The edges detected work as keys to enhancing security in the embedding algorithm by incorporating the modulus four operator and yielding an improved payload capacity. Figures 2 and 3 show the flowchart for embedding and extracting secret data using the proposed method. The procedures for embedding and extracting secret data and fuzzy logic edge detection below illustrate how this suggested scheme works.

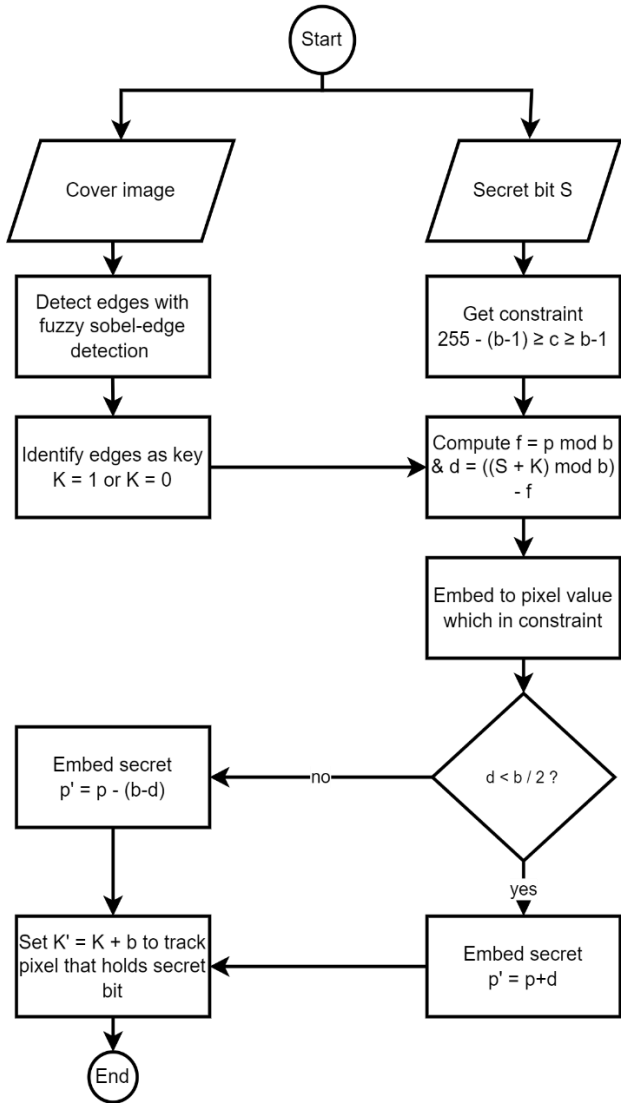

Figure 2. Secret data embedding flowchart

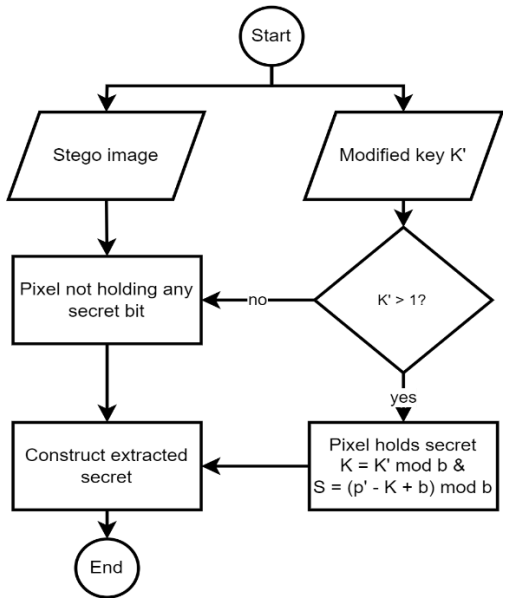

Figure 3. Secret data extraction flowchart

From an information theory perspective, embedding data in edge regions is more conducive to increasing payload and reducing distortion because edges are areas of high contrast and complexity [21, 27]. This complexity masks the presence of embedded data more effectively, leading to lower perceptual visibility and reducing the risk of detection. Additionally, edge regions can tolerate more significant changes without noticeable visual degradation, allowing for a higher payload without compromising image quality [8].

From a number theory perspective, modulo operations enhance the security of the steganographic process by distributing the embedded data across the image in a pseudo-random manner [5]. This randomness makes it more difficult for attackers to detect and extract the hidden information. Modulo operations also ensure that pixel values remain within acceptable ranges, preventing overflow and underflow issues that could degrade the image quality and reveal the presence of hidden data [28]. This controlled randomness, coupled with the innate characteristics of edge regions, creates a robust framework for data concealment.

3.1 Fuzzy-based edge detection in the cover image

The first step in the proposed method is to detect the edges of the cover image using the fuzzy logic algorithm to get the edges and non-edge (background) area. These edges and background areas are then used as a key to perform secure secret bits embedding in the cover image. Therefore, the complete edge detection method is explained throughout the following processes.

1) Load the grayscale image and iterate through its pixels.

2) Calculate the x-axis gradient (Gx) and the y-axis (Gy) by applying a 3 × 3 Prewitt gradient operator kernel. The relations in (1) and (2) show the mathematical computation of the kernels along the x and y axes, respectively. Eqs. (3) and (4) denote the calculation of the gradients along the x-axis and the gradient along the y-axis, respectively. The gradients are then used as the fuzzy inference inputs to output the cover image's edges and background areas.

$$kernelx = \begin{matrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{matrix} \quad (1)$$

$$kernely = \begin{matrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{matrix} \quad (2)$$

$$gx = \sum_{i=1}^{i=3} \sum_{j=1}^{j=3} kernelx_{i,j} \times f_{x+i-2,y+j-2} \quad (3)$$

$$gy = \sum_{i=1}^{i=3} \sum_{j=1}^{j=3} kernely_{i,j} \times f_{x+i-2,y+j-2} \quad (4)$$

3) Fuzzify the two gradients serving as inputs using the Gaussian membership functions, which are then granulated into three variables: LowG(x) using (5), for low gradient values using, MiddleG(x) using (6), for middle gradient values, and HighG(x) using (7) for high gradient values along x-axis and LowG(y) using (8) for low gradient values, MiddleG(y) using (9) for middle gradient values, and HighG(y) using (10) for high gradient values along y-axis. Use Eqs. (5)-(10) to get the inputs' membership degree.

$$\mu LowG(x) = \exp\left(-0.5\left(\frac{x-0}{219.5}\right)^2\right) \quad (5)$$

$$\mu MiddleG(x) = \exp\left(-0.5\left(\frac{x-219.5}{219.5}\right)^2\right) \quad (6)$$

$$\mu HighG(x) = \exp\left(-0.5\left(\frac{x-878}{219.5}\right)^2\right) \quad (7)$$

$$\mu LowG(y) = \exp\left(-0.5\left(\frac{y-0}{208.5}\right)^2\right) \quad (8)$$

$$\mu MiddleG(y) = \exp\left(-0.5\left(\frac{y-208.5}{208.5}\right)^2\right) \quad (9)$$

$$\mu HighG(y) = \exp\left(-0.5\left(\frac{y-834}{208.5}\right)^2\right) \quad (10)$$

4) Infer the edges' and non-edges' output based on the fuzzy rules shown in Table 1.

5) Defuzzify the output to get the edges and background values, represented as ones for the edges and zeros for the non-edges.

Table 1. Fuzzy rules for edge detection

Inputs			Output
Gx	**Operator**	**Gy**	
HighGx	Or	HighGy	Edge
MiddleGx	Or	MiddleGy	Edge
LowGx	And	LowGy	Non-edge

The output of this edge detection step with fuzzy logic is a crucial matrix the same size as the cover image. This matrix holds the value of ones and zeros to be used as a key for the embedding algorithm. This key will ensure that the secret data is securely embedded in the cover image.

3.2 Embedding the secret data

The embedding algorithm is one of the essential steps in steganography. The quality of the steganography scheme itself lies in how good and efficient the embedding algorithm is. Therefore, the following steps detail the embedding process for the proposed approach.

1) Convert the secret bits into base four of the numbering system. Let S, the secret data, be in base four.

2) Iterate through the cover image pixels (p) and only consider the pixels satisfying the condition in Eq. (11) after data embedding to avoid overflow and underflow.

$$base_{four} - 1 \leq p \leq 255 - (base\_four - 1) \quad (11)$$

3) Apply key (K) from the key matrix obtained through the edge detection to the secret bit S using the formula in Eq. (12).

$$S' = (S + K)\ mod\ b \quad (12)$$

4) Compute the function (f) from the modulus function from the p with the base in which the secret data are represented, here base four, using Eq. (13).

$$f = p \; mod \; 4 \tag{13}$$

5) Get the difference (d) between the modified secret bit (S') and the function f using Eq. (14).

$$d = S - f \tag{14}$$

6) Now calculate the stego pixel p' using Eq. (15). To prevent the cover pixel from being increased too high, which can affect the stego image quality, the calculation of the stego pixel is adjusted to be decreased instead of increased if the d is more than the base number divided by 2.

$$P' = \begin{cases} p + d & if \; d < b/2 \\ p - (b - d) & otherwise \end{cases} \tag{15}$$

7) To trace the locations of the stego pixels holding the secret data, we modify the values in the key matrix using Eq. (16) by adding four, the base number, to the key for the secret data position.

$$K' = K + b \tag{16}$$

3.3 Extracting the secret data

To recover the secret data concealed in the stego image, the proposed method utilizes the modified key matrix to get the information on which pixels hold the secret data. The detailed algorithm is explained in the steps below:

1) Iterate through the stego image pixels and check from the key matrix if the i^{th} position key value is more than 1 to confirm that the pixel at that position hosts the secret data.

2) Compute the secret data based on the relation in Eq. (17) and modulus four operations.

$$S = (P' - K + b) \; mod \; 4 \tag{17}$$

3) Compute the pixels of the cover image by subtracting the secret bits from the stego image's pixel values. Finally, the cover-obtained pixel values are used to build the original cover image for data embedding.

4. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental results and discusses the study's conducted experiment in a two-part structure. Firstly, we detail the experiment setting, elucidating the chosen dataset and methodology used to derive performance metrics for the proposed method. This comprehensive description aims to offer a clear understanding of the experimental conditions. Subsequently, in the results and discussion segment, we thoroughly evaluate the proposed method, scrutinizing its effectiveness and comparing it with an alternative steganography technique. This comparative analysis enhances our insights into the proposed method's strengths and limitations within the broader context of steganographic approaches.

4.1 Experimental setup

The conducted experiments in this research utilized publicly available images, sourced explicitly from the USC-SIPI image dataset [26], featuring airplanes, baboons, boats, lakes, and peppers. To evaluate the quality of the embedding algorithm, a payload dataset ranging from 1 to 100 kb in size was employed from the public database [29], with secret data payloads presented in base four formats. Figure 4 visually represents sample images from the considered dataset in this work. All images maintained a standardized size of 512 × 512 pixels and were presented in grayscale. Moreover, this research compares with a previously proposed approach in the preceding study to evaluate the proposed method's performance. The PSNR obtained using Eq. (18), depending on the results of Eq. (19), an evaluation metric used to assess how well a signal or image is compared to another, is particularly used in this work to determine the ratio of the strongest signal to the strongest noise in an image. The PSNR value represents the quality of the images generated by the algorithm about a reference image; a greater PSNR number denotes higher stego image quality.

$$PSNR = 10log_{10}\frac{(255)^2}{MSE} \tag{18}$$

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(A(i,j) - B(i,j))^2 \tag{19}$$

4.2 Results discussion

The experimental results of the proposed method and the existing method used for benchmarking our scheme are recorded in Table 2. It is essential to highlight that methods focusing on different steganography techniques, such as Reduced Difference Expansion (RDE), Difference Expansion and Modulus Function, and Pixel-Value-Ordering, are also compared, in addition to methods using a similar steganography scheme. The results demonstrate that, for the majority of the images and payloads used, the proposed approach yields higher overall PSNR values with an average of 72.24 dB for 1 Kb payload, 62.3 dB for 10 Kb, 59.31 dB for 20 Kb, 57.526 dB for 30 Kb, 56.26 dB for 40 Kb, 55.31 Kb for 50 Kb, and 52.304 dB for 100 Kb. This demonstrates the proposed scheme's outperformance over several alternative steganography methodologies in the state-of-the-art. We can infer that this study's proposed approach can potentially improve the stego image quality based on the PSNR results. Figure 5 depicts the graphic of the proposed method PSNR with different secret payload sizes among the images used.

Figure 4. Dataset images [26] (a) Airplane, (b) Baboon, (c) Boat, (d) Lake, and (e) Pepper

Table 2. Results of comparing the PSNR values between the proposed methodology and the existing methods

Payload (in kb)	Cover Image	PSNR (dB)			
		Method [27]	Method in the Study [30]	Method in the Study [31]	Proposed Method
1	Airplane	-	-	-	72.26
	Baboon	54.38	-	-	72.11
	Boat	66.08	-	-	71.85
	Lake	-	-	-	72.23
	Pepper	66.26	-	-	72.78
10	Airplane	-	64.09	64.18	62.28
	Baboon	45.81	54.75	55.45	62.35
	Boat	54.70	58.83	59.11	62.17
	Lake	-	60.53	60.42	62.41
	Pepper	55.64	-	-	62.31
20	Airplane	-	60.42	60.40	59.24
	Baboon	43.45	56.54	56.84	59.37
	Boat	50.64	54.30	54.74	59.29
	Lake	-	55.36	55.52	59.33
	Pepper	51.82	-	-	59.41
30	Airplane	-	58.31	58.52	57.59
	Baboon	48.63	53.12	53.70	57.51
	Boat	49.72	53.63	54.02	57.43
	Lake	-	52.38	53.11	57.55
	Pepper	49.72	-	-	57.54
40	Airplane	-	58.31	56.72	56.31
	Baboon	41.92	53.12	52.42	56.26
	Boat	46.63	54.02	52.99	56.18
	Lake	-	53.11	52.51	56.30
	Pepper	48.33	-	-	56.30
50	Airplane	-	54.96	54.96	55.33
	Baboon	40.81	51.64	51.64	55.30
	Boat	44.93	52.23	52.23	55.22
	Lake	-	51.73	51.73	55.34
	Pepper	47.31	-	-	55.34
100	Airplane	-	48.59	48.59	52.34
	Baboon	-	44.56	44.56	52.34
	Boat	-	44.89	44.89	52.21
	Lake	-	44.68	44.68	52.32
	Pepper	-	-	-	52.34

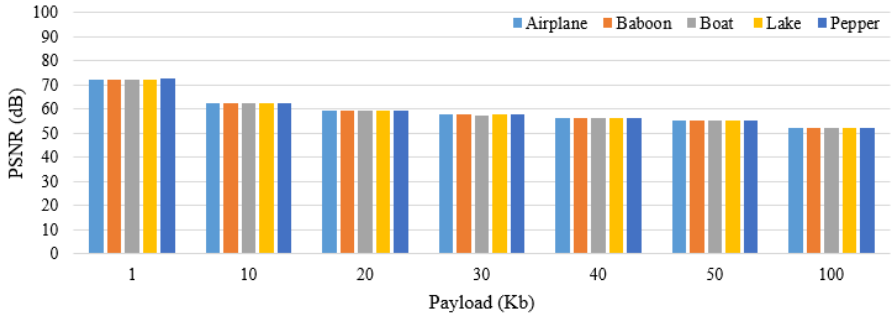

Figure 5. Graph of proposed method PSNR vs. Payload size in different images

A further comparison is made concerning embedding or payload capacity. In steganography, embedding capacity refers to the secret data hidden within a cover image. Table 3 compares the proposed method and several other methods about the embedding capacity. It can be seen that the proposed method achieves a better result in terms of payload capacity compared to some existing approaches, with the values reaching 262144 pixels for the airplane image, 262074 pixels for the Baboon image, 262121 for the Boat image, and 262133 pixels for the Lake image. Table 3 provides a detailed comparison of the embedding capacity between the proposed method and three existing methods [27, 30, 31]. The embedding capacity is measured by the number of bits effectively hidden within each cover image. For the 'Airplane' cover image, the proposed method outperforms all others, offering a significant increase in embedding capacity with 262,144 bits compared to 60,054 [30], 82,701 [31], and 131,072 [27].

Similarly, for 'Baboon,' 'Boat,' and 'Lake' cover images, the proposed method consistently demonstrates superior embedding capacity, showcasing advancements over the other methods. This comprehensive comparison underscores the efficacy of the proposed approach in maximizing the concealment of information within diverse cover images, thereby highlighting its potential for enhanced steganographic applications. The increased embedding capacity across different image types positions the proposed method as a promising solution in the field. Figure 6 visually highlights the comparison of our method to the existing ones. It is worth noting that the proposed method exceeds the embedding capacity of previous methods due to its flexibility in selecting the embeddable pixels on the cover image.

Table 3. Comparison of the embedding capacity between the proposed and the existing methods

Cover Image	Embedding Capacity			
	Method in the Study [30]	Method in the Study [31]	Method in the Study [27]	Proposed Method
Airplane	60054	82701	131072	262144
Baboon	12416	17582	131009	262074
Boat	25782	34059	131021	262121
Lake	26163	36098	131046	262133

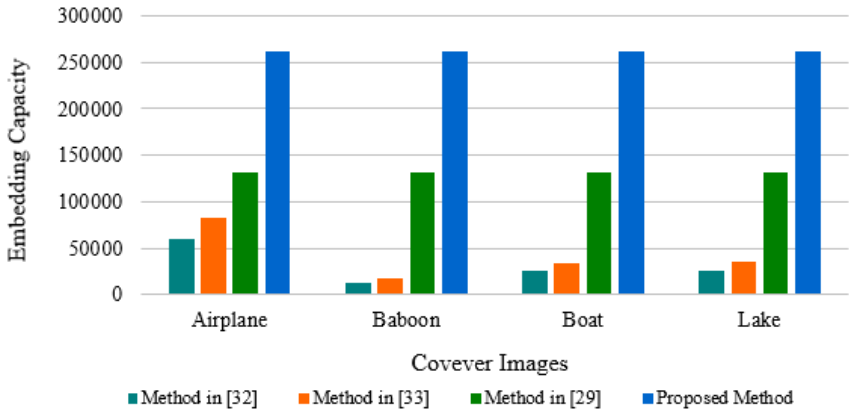

Figure 6. Embedding capacity comparison

The comparative analysis between the cover image (Figure 7(a)) and the stego image embedded with a 100kb payload (Figure 7(b)) further confirms the imperceptibility of differences introduced by the proposed steganographic method. As depicted in Figure 7, the human eye cannot discern the stego image from the original cover image, even under scrutiny. This visual similarity ensures that the stego image remains inconspicuous, concealing the hidden data without drawing attention. These results validate the proposed steganographic scheme's robustness and efficiency in preserving the cover image's visual integrity while embedding significant secret information.

Figure 7. Comparison between cover image (a) and stego image (b)

Figure 8. Sample images used from BOSSBase 1. 01

To verify the robustness and universality of the Proposed algorithm, we conduct an additional experiment using various images. To prove its robustness, we chose images of different types of Break Our Steganographic System (BOSSBase) Version 1 [32]. Figure 8 illustrates the sample images from the BOSSBase, and the results obtained are recorded in Table 4. The results in Table 4 identify that the Proposed algorithm shows promising robustness and ability to maintain image quality while concealing information within images of varying complexity.

Table 4. PSNR results of the algorithm's robustness verification using various images from BOSSBase 1. 01

Payload (in kb)	Cover Image	PSNR in (dB)
10	Image_1	56.36
	Image_2	56.19
	Image_3	56.31
	Image_4	56.27
20	Image_1	53.24
	Image_2	53.24
	Image_3	53.10
	Image_4	53.21
30	Image_1	51.52
	Image_2	51.43
	Image_3	51.48
	Image_4	51.48
40	Image_1	50.25
	Image_2	50.26
	Image_3	50.21
	Image_4	50.23
50	Image_1	49.28
	Image_2	49.29
	Image_3	49.28
	Image_4	49.28

To highlight the Proposed algorithm's practicality in information security, this research also conducts steganalysis attacks using the adaptive steganalysis models [21, 33]. To generate the stego images, we use the Proposed steganographic algorithm with a payload capacity of 50 kb and 100 kb. It is important to note that the stego images pass one or all of the common attack operations (cropping, compression) before training for strong attaching results. The

data in Table 5 show promising resistance to the proposed algorithm because, in all cases, the detection accuracy is always less than 50%. The highest detection accuracy with the preprocessed images, considered a strong steganalysis attack, is only 42.83 %. That justifies the robustness of the Proposed method against attacks.

Table 5. Detection accuracy in percentage (%) of the proposed method by steganalysis attacks

Staganalysis Method (Attaching Algorithm)	Payload Capacity of 50 kb	Payload Capacity of 100 kb
Algorithm in the study [33]	25.21	36.44
Algorithm in the study [21]	32.51	42.83

5. CONCLUSIONS

In recent years, there has been a notable surge in the development of data-hiding techniques to safeguard confidential information by seamlessly integrating it into multimedia objects. Paramount among these considerations are embedding capacity and the degree of similarity between the original cover and resulting stego images. In response to these challenges, this study presents a novel steganography approach prioritizing high capacity and robust security. This is achieved by applying fuzzy logic-based edge detection and modulo operation. The experimental findings underscore the effectiveness of the proposed method, surpassing previous approaches in terms of both embedding capacity and resultant image quality. Specifically, the scheme demonstrates a noteworthy 15% improvement in PSNR alongside a substantial 20% increase in embedding capacity. However, it is essential to acknowledge certain limitations inherent in the current methodology. These include potential susceptibilities to advanced steganalysis techniques and the need for further processing time optimization. Addressing these limitations is critical for the continued advancement and applicability of the proposed approach.

Future research endeavours could focus on developing adaptive algorithms capable of dynamically adjusting embedding parameters based on the unique characteristics of the cover image. Moreover, exploring the integration of machine learning techniques holds promise in enhancing detection capabilities and fortifying resistance against evolving threats in steganography. By pursuing these avenues, we can further bolster the efficacy and resilience of data-hiding methods in safeguarding sensitive information within multimedia contexts.

ACKNOWLEDGEMENTS

The authors sincerely thank the NCC Laboratory, the Department of Informatics at the Sepuluh Nopember Institute of Technology, and all research group members for their invaluable support and contributions.

REFERENCES

[1] Executive Edition: Mandiant M-Trends. (2024). M-Trends 2024 special report executive edition. https://services.google.com/fh/files/misc/m-trends-2024-executive-edition.pdf.

[2] Song, B., Wei, P., Wu, S., Lin, Y., Zhou, W. (2024). A survey on Deep-Learning-based image steganography. Expert Systems with Applications, 254: 124390. https://doi.org/10.1016/j.eswa.2024.124390

[3] Setiadi, D.R.I.M., Rustad, S., Andono, P.N., Shidik, G.F. (2023). Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Processing, 206: 108908. https://doi.org/10.1016/j.sigpro.2022.108908

[4] Kosuru, S.D., Pradhan, A., Basith, K.A., Sonar, R., Swain, G. (2023). Digital image steganography with error correction on extracted data. IEEE Access, 11: 80945-80957. https://doi.org/10.1109/ACCESS.2023.3300918

[5] Hassan, F.S., Gutub, A. (2022). Improving data hiding within color images using hue component of HSV color space. CAAI Transactions on Intelligence Technology, 7(1): 56-68. https://doi.org/10.1049/cit2.12053

[6] Khan, M., Rasheed, A. (2023). A high-capacity and robust steganography algorithm for quantum images. Chinese Journal of Physics, 85: 89-103. https://doi.org/10.1016/j.cjph.2023.06.016

[7] Akhtar, N., Johri, P., Khan, S. (2013). Enhancing the security and quality of LSB based image steganography. In 2013 5th International Conference and Computational Intelligence and Communication Networks, Mathura, India, pp. 385-390. https://doi.org/10.1109/CICN.2013.85

[8] Haq, T.I., Mafazy, M.M., Agustinus, J.T., de La Croix, N.J., Ahmad, T. (2023). Sobel edges key-based method for steganography in spatial domain images. In 2023 3rd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, India, pp. 1-5. https://doi.org/10.1109/ICMNWC60182.2023.10435975

[9] Karakus, S., Avci, E. (2020). A new image steganography method with optimum pixel similarity for data hiding in medical images. Medical hypotheses, 139: 109691. https://doi.org/10.1016/j.mehy.2020.109691

[10] Chen, C.C., Chang, C.C., Chen, K. (2021). High-capacity reversible data hiding in encrypted image based on Huffman coding and differences of high nibbles of pixels. Journal of Visual Communication and Image Representation, 76: 103060. https://doi.org/10.1016/j.jvcir.2021.103060

[11] Rustad, S., Syukur, A., Andono, P.N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. Journal of King Saud University-Computer and Information Sciences, 34(6): 3559-3568. https://doi.org/10.1016/j.jksuci.2020.12.017

[12] Ren, F., Hao, Y., Pang, K., Wu, Z. (2023). Reversible data hiding scheme in encrypted images based on homomorphic encryption and pixel value ordering. Multimedia Tools and Application, 83: 40607-40627. https://doi.org/10.1007/s11042-023-17242-4

[13] Shukla, A.K., Singh, A., Singh, B., Kumar, A. (2018). A secure and high-capacity data-hiding method using compression, encryption and optimized pixel value differencing. IEEE Access, 6: 51130-51139. https://doi.org/10.1109/ACCESS.2018.2868192

[14] Yang, C.Y., Wang, W.F. (2020). Progressive data hiding in integer wavelet transform of electrocardiogram by

using simple decision rule and coefficient calibration. Revue d'Intelligence Artificielle, 34(1): 11-20. https://doi.org/10.18280/ria.340102

[15] Sahu, A.K., Swain, G. (2019). Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis. International Journal of Electronic Security and Digital Forensics, 11(4): 458-476. https://doi.org/10.1504/IJESDF.2019.102567

[16] Zhang, Z., Cao, Y., Jahanshahi, H., Mou, J. (2023). Chaotic color multi-image compression-encryption/LSB data type steganography scheme for NFT transaction security. Journal of King Saud University-Computer and Information Sciences, 35(10): 101839. https://doi.org/10.1016/j.jksuci.2023.101839

[17] Fahim, A., Raslan, Y. (2023). Optimized steganography techniques based on PVDS and genetic algorithm. Alexandria Engineering Journal, 85: 245-260. https://doi.org/10.1016/j.aej.2023.11.013

[18] Grajeda-Marín, I.R., Montes-Venegas, H.A., Marcial-Romero, J.R., Hernandez-Servin, J.A., De Ita, G. (2016). An optimization approach to the TWPVD method for digital image steganography. In Pattern Recognition: 8th Mexican Conference, MCPR 2016, Guanajuato, Mexico, pp. 125-134. https://doi.org/10.1007/978-3-319-39393-3_13

[19] Djemame, S., Fichouche, S. (2022). A novel edge detection algorithm based on outer totalistic cellular automata. Revue d'Intelligence Artificielle, 36(1): 19-30. https://doi.org/10.18280/ria.360103

[20] Théophile, I., De La Croix, N.J., Ahmad, T. (2023). Fuzzy logic-based steganographic scheme for high payload capacity with high imperceptibility. In 2023 11th International Symposium on Digital Forensics and Security (ISDFS), Chattanooga, TN, USA, pp. 1-6. https://doi.org/10.1109/ISDFS58141.2023.10131727

[21] De La Croix, N.J., Ahmad, T., Han, F. (2023). Enhancing secret data detection using convolutional neural networks with fuzzy edge detection. IEEE Access, 11: 131001-131016. https://doi.org/10.1109/ACCESS.2023.3334650

[22] Navdeep, Singh, V., Rani, A., Goyal, S. (2020). An improved hyper smoothing function based edge detection algorithm for noisy images. Journal of Intelligent & Fuzzy Systems, 38(5): 6325-6335. https://doi.org/10.3233/JIFS-179713

[23] Kuyoro, A., Nzenwata, U.J., Awodele, O., Idowu, S. (2022). GAN-based encoding model for reversible image steganography. Revue d'Intelligence Artificielle, 36(4): 561-567. https://doi.org/10.18280/ria.360407

[24] AbdAl-Hameed, S.A., Abdullah, H.N., Khalf, N.H., Alghazo, J.M. (2023). An enhanced steganography approach for concealing audio in images using double density-dual tree wavelet transform. Revue d'Intelligence Artificielle, 37(5): 1237-1244. https://doi.org/10.18280/ria.370516

[25] Torres, C., Gonzalez, C.I., Martinez, G.E. (2022). Fuzzy edge-detection as a preprocessing layer in deep neural networks for guitar classification. Sensors, 22(15): 5892. https://doi.org/10.3390/s22155892

[26] Signal and Image Processing Institute, Ming Hsieh Department of Electrical and Computer Engineering. The USC-SIPI image database. https://sipi.usc.edu/database/database.php?volume=mis, accessed on Oct. 9, 2024.

[27] De La Croix, N.J., Islamy, C.C., Ahmad, T. (2022). Secret message protection using fuzzy logic and difference expansion in digital images. In 2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON), Lagos, Nigeria, pp. 1-5. https://doi.org/10.1109/NIGERCON54645.2022.9803151

[28] Sahu, A.K., Swain, G. (2019). An optimal information hiding approach based on pixel value differencing and modulus function. Wireless Personal Communications, 108: 159-174. https://doi.org/10.1007/s11277-019-06393-z

[29] Lorem Ipsum. The Standard Lorem Ipsum Passage. https://www.lipsum.com/.

[30] Ding, W., Zhang, H., Reulke, R., Wang, Y. (2022). Reversible image data hiding based on scalable difference expansion. Pattern Recognition Letters, 159: 116-124. https://doi.org/10.1016/j.patrec.2022.05.014

[31] Chang, J., Ding, F., Li, X., Zhu, G. (2021). Hybrid prediction-based pixel-value-ordering method for reversible data hiding. Journal of Visual Communication and Image Representation, 77: 103097. https://doi.org/10.1016/j.jvcir.2021.103097

[32] Bas, P., Filler, T., Pevný, T. (2011). "Break our steganographic system": The ins and outs of organizing BOSS. In International Workshop on Information Hiding, pp. 59-70. https://doi.org/10.1007/978-3-642-24178-9_5

[33] Ntivuguruzwa, J.D.L.C., Ahmad, T. (2023). A convolutional neural network to detect possible hidden data in spatial domain images. Cybersecurity, 6(1): 23. https://doi.org/10.1186/s42400-023-00156-x