Received: September 14, 2024. Revised: October 24, 2024.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

DualLSBStego: Enhanced Steganographic Model Using Dual-LSB in Spatial Domain Images

Aria Nalini Farzana[1] **Ntivuguruzwa Jean De La Croix**[1,2] **Tohari Ahmad**[1]*

[1]*Department of Informatics, Institut Teknologi Sepuluh Nopember, Surabaya 60111, Indonesia*
[2]*College of Science and Technology, University of Rwanda, Kigali 3900, Rwanda*
* Corresponding author's Email: tohari@its.ac.id

Abstract: In the age of information technology, the secure transmission of sensitive data over public networks is essential. Steganography, a data-hiding technique, is used to transmit information covertly between parties. However, many existing algorithms face a significant challenge: balancing payload size with the quality of the stego image. This article presents a new steganographic framework, DualLSBStego, using Dual-LSB in spatial domain images to address this issue. The DualLSBStego adaptively selects the two least significant pixel bits to hide secret data, enhancing the tradeoff between capacity and image quality. Experimental results on standard datasets in steganography of digital images, SIPI images datasets, show that the DualLSBStego achieves a Peak Signal-to-Noise Ratio (PSNR) of up to 79.64 decibels (dB) with an Airplane cover image at a payload size of 1 kilobit (kb). The DualLSBStego model's performance was compared to recent Difference Expansion (DE) techniques, achieving a Structural Similarity Index Measure (SSIM) of 1, which indicates a high-quality stego image.

Keywords: Network infrastructure, Image steganography, Information security, Spatial domain images, Image pixels.

Nomenclature

bin2dec	Binary to Decimal
bpp	Bit per pixel
C	Cover
Concat	Concatenation operation
dB	Decibel
dec2bin	Decimal to binary
Ip	Image Pixel
kb	Kilobit
LSB	Least significant bit
MSE	Mean squared error
PSNR	Peak signal-signal-to-noise ratio
PVD	Pixel value differencing
SSIM	Structural similarity index measure

1. Introduction

In recent decades, the rapid advancement of information technology and the internet has caused an exponential increase in the volume of data transmitted across publicly used networks [1, 2]. The rise of the data that needs to be transmitted over the vulnerable shared data transmission medium, the internet, resulted in the need to secure the data to prevent any unwanted access by any third party [3]. Cryptography is a prevalent approach for mitigating these concerns by safeguarding sensitive information from unauthorized access [4]. However, the ciphertext produced by conventional encryption algorithms often appears as an unintelligible sequence of bits, lacking semantic value and potentially drawing the scrutiny of adversaries. This perceptibility can inadvertently attract malicious actors, undermining the encrypted data's intended security. Steganography, a sister paradigm to cryptography, has emerged as a powerful tool for covert communication by concealing the secret bits from confidential messages in the content of digital objects [5-7]. The commonly used digital objects in carrying the secret bits are the texts [8], videos [9], Audio [10], and images [11]. Unlike cryptography, steganography aims to conceal the very existence of the message in the cover object with high imperceptibility of their existence, permitting their

transmission in plain sight without any Human Vision system-based detection.

Steganography has seen significant advancements as the demand for secure communication grows in the current developing digital world [12-14]. Traditional steganographic methods, while effective, often face challenges in balancing security, which is mainly evaluated based on the perceptibility of the secret data existence, the concealable secret data capacity, and steganographic robustness [5]. Several steganographic approaches have been proposed to mitigate the problems of steganography, improving the data imperceptibility [15, 16], which is supposed to be quantified by an envisaged high Peak Signal-to-Noise Ratio (PSNR) and enhancing the cover images' capacity to host the secret bits in unnoticed fashion [17-19] when nagAs detection techniques become more sophisticated, there is a growing need for innovative approaches that enhance the stealth and effectiveness of hidden communication [20].

Although significant advancements in addressing cover image distortion under high payload conditions, steganography in digital images still faces critical challenges that need to be addressed. One of the primary limitations is the insufficient embeddability of cover images, which restricts the practical application of steganographic techniques in real-world scenarios. Real-life applications often require robust systems capable of securely hiding secret data without compromising the quality or integrity of the cover image. To meet these demands, there is a pressing need to enhance steganographic methods to improve their effectiveness and resilience.

This article introduces a novel steganography approach, DualLSBStego, designed to enhance payload capacity while ensuring optimal stego image quality with a PSNR that outperforms existing techniques. DualLSBStego employs a dynamic embedding algorithm based on an advanced pixel transformation model, enabling more efficient and secure data concealment. Refining the process of embedding secret bits into the cover image significantly increases imperceptibility, making the concealed data less detectable to unauthorized parties. The novelty of the proposed DualLSBStego method lies in its adaptive, intensity-based embedding strategy, which improves payload capacity without compromising image quality. The technique significantly increases the payload by dynamically selecting embedding areas based on pixel intensity and utilizing two least significant bits (LSBs) for data concealment in low-intensity pixels. Additionally, it enhances imperceptibility by embedding data subtly in medium- and high-intensity pixels, achieving a superior tradeoff between payload, security, and image quality compared to existing techniques. The contributions of the proposed DualLSBStego that collectively advance the state-of-the-art by optimizing the tradeoff between payload, imperceptibility, and robustness are summarized in the following points:

1. *Adaptive Selection of Embedding Areas*: DualLSBStego introduces an adaptive mechanism for selecting embeddable areas within the cover image based on pixel intensity values. By categorizing pixels into low, medium, and high-intensity groups, the method dynamically identifies optimal regions for embedding, enhancing both the payload capacity and security of the steganographic process.
2. *Enhanced Payload Capacity through Dual-LSB Embedding*: The proposed method significantly improves payload capacity by leveraging pixel values' two least significant bits (LSBs) to embed secret data. This approach is intensity-aware; low-intensity pixels use both LSBs for embedding, effectively doubling the payload without significantly affecting image quality.
3. *Improved Imperceptibility via Intensity-Based Adaptive Embedding*: To enhance imperceptibility, DualLSBStego employs a novel adaptive embedding strategy where embedding depth is directly correlated with pixel intensity. Low-intensity pixels embed data in both LSBs, medium-intensity pixels embed in a single LSB, and high-intensity pixels remain unchanged.

The rest of this work is organized into three sections: Section 2 discusses the state-of-the-art, highlighting the gap in the current works that needs to be addressed by the proposed method, DualLSBStego, in Section 3. The results from experimentations and their discussion are given in Section 4, and Section 5 concludes the work.

2. Literature review

The Ancient Greeks are credited with developing steganography around 484-425 BC. A notable example involves Histaeus, the ruler of Miletus, who devised a method to secretly communicate by shaving the head of a trusted enslaved person and tattooing a covert message or symbol on the exposed skin. After the enslaved person's hair grew back, effectively hiding the tattoo, the enslaved person was sent to Aristagoras to deliver the concealed message. Upon arrival, the enslaved person's head was shaved again, revealing the hidden message once more [21].

Since its inception, many experts have developed various techniques, especially in image steganography. These methods have been applied across multiple fields to hide confidential information. The following sections will briefly discuss and critically evaluate several LSB-based image steganography methods.

Rahman et al. (2022) proposed a novel data-hiding technique utilizing LSB substitution to achieve high embedding capacity with minimal distortion [22]. This approach generates four additional pixels from each pixel of the original image. The modified LSB matching method is then applied to conceal the hidden data within these generated pixels. To further reduce perceptual alterations, in [23], another steganographic algorithm based on the adaptiveness of the pixels to improve the embeddability has been proposed to resist the steganalytic attackers with all pixels undergoing additional modifications using pixel value differencing. However, these methods have shown limitations in terms of robustness and security, which could be addressed by implementing dual LSB steganography to enhance data concealment and resistance to steganalysis.

An image steganography technique in the spatial adaptive domain is described, which utilizes LSB replacement in conjunction with the concept of adjacent pixel value differencing [6, 24, 25]. This method employs a 3×3 pixel block structure, using all edge pixels in various ways. The proposed approach comprises three key stages: (i) data encoding via XOR operation, (ii) embedding the encoded bits using Pixel Value Differencing (PVD) alongside LSB substitution, and (iii) the extraction phase. Experimental results in [24] show that this technique achieves a high embedding capacity of approximately 3.498 bits per pixel (bpp) with a PSNR of 38.23 dB. The results from [6] also show promising results in the stego image quality. Generally, the results from these works demonstrate that the choice of cover image dramatically affects the performance of the steganography method. However, an efficient cover image selection strategy could be integrated with the proposed approach to refine further and enhance the results.

Pixel Value Differencing (PVD) is a widely recognized steganographic technique that achieves high embedding capacity by using a range table. However, it remains susceptible to attacks based on histogram steganalysis [26, 27], and [28]. A randomly generated key is often employed to encrypt the secret message bits before embedding them to enhance the security of hidden data. The method proposed in [27] presented an alternative approach that avoids using a range table, instead expanding the cover image by using 2 × 2 non-overlapping pixel blocks. Compared to the established method by Maji et al. (2019) in [26], their technique produced a superior-quality cover image. Nonetheless, both Maji's and Parmar's methods have limitations. Maji's method is vulnerable to histogram analysis, and Parmar's method, which relies on non-overlapping blocks like the method in [28], may limit robustness and capacity. These challenges could be addressed by adopting dual LSB steganography, which might offer improved resistance to steganalysis and enhanced data-hiding capacity through a dual-layer embedding process.

A novel approach to image steganography was proposed in [29] and further explored in [30], where the initial characters of the hidden message are converted into binary bits, followed by the identification of edge regions for data embedding. The method introduced in [29] is distinguished by its use of randomization as a fundamental aspect of the algorithm. Based on the experimental results, this technique robustly embeds hidden data into images by using edge pixels, incorporating randomness, and applying variable mounting parameters, which enhances security against visual and histogram-based attacks. Additionally, efforts have been made to improve image quality and enhance the imperceptibility of the hidden data utilizing a hybrid paradigm from the PVD and modulus function [31]. However, these methods still face vulnerabilities, including susceptibility to advanced statistical and structural steganalysis, potentially compromising the hidden data. These limitations could be mitigated by adopting dual LSB steganography, which offers increased robustness and improved concealment through a dual layer embedding process, thereby enhancing security and data capacity.

The application of LSB-based bit-flipping techniques has been further investigated, building on the findings presented in [32]. This study employs the bit-flipping approach for color images, embedding messages at maximum capacity, and the results demonstrate that the technique performs exceptionally well in digital images. However, despite its strengths, the bit-flipping method has drawbacks, including increased susceptibility to noise and image distortions, which can compromise the hidden data, and its reliance on predictable patterns makes it more vulnerable to detection by advanced steganalysis techniques. The proposed dual LSB steganography method addresses these limitations using a dual layer embedding process that enhances data robustness against noise and distortions. Additionally, by incorporating layers of

randomness and varying embedding depths, dual LSB steganography reduces the predictability of hidden data patterns, significantly improving resistance to detection by sophisticated steganalysis methods.

3. Proposed DualLSBStego

This paper presents a framework named the "DualLSBStego" that considers the two least significant bits of the image's pixels to find the potential positions to embed the secret bits. In DualLSBStego, the pixels are first transformed into binary representations, and then, based on their intensity, they are classified into low, medium, and high intensity. **Algorithm I** contains a detailed pseudocode for the cover preprocessing and pixel classification based on their intensities. The pseudocode outlines an algorithm for converting a payload and a cover image into binary formats, classifying the image pixels by their intensity, and storing the associated key values for further processing. The algorithm begins by loading the payload (P) and the cover image (C). The algorithm classifies the pixels of the cover image based on their intensity values into low, medium, and high-intensity categories. For low-intensity pixels ($0 \leq$ pixel < 100), the key is set to 10; for medium-intensity pixels ($100 \leq$ pixel< 200), the pixel value is taken as it is with a key value of 1 stored in K. If the intensity does not fit these conditions, the key is set to 0, stored in K, and the algorithm exits.

Algorithm I. Pseudocode for the cover preprocessing task

Notation 1: P -> Payload
Notation 2: $\boldsymbol{P_b}$ -> Payload in binary
Notation 3: C -> Cover Image
Notation 4: $\boldsymbol{C_b}$ -> Cover Image in binary
Notation 5: $\boldsymbol{I_p}$ -> Pixel intensity
Notation 6: p -> Pixel
Notation 7: p' -> New pixel
Notation 8: k -> Key
Notation 9: K -> Key file

Input: Payload (P), Cover Image (C)
Output: Cover Image in Binary (C_b) and its pixel classification (Into Low, Medium, and High Intensity)

1: Start
2: Load C and P
3: Convert C into $\boldsymbol{C_b}$
4: If $\mathbf{0} \leq \boldsymbol{I_p} < \mathbf{100}$ *then*
$\boldsymbol{p'} = \boldsymbol{p}[\boldsymbol{Counter}:\boldsymbol{Counter}+\mathbf{1}]$
k = 10, store k in K
else
If $\mathbf{100} \leq \boldsymbol{I_P} < \mathbf{200}$ *then*
$\boldsymbol{p'} = \boldsymbol{p}[\boldsymbol{Counter}]$
k = 1, store k in K
else
k = 0, store k in K
break
end If
6: End.

The next steps of the DualLSBStego consist of embedding and extracting the secret data to the binary-set cover image. Fig. 1 gives a pictorial representation of the stages of the embedding process. The data concealment is done considering the pixel intensity to distinguish which pixels to host two, one, one zero bits of the secret data. The embedding process is validated as a reversible data-hiding method because it makes the hidden data possible to extract.

3.1 Embedding the payload

The data concealment process in the proposed DualLSBStego method consists of three main stages: cover pixel conversion and classification, data embedding, and post-conversion of the stego image. The conversion of the stego image involves transforming the pixel values into their decimal format to match the type of the cover image, ensuring consistency between the stego and cover images.

Stage 1) Cover Image Conversion and pixels classification

In the initial data processing phase, the pixels of the cover image are converted into binary format. This conversion is necessary to align the format with the secret bits initially in binary representation, facilitating the data embedding process. The cover image retains its original dimensions and undergoes the embedding process in its binary state. Before converting to binary, the pixels are classified into low, medium, and high-intensity categories, as described in Algorithm I. This classification aims to determine the optimal payload size for embedding into each pixel, ensuring the best visual quality of the stego image. The binary conversion is performed according to Eq. (1) below.

$$I_{cover}(i,j) = dec2bin(I(i,j),8) \quad (1)$$

Stage 2) Secret Bits Concealment

This approach dynamically employs Dual-LSB's advantages, with the secret bits' capacity determined

by the intensity of each pixel color. In the binary representation, an adaptive selection of the least significant bits is employed to conceal the secret bits. Then, data embedment uses the Concat operator following Eq. (2) for an adaptive fashion of data placement. in the specific context. The embedding paradigm specifies the embedding capacity of a pixel $P(i,j)$ based on its intensity value and set conditions. For pixels with low intensity (L), $0 \leq P(i,j) < 100$ and where a specified condition for the payload availability ($Payload_{length} \leq Payload_{length} - 1$) is met, the embedding capacity is set to 2 bits, and the associated key is '10'. This allows for more data embedding in darker pixels, which are less likely to affect the overall image quality. For pixels with medium intensity (M) $100 \leq P(i,j) < 200$ and where the condition of payload availability is met, the embedding capacity is reduced to 1 bit, with the key '1' used to denote this state. For high-intensity pixel (H)$200 \leq P(i,j) < 255$, no data is embedded, as altering these brighter pixels could more noticeably degrade the image quality. The key '0' is associated with this condition, indicating no data embedding. The number of secret bits to be embedded is determined by the parameters specified in Eq. (2). Depending on these parameters, the binary representation uses two, one, or none of the least significant bits of a pixel, optimizing the embedding capacity while keeping changes visually insignificant. Each iteration generates a key value indicating the number of secret bits embedded in each pixel, which is then used during extraction. This method ensures efficient data embedding without compromising image quality.

$$Bits\_Host\_Capacity = \begin{cases} 2, \ if \ P(i,j) \in L \\ 1, \ if \ P(i,j) \in M \\ 0, \ if \ P(i,j) \in H \end{cases} \quad (2)$$

Step 3) Conversions after data embedding

Following data embedding, the new array of image binary is saved and converted back into decimal format. Eq. (3) defines the conversion process for each pixel in the stego image. Here, $I_{stego}(i,j)$ represents the pixel value at position (i,j) in the stego image, while $I_{Bin}(i,j)$ denotes the corresponding pixel value in binary form. The function $bin2dec$ converts the binary value back into its decimal representation, which is suitable for standard image formats. This operation is performed for all pixels across the image, where i ranges from 1 to the total number of rows, and j ranges from 1 to the total number of columns in the image. This step aims to revert the binary-modified pixel values into a format that can be visually rendered to complete the embedding process.

$$I_{stego}(i,j) = bin2dec\big(I_{Bin}(i,j)\big) \quad (3)$$

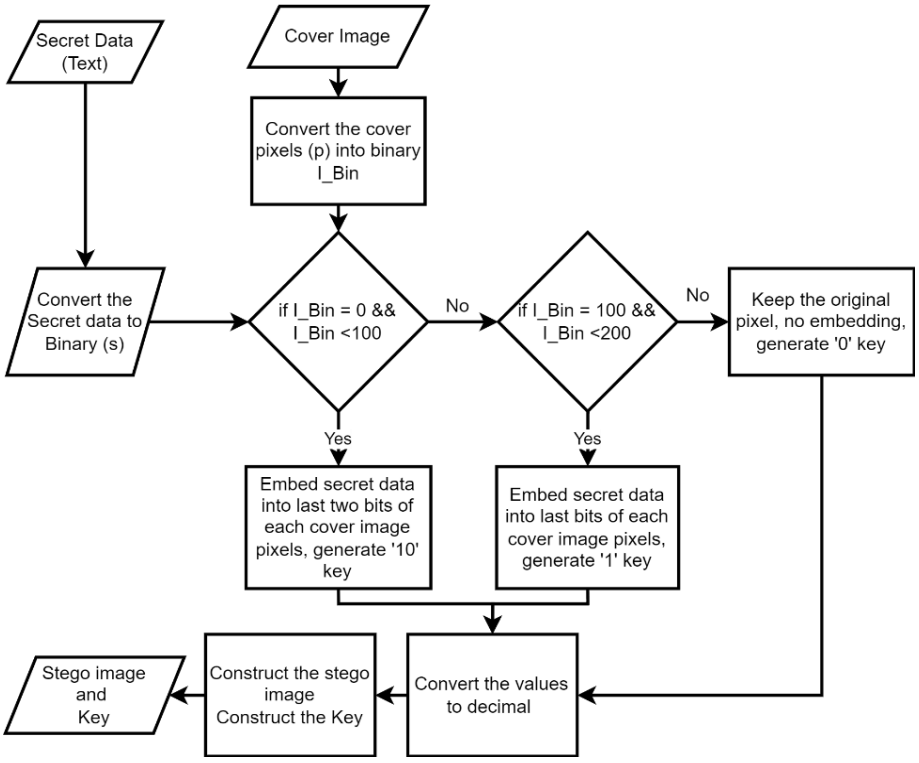


Figure. 1 DualLSBStego Embedding Process

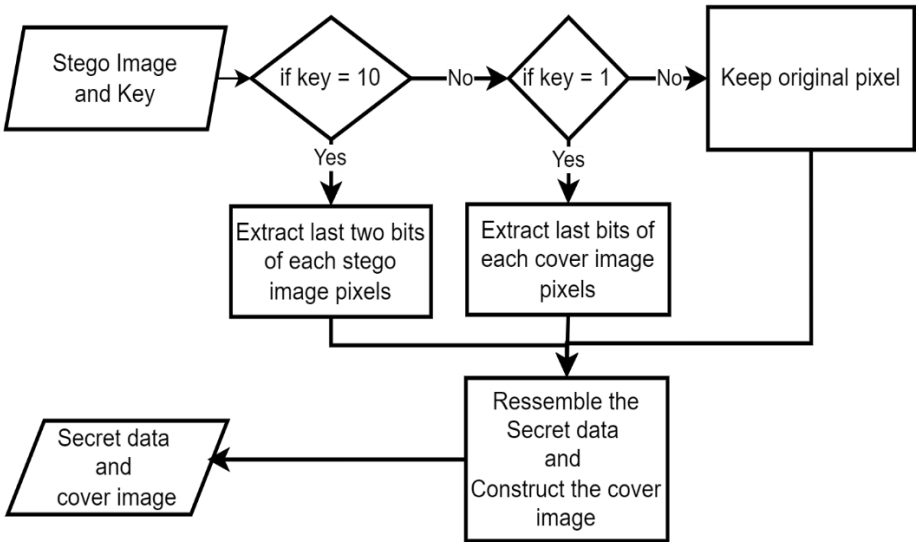


Figure. 2 DualLSBStego the Process to Extract the Cover and Secret Data

3.2 Recovering the secret data and cover image

The extraction process, mirroring the embedding process, consists of three stages. The stego image is converted from its original decimal representation into binary format in the first stage. The second stage follows the steps outlined in Fig. 2, which detail the lossless extraction of the concealed secret data and the original image used as the carrier. In the final stage, the carrier image extracted in stage 2 is converted back to decimal format to match the original format of the cover image. This triplet of stages ensures the accurate retrieval of the embedded data and the original cover image.

Stage 1: Preprocessing the Stego Image

In the initial data processing phase, each pixel of the stego image is converted into an 8-bit binary format using Eq. (4). This step facilitates the extraction process by representing each pixel value in binary form, making it easier to manipulate the embedded data. It is important to note that the stego image maintains its original dimensions and remains in this binary format throughout the extraction procedure.

$$I_{stego}(i,j) = dec2bin(I(i,j),8) \quad (4)$$

Step 2) Extracting the Secret Bits and the Cover Image

The stego image must be processed pixel-by-pixel basis using its binary representation to recover the payload and cover image. Access to a key file is required to determine the number of secret bits embedded in each pixel. The identified bits containing the hidden data are then extracted according to the procedure detailed in Fig. 2 and stored for subsequent payload reconstruction. The remaining portions of the binary values of each pixel are utilized to reconstruct the cover image, as outlined in Eq. (5).

$$Secret_{Bits} = \begin{cases} 2\ LSB\ , & if\ K = '10' \\ 1\ LSB, & if\ Key = '1' \\ 0, & Otherwise \end{cases} \quad (5)$$

Step 3) Reconstruction of the cover image

After the extraction process, the binary values of the recovered cover image are reconstructed by converting them back to decimal format using Eq. (6). This step ensures that the extracted cover image matches the original image exactly, with no differences. The bits identified as containing secret data are extracted according to the specified process and stored for the subsequent reconstruction of the payload. The remaining portions of each pixel's binary value are then used to reconstruct the cover image, ensuring an accurate recovery of the original content.

$$I_{stego}(i,j) = bin2dec\big(I_{Bin}(i,j)\big), \quad \forall i \in [1, rows], j \in [1, cols] \quad (6)$$

4. Results

4.1 Experimental dataset

The proposed DualLSBStego method was evaluated using images from the SIPI database, a well-regarded source of experimental images commonly utilized in steganography research [33].

The dataset comprises grayscale images with a resolution of 256 × 256 pixels. To test the method, 11 random secret bits were generated using the Lorem Ipsum approach [34], varying sizes between 1 and 100 kilobits (kb). The selection of test images from the SIPI database, along with Lorem Ipsum text files, provides a robust basis for evaluating the performance of the proposed steganographic method. This dataset enables a comprehensive assessment of the method's effectiveness, facilitating comparisons with previously established techniques. By benchmarking against existing methods, the evaluation highlights the strengths and potential improvements of the proposed approach.

4.2 Evaluation metrics

To effectively evaluate image quality, we use the PSNR as outlined in Eq. (7) and the SSIM as detailed in Eq. (8). In these calculations, $A(i,j)$ refers to the original image, while $B(i,j)$ corresponds to the image containing the hidden data, both utilized in the Mean Squared Error (MSE) computation in Eq. (9). The SSIM calculation involves parameters $\emptyset_i$ and $\emptyset_j$ representing average pixel intensities, ϑ_i and ϑ_j representing the variations in intensity along the horizontal and vertical axes and $\vartheta_{i,j}$ indicating the covariance between these intensities.

In the proposed DualLSBStego, the PSNR and SSIM are used as essential metrics for evaluating the quality of the obtained stego image by comprehensively comparing it to the cover image. PSNR provides a straightforward numerical indication of how closely the cover and stego images match signal integrity. Conversely, SSIM offers a more nuanced evaluation of visual likeness by factoring in brightness, contrast, and structural similarity. Using both measures allows for a comprehensive analysis, ensuring the embedding process retains the cover image's appearance while securely incorporating the hidden bits from the secret message.

$$PNSR = 10 \times log_{10} \frac{255^2}{MSE} \quad (7)$$

$$SSIM = \frac{(2\emptyset_i\emptyset_j + A_i)(2\vartheta_{ij} + B_i)}{(\emptyset_i^2 + \emptyset_j^2 + A_i)(\vartheta_i^2 + \vartheta_j^2 + B_i)} \quad (8)$$

$$MSE = \frac{1}{K \times L} \sum_{i=1}^{K} \sum_{j=1}^{L} (A(i,j) - B(i,j))^2 \quad (9)$$

4.3 Obtained results

The results from the experimental evaluation of the proposed DualLSBStego demonstrate its effectiveness in balancing the critical tradeoff between payload size and image quality, a persistent challenge in the steganography of digital images. The results in Fig. 3, which illustrates the obtained PSNR for the test images, indicate that while the PSNR generally decreases with increasing payload size, the decline is relatively moderate, suggesting that the DualLSBStego maintains acceptable visual quality even at higher embedding capacities. The average PSNR across various cover images ranges from approximately 55 to 78 dB, indicative of high-quality image retention. Referring to Fig. 4, which shows the results obtained by the SSIM and MSE, the proposed method for all the test images shows a promising performance.

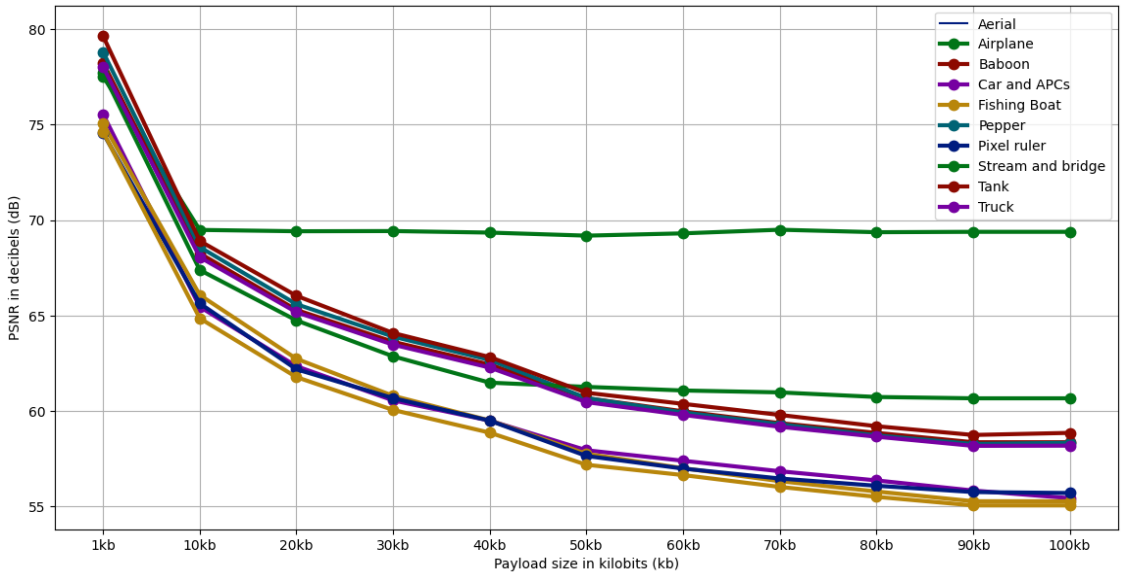
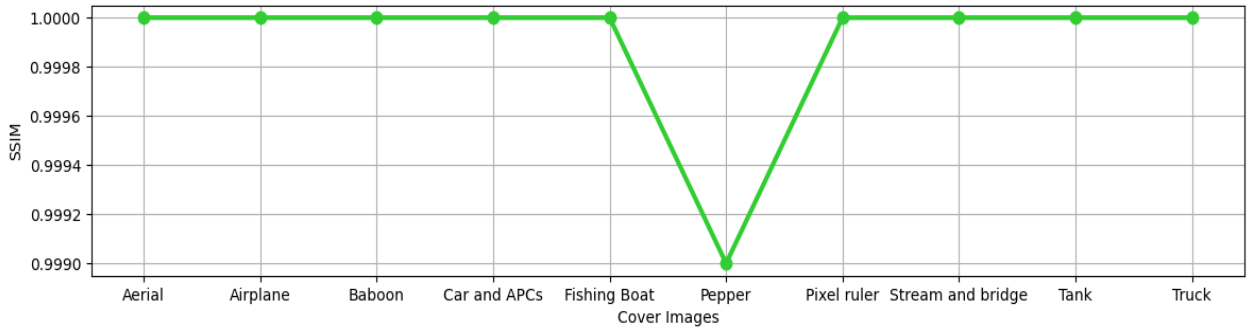
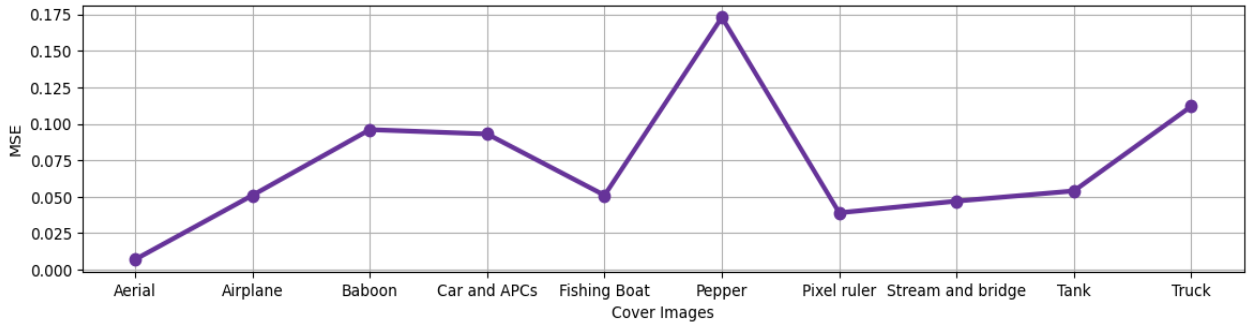


Figure. 3 PSNR Values for Each Test Cover Image



(a)



(b)

Figure. 4: (a) The SSIM values for the Test Images and (b) The MSE values for the Test Images

Considering Fig. 4 (a), the SSIM values remain consistently close to 1 across all payload sizes, highlighting the DualLSBStego strength in preserving the cover images' structural and perceptual integrity. Fig. 4 (b) also represents the MSE curve, almost tending to zero, reflecting the minimal error, showing the algorithm's performance, DualLSBStego. Based on the portraits in Fig. 4, the SSIM values are predominantly at the maximum score of 1.000, with only one instance slightly lower at 0.917, highlighting DualLSBStego's ability to preserve the structural integrity of images and ensuring that embedded data remains imperceptible to the human vision system. Correspondingly, the MSE values, which quantify the average squared differences between the original and stego images, are exceptionally low, ranging from 0.007 to 0.159, demonstrating that the method introduces minimal error during data embedding.

Moreover, by generally considering the DualLSBStego results, it is shown that it performs exceptionally well with smaller payloads, where PSNR values are remarkably high, often exceeding 75 dB. This is most evident in images such as "Aerial" and "Airplane," which exhibit PSNR values above 77 dB for a 1 kb payload, demonstrating the method’s ability to embed small amounts of data with minimal impact on image quality. As the payload size increases, a gradual reduction in PSNR is observed; however, the decline remains within acceptable bounds, with values rarely falling below 55 dB, even for the most oversized payloads tested (100 kb). This gradual decline contrasts sharply with many existing steganographic techniques, where PSNR often drops significantly as payload size grows, leading to more noticeable degradation in image quality. The SSIM values provide additional insight into the DualLSBStego performance, showing consistently high scores close to 1 across all test conditions. This indicates that DualLSBStego effectively maintains the visual similarity between the cover and stego images, even as payload size increases. High SSIM values across all payloads suggest that the method not only preserves pixel intensity but also retains essential structural information and contrast, which are critical for maintaining the overall appearance of the images.

4.4 Benchmarking DualLSBStego the methods in the state-of-the-art

The data presented in Table 1 illustrate the contribution of DualLSBStego in enhancing the PSNR compared to existing methods. Across all the compared test images, DualLSBStego consistently achieves the highest PSNR values, indicating

superior image quality and minimal distortion following data embedding. For example, DualLSBStego attains a PSNR of 60.29 dB for the Baboon image, surpassing the best method, Rustad et al. (2022), at 57.01 dB [29]. In the case of the Boat image, DualLSBStego's PSNR of 63.16 dB not only exceeds Chanda et al. (2023) at 55.89 dB [6] but also demonstrates a remarkable improvement over methods like Sahu and Swain (2019a) in [23], which achieves only 36.66 dB. These findings identify the DualLSBStego's ability to produce high-fidelity stego images, showing significant outperformance.

Furthermore, the results for the Lena and Pepper images reinforce the performance of DualLSBStego. With the PSNR values of 63.15 dB and 60.11 dB, respectively, DualLSBStego outperforms all compared methods. For instance, Chanda et al. (2023) achieved a PSNR of 59.23 dB for Lena, while Rustad et al. (2022) reached only 52.49 dB, and Sahu and Swain's techniques yield PSNR values as low as 36.93 dB and 37.81 dB. These results highlight DualLSBStego's effectiveness in maintaining high image quality for the stego images, showing its robustness. The DualLSBStego's consistent ability to produce high PSNR values emphasizes its significant contribution to the field by optimizing the tradeoff between payload capacity, imperceptibility, and security in steganography.

Additionally, Fig. 5 illustrates the performance of the proposed DualLSBStego method in terms of the SSIM compared to the existing methods. SSIM values are critical in evaluating the quality of stego images, as they reflect how well the embedding process maintains the perceptual integrity of the original image. DualLSBStego stands out with consistently high SSIM values, achieving a perfect score 1.00 for both the Boat and Pepper images. This indicates that the data embedding process has negligible impact on the visual quality of these images, demonstrating the DualLSBstego's effectiveness in achieving imperceptibility.

Table 1. Average PSNR (in dB) comparison between the DualLSBStego and the existing works

Method	**Test Images**			
	Baboon	**Boat**	**Lena**	**Pepper**
Chanda et al. (2023)	55.85	55.89	59.23	55.72
Sahu and Swain (2019a)	36.24	36.66	36.93	37.81
Rustad et al. (2022)	57.01	-	52.49	57.41
Fahim and Ruslan (2023)	37.42	39.36	39.58	38.82
Sahu and Swain (2019b)	38.83	41.75	42.98	43.23
DualLSBStego	60.29	63.16	63.15	60.11

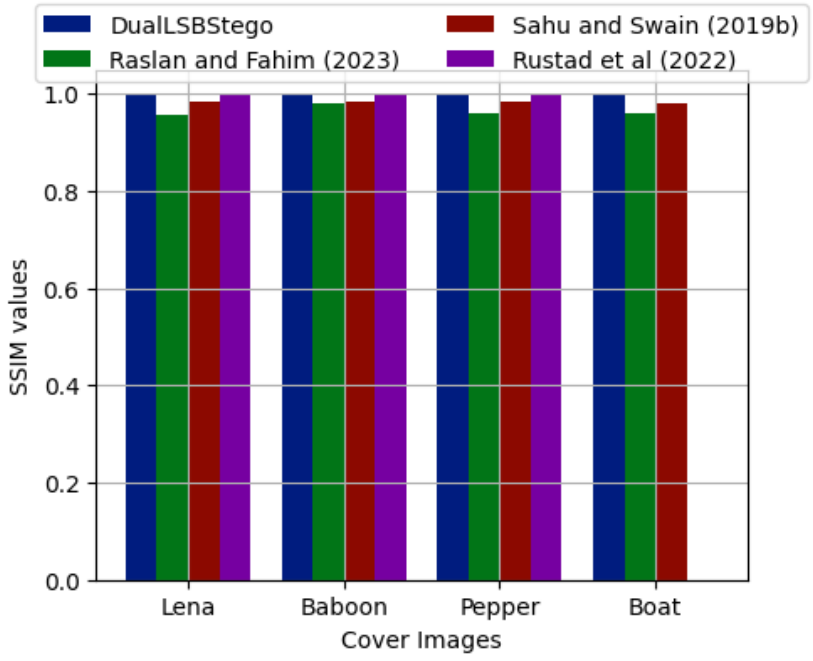


Figure. 5 SSIM Comparison between the DualLSBStego and the existing methods

In contrast, existing methods demonstrate a notable reduction in SSIM values. For instance, Raslan and Fahim (2023) in [28] report SSIM values of 0.999 for Lena, 0.998 for Baboon, 0.999 for Pepper, and 0.999 for Boat. Similarly, Rustad et al. (2022) in [29] achieved 0.999 for Lena and 0.998 for Baboon but only 0.997 for Pepper. Sahu and Swain (2019b) exhibit the lowest performance with SSIM values of 0.98 for Lena, 0.96 for Baboon, 0.96 for Pepper, and 0.96 for Boat [31]. This comparative analysis demonstrates the scientific contribution of DualLSBStego in enhancing the robustness and efficiency of data embedding techniques. By achieving perfect SSIM values, DualLSBStego significantly improves the imperceptibility of hidden data while increasing payload capacity, thus significantly improving the existing methods.

4.5 DualLSBStego security analysis

The security analysis of the proposed DualLSBStego method, as evidenced by the data in Table 2, demonstrates its strong performance in maintaining data concealment and image quality under compression. The average PSNR values, which range from 22.927 in complex images like 'Baboon' to 39.930 in more straightforward images like 'Pixel ruler,' indicate that DualLSBStego effectively balances data embedding without noticeably degrading the visual quality of the stego images, even after compression. The obtained SSIM scores, with most images scoring above 0.7 and reaching as high as 0.996, highlight the DualLSBStego's ability to preserve the structural similarity of the images, making it challenging for attackers to detect any the presence of steganographic payload. This resilience ensures the hidden data remains secure and intact, enhancing the steganographic process's security using DualLSBStego.

5. Conclusion

The DualLSBStego framework introduces a new steganographic algorithm that improves security by selecting pixels for embedding based on their intensity. It ensures that data is hidden randomly and uniformly within the cover image. Tests using PSNR and SSIM metrics show that DualLSBStego performs better than existing methods, proving it is effective for secure data embedding. The framework provides a promising solution to the problem of balancing the amount of data embedded with the quality of the image. Results, with PSNR values between 55 and 80 dB and SSIM values close to 1, confirm its main contributions: (1) improved selection of areas to embed data, showing the algorithm’s strength; (2) increased capacity to hold more data, making it useful for cases where large amounts of information need to be hidden; and (3) improved invisibility of the embedded data through adaptive embedding based on pixel intensity. By keeping the image quality high, even with large amounts of embedded data, DualLSBStego ensures the stego images look almost identical to the original, enhancing security and reliability.

Future work will focus on applying this method in various fields and exploring additional techniques to improve its applicability. Further development will include integrating machine learning and deep learning models to optimize the selection of message sizes for different image types, enhancing the overall performance of the proposed framework.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, ANF, NJDLC, and TA; methodology, ANF, NJDLC, and TA; software development, ANF, and NJDLC; formal analysis, ANF, NJDLC, and TA; original draft writing, and visualization, ANF and NJDLC; review and editing of the manuscript, NJDLC, and TA; supervision, TA; project administration, TA; and acquisition of funding, TA.

Acknowledgments

The authors thank all the NCC laboratory, Department of Informatics, ITS, and all the research group members for their invaluable contributions and support.

References

[1] A. Duraj and P. Szczepaniak, “Detection of outlier information using linguistically quantified statements - the state of the art”, *Procedia Comput Sci*, Vol. 207, pp. 1953-1958, 2022, doi: 10.1016/j.procs.2022.09.254.

[2] B. Lorch, F. Schirrmacher, A. Maier, and C. Riess, “On the Security of the One-and-a-Half-Class Classifier for SPAM Feature-Based Image Forensics”, *IEEE Transactions on Information Forensics and Security*, Vol. 18, pp. 2466-2479, 2023, doi: 10.1109/TIFS.2023.3266168.

[3] M. A. Hameed, M. Hassaballah, R. Abdelazim, and A. K. Sahu, “A novel medical steganography technique based on Adversarial

Neural Cryptography and digital signature using least significant bit replacement", *International Journal of Cognitive Computing in Engineering*, Vol. 5, pp. 379-397 Aug. 2024, doi: 10.1016/j.ijcce.2024.08.002.

[4] W. El-Shafai, F. Khallaf, E. S. M. El-Rabaie, and F. E. Abd El-Samie, "Proposed neural SAE-based medical image cryptography framework using deep extracted features for smart IoT healthcare applications", *Neural Computing and Applications*, Vol. 34, No. 13, pp. 10629-10653, 2022, doi: 10.1007/s00521-022-06994-z.

[5] P. C. Mandal, I. Mukherjee, G. Paul, and B. N. Chatterji, "Digital image steganography: A literature survey", *Information Sciences*, Vol. 609, pp. 1451-1488, 2022, doi: 10.1016/j.ins.2022.07.120.

[6] A. W. Chanda D'Layla, M. Nevin, G. G. Sunardi Putra, N. J. de La Croix, and T. Ahmad, "Steganography in Grayscale Images: Improving the Quality of a Stego Image", In: *Proc. of 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, pp. 1-6, 2023, doi: 10.1109/SMARTGENCON60755.2023.10442310.

[7] N. J. D. La Croix, T. Ahmad, and F. Han, "Comprehensive Survey on Image Steganalysis Using Deep Learning", *Array*, pp. 100353, 2024, doi: 10.1016/j.array.2024.100353.

[8] K. Kaushik and A. Bhardwaj, "Zero-width text steganography in cybercrime attacks", *Computer Fraud & Security*, Vol. 2021, No. 12, pp. 16-19, 2021, doi: 10.1016/S1361-3723(21)00130-5.

[9] S. Debnath, R. K. Mohapatra, and R. Dash, "Secret data sharing through coverless video steganography based on bit plane segmentation", *Journal of Information Security and Applications*, Vol. 78, pp. 103612, 2023, doi: 10.1016/j.jisa.2023.103612.

[10] X. Zhang, C. Li, and L. Tian, "Advanced audio coding steganography algorithm with distortion minimization model based on audio beat", *Computers and Electrical Engineering*, Vol. 106, pp. 108580, 2023, doi: 10.1016/j.compeleceng.2023.108580.

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

[12] T. Alobaidi and W. Mikhael, "An adaptive steganography insertion technique based on wavelet transform", *Journal of Engineering and Applied Science*, Vol. 70, No. 1, pp. 144, 2023, doi: 10.1186/s44147-023-00300-x.

[13] G. Swain and A. Pradhan, "Image Steganography Using Remainder Replacement, Adaptive QVD and QVC", *Wirel Pers Commun*, Vol. 123, No. 1, pp. 273-293, 2022, doi: 10.1007/s11277-021-09131-6.

[14] W. Luo, F. Huang, and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited", *IEEE Transactions on Information Forensics and Security*, Vol. 5, No. 2, pp. 201-214, Jun. 2010, doi: 10.1109/TIFS.2010.2041812.

[15] Y. Peng, C. Fu, Y. Zheng, Y. Tian, G. Cao, and J. Chen, "Medical steganography: Enhanced security and image quality, and new S-Q assessment", *Signal Processing*, Vol. 223, pp. 109546, 2024, doi: 10.1016/j.sigpro.2024.109546.

[16] N. Akhtar, P. Johri, and S. Khan, "Enhancing the Security and Quality of LSB Based Image Steganography", In: *Proc of 2013 5th International Conference on Computational Intelligence and Communication Networks*, 2013, pp. 385-390. doi: 10.1109/CICN.2013.85.

[17] I. Théophile, N. J. De La Croix, and T. Ahmad, "Fuzzy Logic-based Steganographic Scheme for high Payload Capacity with high Imperceptibility", In: *Proc of 2023 11th International Symposium on Digital Forensics and Security (ISDFS)*, 2023, pp. 1-6. doi: 10.1109/ISDFS58141.2023.10131727.

[18] Y. Pei, X. Luo, Y. Zhang, and L. Zhu, "Multiple Images Steganography of JPEG Images Based on Optimal Payload Distribution", *Computer Modeling in Engineering & Sciences*, Vol. 125, No. 1, pp. 417-436, 2020, doi: 10.32604/cmes.2020.010636.

[19] P. Puteaux and W. Puech, "A Recursive Reversible Data Hiding in Encrypted Images Method with a Very High Payload", *IEEE Trans Multimedia*, Vol. 23, pp. 636-650, 2021, doi: 10.1109/TMM.2020.2985537.

[20] Z. Fu, X. Chai, Z. Tang, X. He, Z. Gan, and G. Cao, "Adaptive embedding combining LBE and IBBE for high-capacity reversible data hiding in encrypted images", *Signal Processing*, Vol. 216, pp. 109299, 2024, doi: 10.1016/j.sigpro.2023.109299.

[21] M. Bachrach and F. Y. Shih, "Survey of Image Steganography and Steganalysis", *Multimedia Security*, 2017, pp. 201-214. doi: 10.1201/b12697-11.

[22] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method", *IEEE Access*, Vol. 10, pp. 124053-124075, 2022, doi: 10.1109/ACCESS.2022.3224745.

[23] A. K. Sahu and G. Swain, "Data hiding using adaptive LSB and PVD technique resisting PDH and RS analysis", *International Journal of Electronic Security and Digital Forensics*, Vol. 11, No. 4, pp. 458, 2019, doi: 10.1504/IJESDF.2019.102567.

[24] M. Kalita, T. Tuithung, and S. Majumder, "An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique", *Cryptologia*, Vol. 43, No. 5, pp. 414-437, 2019, doi: 10.1080/01611194.2019.1579122.

[25] U. A. Md. Ehsan Ali, E. Ali, Md. Sohrawordi, and Md. N. Sultan, "A LSB Based Image Steganography Using Random Pixel and Bit Selection for High Payload", *International Journal of Mathematical Sciences and Computing*, Vol. 7, No. 3, pp. 24-31, Aug. 2021, doi: 10.5815/ijmsc.2021.03.03.

[26] B. M. Parmar and C. Rakesh Kumar, "High PSNR Based Image Steganography", *International Journal on Recent and Innovation Trends in Computing and Communication*, 2017, [Online]. Available: http://www.ijritcc.org

[27] G. Maji, S. Mandal, and N. C. Debnath, "Pixel Value Difference Based Image Steganography with One Time Pad Encryption Soumya Sen", In: *Proc of IEEE 17th Int. Conf. Ind. Informat. (INDIN)*, pp. 22-25, 2019.

[28] A. Fahim and Y. Raslan, "Optimized steganography techniques based on PVDS and genetic algorithm", *Alexandria Engineering Journal*, Vol. 85, pp. 245-260, 2023, doi: 10.1016/j.aej.2023.11.013.

[29] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility", *Journal of King Saud University - Computer and Information Sciences*, Vol. 34, No. 6, pp. 3559-3568, 2022, doi: 10.1016/j.jksuci.2020.12.017.

[30] L. Almazaydeh, "Secure RGB image steganography based on modified LSB substitution", *Int J Embed Syst*, Vol. 12, No. 4, pp. 453, 2020, doi: 10.1504/IJES.2020.107644.

[31] A. K. Sahu and G. Swain, "An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function", *Wirel Pers Commun*, Vol. 108, No. 1, pp. 159-174, 2019, doi: 10.1007/s11277-019-06393-z.

[32] E. Z. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker, "LSB-based Bit Flipping Methods for Color Image Steganography", *J Phys Conf Ser*, Vol. 1501, No. 1, pp. 012019, 2020, doi: 10.1088/1742-6596/1501/1/012019.

[33] University of Southern California, Signal and Image Processing Institute, "Miscellaneous", Accessed: May 01, 2024. [Online]. Available: https://sipi.usc.edu/database/database.php?volume=misc

[34] Lorem Ipsum, *The Standard Lorem Ipsum Passage*, Accessed: May 1, 2024. [Online]. Available: https://www.lipsum.com/