IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Mathematical Modelling of Engineering Problems
Vol. 11, No. 6, June, 2024, pp. 1403-1416
Journal homepage: http://iieta.org/journals/mmep

Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach

Mohammed Sabri Abuali[1,2*], C. B. M. Rashidi[1], Rafikha Aliana A. Raof[3], Ku Nurul Fazira Ku Azir[1], Safa Saad Hussein[1], Ahmed Q. Abd-Alhasan[2,3]

[1] Centre of Excellence for Advanced Communication Engineering, Faculty of Electronic Engineering & Technology, Universiti Malaysia Perlis, Perlis 02600, Malaysia
[2] South Refineries Company (SRC), Ministry of Oil, Basra 62001, Iraq
[3] School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, Johor 79000, Malaysia

Corresponding Author Email: mohmedsabry847@gmail.com

https://doi.org/10.18280/mmep.110602

Received: 13 October 2023
Revised: 2 December 2023
Accepted: 15 December 2023
Available online: 22 June 2024

Keywords:
Wavelet Obtained Weights, Dynamic Least Significant Bit, steganographic, steganography

ABSTRACT

This paper introduces a novel approach to enhancing multi-level security using steganography, a method of concealing information within non-secret data. This paper introduces an innovative approach to multi-level security enhancement using steganography, the art of concealing information within non-obvious data. Our proposed method uniquely combines Dynamic Least Significant Bit (DLSB) steganography with Wavelet Obtained Weights (WOW) steganographic algorithms, forging a sophisticated and adaptable system for secret data embedding. In our enhanced approach, we start by embedding text into an image using an optimized version of DLSB steganography. This refined technique adapts intelligently to the image's local contrast, thereby preserving its visual quality and ensuring the integrity of the embedded information. Subsequently, the payload image is merged with a cover image through the WOW algorithm. This step optimally selects pixels for data embedding, creating a steganographic image that is virtually indistinguishable from the original. The novelty of our work lies in the seamless integration of these two advanced steganographic techniques, which significantly elevates the security and invisibility aspects beyond the current state-of-the-art methods in digital steganography. For validation, we utilized a pretrained MobileNet model to differentiate between original and stego images. This model plays a crucial role in demonstrating the indetectability of our method, achieving an impressive accuracy of 85% in distinguishing stego images from their originals. Our rigorous testing across various metrics — including Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Bit Error Rate (BER), and Mean Squared Error (MSE) — showcases the effectiveness of our approach. The results indicate a robust performance, marking a significant advancement in secure digital communication. In this paper, we focus primarily on the detailed presentation of our results and the significant contributions of our current research, setting a strong foundation for future exploration in increasing robustness against steganalysis and improving the statistical invisibility of the steganography process.

1. INTRODUCTION

The common ease of connectivity made possible by the growth of digital communication has significantly increased the number of active users. However, when sending data over a public network, this convenience presents security issues. Digital watermarking and steganography are the two main methods that have been used to overcome these issues and guarantee data security.

A pioneering method in this area, digital watermarking, was created to protect the transmission of personal data. Digital watermarking has been suggested as a number of ways to protect communication privacy. Its goal is to secure the validity, integrity, and protection of concealed information by embedding it into a carrier.

On the other hand, steganography entails transforming a message into a format that is absolutely undetected within the carrier. It seeks to maintain the human visual system's (HVS) incapability to detect any concealed information [1]. The terms "steganos" (which means covered, veiled, or protected) and "graphein" (which means write) are the roots of the phrase "steganography" [2]. In contrast to cryptography, which scrambles data to change its meaning and quality for unauthorized users, steganography primarily focuses on hiding the presence of hidden information [3]. Steganography, which involves silently concealing information inside media carriers such that it is invisible to and undiscovered by the human visual system (HVS), is both a science and an art of

clandestine communication [1, 4]. The term "steganography" has its roots in the Greek words "steganos," meaning "covered" or "hidden," and "graphein," which translates to "write." Essentially, it refers to the art of secret writing. While steganography focuses on concealing the very presence of secret information, cryptography, on the other hand, transforms data to appear nonsensical to unauthorized viewers.

Several aspects are taken into account in order to evaluate the steganographic techniques' advantages and disadvantages. These characteristics include capacity, security, and invisibility. The capacity of a cover object is the maximum amount of hidden data that may be stored there without materially affecting the quality of the images. Bits per pixel (bpp) are commonly used to quantify a steganographic technique's capabilities [5, 6]. Another essential quality is security, as a good steganography method should be impervious to steganalysis assaults. The attribute connected to the image's quality and transparency is imperceptibility. The stego-picture may degrade slightly from the original image after hiding the secret data under the cover image, but maintaining high quality and transparency is the major objective.

The imperceptibility of the stego-picture is frequently assessed using the Peak Signal-to-Noise Ratio (PSNR), with higher PSNR values indicating better image quality [7].

Data is hidden via steganography within a carrier media, such as music, video, or text [7]. Depending on the kind of carrier media, many steganography techniques exist, such as picture, video, text, and audio steganography [8, 9]. In steganography, the carrier medium is referred to as the cover object, and the concealed data is referred to as the payload capacity. The amount of secret data to be inserted determines the type of cover object to use, and the resilience of the system determines how undetectable the secret message will be. Since they are so widely utilized and so redundant, images are frequently employed as cover items.

The final image that includes the concealed data is known as the stego image. Spatial domain methods and transform domain methods are the two primary kinds of approaches in picture steganography [10].

Security, capacity, and imperceptibility concerns must be addressed in order for a steganography technique to be effective. Among these issues, imperceptibility significantly affects how difficult it is to tell if a hidden message is present or not. Techniques like odd/even pixels distribution formats are frequently used to achieve imperceptibility. A steganography system's security is its resistance against outside threats. The largest amount of data that may be securely contained in a cover picture without significantly distorting it or impairing data detection is referred to as capacity. These issues with the current steganography systems are intended to be addressed by the suggested technique [11, 12].

In this paper, we propose a novel application of multilevel security through steganography, targeting the enhancement of data privacy and security. Our methodology centers around a two-tiered approach. The first tier involves embedding text within an image, creating an initial layer of hidden information. This process not only conceals the data but also preserves the integrity and quality of the image. In the second tier, we take this 'embedded image' and further embed it within another image. This layered embedding technique, leveraging Binary Image Texts (BITS), ensures a more sophisticated and secure method of data concealment. The BITS technique involves converting text into a binary format and then embedding this binary data into images at various levels, significantly enhancing the security of the embedded information.

The effectiveness of our approach stems from the intricate embedding process. The two-tiered strategy multiplies the security barriers, making the detection and deciphering of the embedded data increasingly challenging. The first tier masks the presence of hidden data within the primary image, while the second tier adds an additional layer of obfuscation by embedding this altered image into another. This approach not only complicates potential steganalysis but also maintains the visual quality of the images, a crucial aspect in steganographic practices.

The remainder of this paper is organized as follows: Section 2 delves into the theoretical underpinnings of our steganographic method, including a detailed explanation of Binary Image Texts and their role in enhancing security. Section 3 outlines our methodological approach, describing the step-by-step process of the two-tiered embedding technique. In Section 4, we present a series of experiments and results, demonstrating the efficacy of our approach. Section 5 discusses the potential application scenarios, highlighting how this method can be effectively utilized in various fields requiring secure data transmission. Finally, Section 6 concludes the paper with a summary of our findings and suggestions for future research in this domain.

1.1 Problem statement

Despite the existing methodologies for secure communication, there is a pressing issue regarding the potential vulnerability of single-layer steganography. While these techniques have traditionally provided a degree of security by concealing data within an image, they are increasingly susceptible to steganalysis, a process of detecting hidden information within digital media. Additionally, single-layer steganography techniques often face limitations in the volume of data that can be concealed, which restricts their applicability in various scenarios where large-scale secure data transmission is required.

The problem, therefore, lies in enhancing the security and capacity of current steganographic techniques to overcome these vulnerabilities. This paper proposes a multilevel steganographic technique as a potential solution. However, implementing such a technique presents its own set of challenges. These include ensuring the integrity and recoverability of the hidden data, managing the increased computational complexity that comes with multiple layers of steganography, and maintaining the perceptual invisibility of the carrier image despite the added layers of embedded information. A comprehensive exploration and evaluation of these complexities form the problem statement of this paper.

1.2 Contribution

In this paper, we make a significant contribution to the field of secure data transmission by introducing a novel, multilevel steganographic technique. Our approach is distinguished by the innovative use of multiple Binary Image Texts (BITS) and an advanced multilevel concealment strategy. By leveraging BITS, we scatter concealed information throughout different parts of an image, effectively minimizing the risk of detection. This technique dilutes any sharp transitions in the image that might otherwise draw attention, thereby reducing detectability.

Moreover, using multiple BITS allows us to embed larger volumes of data compared to traditional methods, substantially increasing the capacity for data hiding.

In addition to the BITS strategy, we introduce a pioneering method of multilevel concealment. This involves embedding an image containing hidden data within another image, creating a complex layered effect. Each layer of embedding adds a level of obscurity, significantly increasing the challenge for adversaries in detecting and extracting the concealed information. This multilayer approach is a marked progression from conventional single-layer steganography, effectively countering the growing sophistication of steganalysis techniques.

Another critical aspect of our contribution is the incorporation of the MobileNet deep learning model into our detection process. MobileNet, known for its efficiency and compact architecture, is adept at differentiating between cover images and stego images. We have extensively trained this model to recognize the subtle differences introduced by our steganographic process. Through rigorous testing, we demonstrate that MobileNet effectively identifies stego images, providing a robust means to evaluate the stealthiness of our method. The successful application of MobileNet in our experiments underlines the effectiveness of our multilevel steganographic approach, showcasing its potential as a highly secure method of data concealment.

Our work not only addresses the current challenges in steganography but also sets a new benchmark for secure communication methodologies. By introducing these novel techniques and demonstrating their effectiveness, we contribute significantly to the evolution of data security practices.

2. RELATED WORK

In the realm of ***visual cryptography*** which entailed exploiting cover-based semi-groups to improve picture contrast, was first proposed by Naor and Shamir [13] in 1994. They also introduced the visual cryptography method VCS (k, n) [14].

The integration of ***deep learning*** with steganography, by combining steganographic methods with deep learning and visual cryptography, Seuti et al. [15] suggested a revolutionary method in the realm of picture steganography. By using the LSB technique, for example, where the buried information might be easily retrieved if the location is known, they sought to overcome the security issues with conventional techniques. The authors devised a multi-step procedure for concealing a hidden image under a cover photo in order to get around these restrictions. First, they used an autoencoder, which combines an encoder and a decoder, to process the secret picture. The security of the secret image was increased by this autoencoder's compression and unrecognizability. The next step was to use visual cryptography. To achieve this, the authors performed an exclusive OR (XOR) operation on the compressed secret picture with a randomly generated image called mask1. The hidden image's content was further obscured by this visual encryption stage. Finally, the authors hid the encrypted secret picture within the carrier or cover image using the LSB approach. By using deep learning and visual cryptography, this guaranteed that the secret picture stayed concealed within the cover image while adding an extra degree of protection. The authors tested the suggested method and used image quality criteria to determine how consistently the stego picture was produced. The experimental findings showed that, in comparison to current technologies, the suggested strategy improved security. A comparative study was also conducted to show how much better the authors' approach is than most other approaches used today. The authors' method of merging visual cryptography, deep learning, and steganography presents a possible remedy to the security issues with existing picture steganography techniques. Their findings demonstrate the potency and excellence of their suggested method, pointing to its potential for use in secure communication and information concealment.

Digital watermarking with visual cryptography mechanisms was also carried out [16]. A visual cryptography approach for copyright security in watermarking was presented by Tijedjadjine et al. [17].

An adaptive fuzzy inference technique for color picture steganography was put out in a 2021 study. This approach considered picture complexity elements as brightness, color sensitivity, and pixel similarity [18]. A hybrid data transmission technique that included steganography and encryption was presented at around the same time by Gupta and Saxena. Additionally, they created a program that uses steganography and cryptography to hide data [19, 20].

A steganography method that used the LSB approach to conceal data and pictures within other images was proposed by Shekhawat et al. [20] in 2020.

Encoding the secret message in the least significant bit (LSB) of each pixel is a widely used technique in the field of picture steganography. This technique is widely used since changing the LSB has little effect on the carrier picture because it is challenging for the human eye to distinguish between the original and changed cover images.

In order to evaluate several LSB-based steganography techniques and determine if a person could tell the difference between the stego picture and the original cover image, Chandramouli and Memon [21] carried out research.

Karim et al. [22] offered a brand-new LSB-based method for concealing a secret picture utilizing a cover image and a secret key. Based on the secret key, the cover image layer was selected in this technique to cover the concealed picture. The stego key was transformed into a 1D circular array bitstream, and then the secret picture was put to it. The LSB of the first red layer pixel and the first bit of the stego key were both subjected to operations throughout the encoding process. If the last bit was 1, the green layer of the cover picture was chosen to hide the concealed image's single bit. If the outcome bit was 0, on the other hand, the blue layer of the cover picture was picked. The next red layer pixel and the next bit of the stego key were both taken into consideration as the concealed image's succeeding bits were processed in the same manner. The LSB of the red layer and the matching pixel of the secret key were used in an XOR operation to decode the secret picture. If the outcome bit was 1, the green layer's LSB contained the hidden information. The LSB of the blue layer was used to retrieve the secret information if the resulting bit was 0. To successfully recover the secret picture, the information was then reorganized into a 2D binary image matrix.

Three steganography techniques, each with its unique traits, were introduced by Hossain et al. [23]. These methods made use of tools to estimate the smooth and angular regions of a picture while taking into consideration the bit's dependence on its surroundings and psychovisual redundancy. The initial

method involves embedding three bits per pixel in smooth zones, taking advantage of their uniformity to conceal extra information. The second method, on the other hand, used variable-rate pixel embedding, changing the embedding rate dependent on the complexity of the region, in edged sections where there are more changes. Although these techniques proved they could create high-quality stego pictures, it should be highlighted that they did not use any particular security measures. The fundamental goal of these methods was to provide the best possible images while maintaining the visual imperceptibility of the hidden information. However, in order to secure the concealed data from being easily recovered or identified, more security measures would be required in terms of resilience against assaults or illegal access.

Płachta et al. [24] suggested addressing the issue of spotting steganographically altered JPEG photos. They looked at the effectiveness of several shallow and deep learning techniques for detecting picture steganography. They used photos from the BOSS database that had been processed using three well-known steganographic algorithms: nsF5, uniform embedding revisited distortion (UERD), and JPEG universal wavelet relative distortion (J-Uniward). At two different densities, the steganographic methods were used. In an effort to increase the detection accuracy, the authors investigated several feature spaces. They discovered that the Gabor filter residuals (GFR) and discrete cosine transform residuals (DCTR) generated the most encouraging outcomes. At a density of 0.4 bpnzac (99.9% accuracy), they specifically obtained virtually perfect detection accuracy for the nsF5 method. However, with a maximum accuracy of just 56.3%, finding J-Uniward at a density of 0.1 bpnzac proved to be quite difficult. The authors' investigation also took into account ensemble classifiers as a deep learning-based detection technique substitute. The ensemble classifiers produced encouraging results, indicating their potential as successful steganography detection strategies. The study of the authors clarifies the issue of identifying steganographically altered JPEG photographs. They investigated numerous feature spaces, tested the accuracy of various steganographic techniques, and evaluated the performance of several shallow and deep learning algorithms. Their research adds to the corpus of knowledge and sheds light on the efficiency of ensemble classifiers in the detection of steganography.

Duan et al. [25] suggested a novel deep learning-based high-capacity picture steganography technique. They set out to overcome the drawbacks of conventional methods of picture steganography, which frequently prioritize the safe embedding of sensitive information while ignoring the payload capacity and steganographic image quality for the Human Visual System (HVS). The authors' suggested technique involved transforming the secret picture using the discrete cosine transform (DCT). The generated steganographic picture was then encrypted with Elliptic Curve Cryptography (ECC) to improve its anti-detection capabilities. The SegNet Deep Neural Network, which was made up of a collection of Hiding and Extraction networks, was used by the authors to increase the steganographic capability. This framework made full-size picture extraction and effective steganography possible. The trial outcomes showed how well the suggested technique worked to assign each pixel in the image to a location that would result in a relative steganographic capability of 1. The Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) values of the steganographic pictures produced by this approach were also greater, reaching 40dB and 0.96, respectively.

In recent years, the field of optical communications has seen a myriad of advancements. Notably, the optical vortex has garnered significant attention among researchers, primarily due to its multi-faceted applications. It is an intriguing feature in optics that has been employed in diverse fields like optical tweezers, microscopy, quantum information processing, optical trapping, and laser machining. More than just a fascinating phenomenon, an optical vortex carries a helical wavefront, an intrinsic characteristic that allows it to transport orbital angular momentum. This unique property is pivotal, especially when applied to heralded single-photon transfer in the transverse amplitude.

Each study mentioned has been pivotal in its own right. For instance, the use of visual cryptography [13, 14] laid the groundwork for future developments in image-based security. The LSB-based techniques used by Shekhawat et al. [26] and Chandramouli and Memon [21] were significant for demonstrating how subtle changes can be effectively used for data concealment. In deep learning, the studies cited in studies [15, 25] showed how integrating AI can substantially enhance steganographic capabilities. The optical communication techniques used by Ghazi et al. [27] and Alayedi et al. [28] represented a leap in increasing the capacity and security of communication channels.

The relationship between these studies is integral to understanding the evolution of steganographic and optical communication techniques. Each study builds upon the findings of previous works, progressively advancing the field. Our research aims to bridge the gaps identified in these studies, particularly in terms of security, efficiency, and capacity.

Comparatively, visual cryptography is foundational but somewhat limited in scope. LSB-based steganography offers simplicity and effectiveness but can be vulnerable to detection. Deep learning approaches, while more complex, provide enhanced security and adaptability. Optical communication techniques, though not directly related to steganography, demonstrate the potential for high-capacity secure transmissions. Our work seeks to synthesize these various approaches, combining the best aspects of each to create a more comprehensive and secure steganographic method.

The advancements in ***optical communications***, a pivotal study [27] delved deep into integrating the optical vortex with optical-CDMA (optical code-division multiple-access). This combination was further enhanced by integrating with WDM (wavelength division multiplexing). The primary objective behind this amalgamation was to amplify both the capacity and security facets of optical communication. By adopting Laguerre-Gaussian (LG) modes and leveraging the optical vortex based on a one-dimensional zero cross-correlation (ZCC) code, the study revealed a substantial decrease in mode coupling. This reduction proved consequential in augmenting channel performance and response. In a more comprehensive scope, the study evaluated LG modes grounded on the 1D-ZCC code, which were then propagated over a multi-mode fiber (MMF) incorporating the optical vortex. The outcomes were promising, showcasing a significant mitigation in channel effects. Collectively, the results pointed towards the potential development of a hybrid WDM-Optical-CDMA system utilizing the optical vortex over MMF.

Parallelly, another significant contribution [28] to the field was made through the introduction of a novel zero cross correlation (ZCC) code, specifically tailored for spectral amplitude coding-optical code division multiple access (SAC-

OCDMA) systems. This code, uniquely initiated from the identity matrix, showcases multiple advantages, especially when emphasizing its simplicity and adaptability. In terms of performance metrics, this proposed ZCC code not only adapts seamlessly with SAC-OCDMA systems but also flaunts a high SNR value. When benchmarked against previously established codes, notably the modified quadratic congruence (MQC) and modified double weight (MDW) codes, the novel ZCC code outperformed them by reaching 3.18 and 1.84 times of the system capacity, respectively.

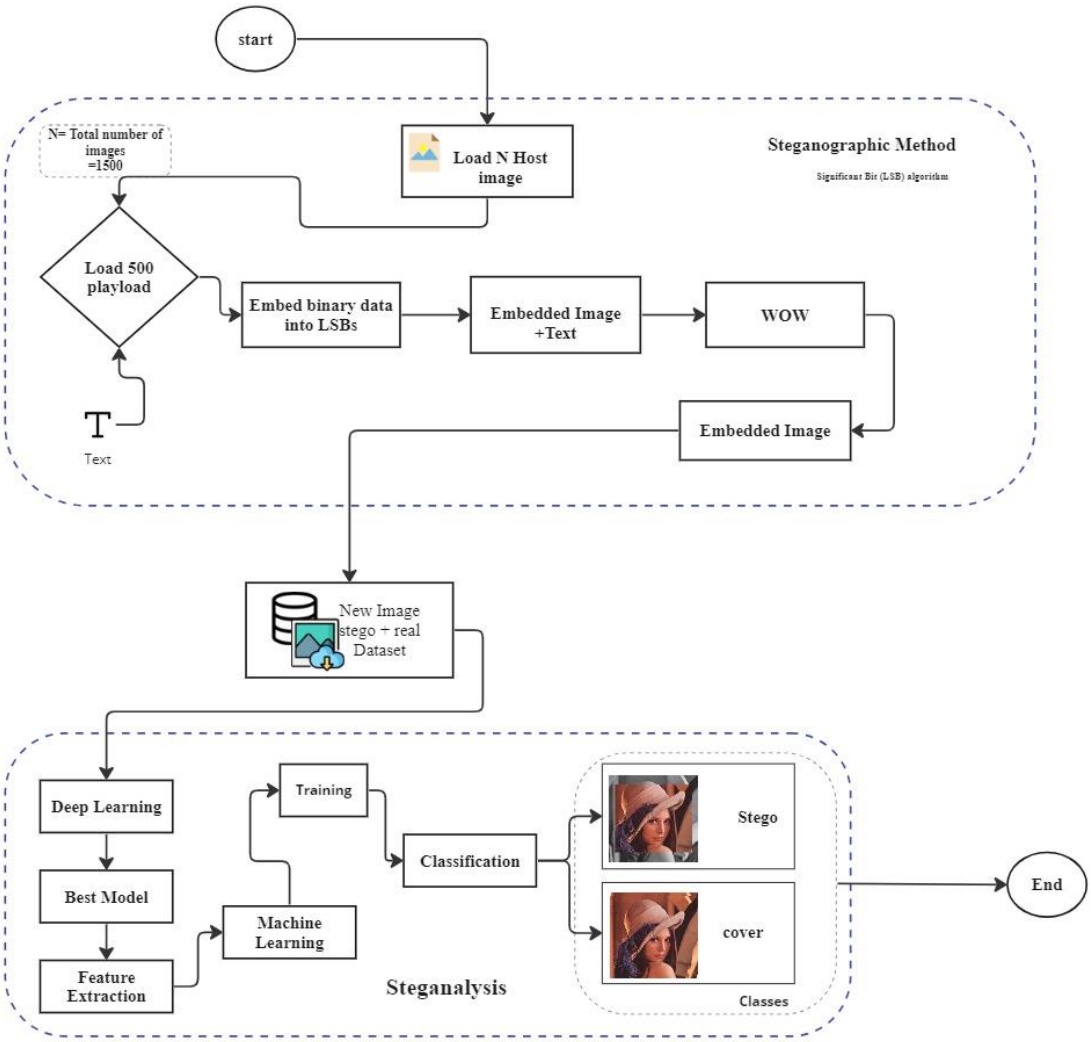

Figure 1. General flowchart

3. METHODOLOGY

Our methodology as illustrate in Figure 1 initiates with the division of a dataset into cover and payload images. Subsequently, we employ a novel approach termed “Dynamic Least Significant Bit” to embed text into the payload images, constituting the first layer of our multilevel steganographic technique. Further advancing the complexity, the manipulated payload image, now embedded with hidden text, is concealed within the cover image, forming the second layer of obfuscation. Upon successful embedding, the original and stego images are consolidated into a single dataset and divided into training and testing sets. This data is utilized to train and evaluate the performance of a pretrained deep learning model, MobileNet, renowned for its efficiency in mobile and embedded vision applications. After training, the model’s proficiency is gauged by its accuracy in distinguishing between the original and stego images in the testing set, thus validating the effectiveness of our proposed multilevel steganographic technique.

3.1 Dataset

In this subsection, we introduce the use of a specific dataset, “BOSSBase 1.01”. This dataset, containing a total of 1500 images, forms the basis for our multilevel steganographic experiment. Our methodology commences with loading this substantial dataset into our system.

To effectively utilize these images for our steganographic purposes, we implement a strategic division of the loaded dataset into two distinct sets. Of the total 1500 images, we earmark 1000 images to serve as ’cover’ images. These images play a crucial role in our strategy as they function as the outermost layer or facade, beneath which our multilevel concealed data resides.

The remaining 500 images from the dataset are designated as ’payload’ images. These images form the core of our data hiding operation. The selected text will be skillfully embedded within these payload images, which are subsequently embedded within the cover images. This arrangement is essential to our multilevel steganographic approach as it

allows for an additional layer of data hiding and hence, an enhanced level of security.

Our methodology, leveraging the BOSSBase 1.01 dataset and the systematic division of images into cover and payload sets, provides the foundation for the effective execution and evaluation of our multilevel steganographic technique.

In selecting the BOSSBase 1.01 dataset for our research, we were guided by several critical factors that make it particularly suitable for our multilevel steganographic experiment. Primarily, the BOSSBase 1.01 dataset is renowned for its diversity and representativeness, encompassing a wide range of image types and content. This variety ensures that our methodology and results are not biased towards a specific type of image or limited by a narrow data scope. Furthermore, the dataset is a standard benchmark in the field of steganography, frequently used by researchers to test and validate steganographic algorithms. This widespread adoption in the research community lends credibility to our experiments and allows for meaningful comparisons with existing studies. The high quality and resolution of the images in the dataset are also crucial, as they provide the necessary detail and complexity for effective data embedding and concealment. By using the BOSSBase 1.01 dataset, we ensure that our findings are robust, reproducible, and relevant to current steganographic practices.

3.2 Text steganography

The second stage (Figure 2) in our methodology is the process of embedding text into the payload images. In order to do this, we utilize an innovative technique that has its roots in the traditional Least Significant Bit (LSB) steganography method.

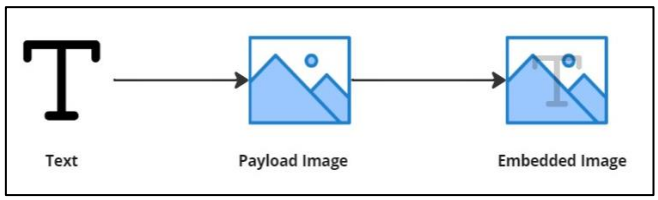

Figure 2. Text steganography

i. Standard LSB: The researchers employed the standard or general Least Significant Bit (LSB) [29] technique as a basis for their embedding process. In this technique, the aim is to replace the least significant bit—the final bit—in a certain number of bytes within the cover file with a sequence of bytes containing the hidden data. Given that the LSB is the smallest and least consequential bit within a byte, modifying it incurs minimal impact on the file. This subtlety ensures that the alterations to the file remain largely imperceptible to human senses, offering a discreet method for data concealment. This traditional LSB technique, though simple in its approach, forms the core of the researchers' advanced steganographic methodology.
ii. LSB Optimization: Additionally, the researchers adopted an enhanced version of the standard LSB method [30]. This refined technique, known as the LSB optimization, expands upon the conventional approach by utilizing the two least significant bits (2 bits) in a byte for the embedding process, as opposed to just the last bit. This modification facilitates the hiding of more data within the cover file, effectively doubling the capacity of concealed information compared to the standard LSB technique. This optimized method not only maintains the subtlety and undetectability of the traditional LSB technique, but also significantly improves upon its data hiding capabilities, paving the way for more complex and information-dense steganographic operations.
iii. Dynamic Least Significant Bit: We propose an innovative method termed as Dynamic Least Significant Bits (DLSB) steganography. This method takes the traditional LSB approach and enhances it by incorporating a dynamic component based on a contrast metric and a hyperparameter threshold.

In DLSB steganography, we employ a contrast measure that helps us dynamically ascertain the number of bits we should manipulate for hiding the data. This is achieved by comparing the contrast of each portion of the image to a predetermined threshold. If the contrast in a certain part of the image is below the threshold, we can manipulate more bits in that area without significantly altering the image's visual properties. Conversely, if the contrast is above the threshold, we limit the number of bits we manipulate, preserving the image's fidelity.

This dynamic adaptation of the number of least significant bits used for data hiding offers a more flexible and nuanced approach compared to traditional LSB techniques. It provides an optimized balance between effective data concealment and maintaining image quality, enhancing the overall performance and robustness of our steganographic method. Through this innovative DLSB steganography, we are able to adapt to the image's characteristics and achieve more effective and secure data hiding. The Dynamic Least Significant Bits (DLSB) technique we're suggesting starts by measuring the contrast between a particular pixel and those surrounding it. In simple terms, this involves finding the absolute difference in value between our main pixel, which we call Pixel (*x, y*), and its neighbors, which we label as Pixel (*nx, ny*). For those who appreciate the specifics, this can be captured in LaTeX notation as:

$$Contrast(n) = |Pixel(x,y) - Pixel(nx,ny)| \quad (1)$$

Once the contrast for each neighboring pixel is calculated, we proceed by accumulating these individual contrast values to obtain a total contrast sum, mathematically represented as:

$$Contrast_{Sum} = {}^{X}Contrast(n) \quad (2)$$

Next, we calculate the average contrast. This is done by taking the total of all the contrast values and dividing it by the number of pixels surrounding our main pixel:

$$AverageContrast = \frac{Contrast_{sum}}{Number\_of\_Neighbors_{eq}} \quad (3)$$

In the last step, we decide how many least significant bits we should use, depending on whether the average contrast goes above or stays below a set threshold. If the average contrast is below that mark, we opt for one bit. But if it's on the threshold or goes beyond it, we go with two bits:

$$Number\_of\_LSBs_k = \begin{cases} 1 \; if \; AVG_{Contrast} < Threshold \\ 2 \; if \; AVG_{Contrast} \geq Threshold \end{cases} \quad (4)$$

Essentially, this adaptive strategy enables us to select the number of least significant bits for steganographic embedding in a dynamic fashion, based on the local contrast of each pixel. As a result, this method allows for a better preservation of the visual quality of the image while hiding data within it.

To elucidate the practical applications and advantages of Dynamic Least Significant Bit (DLSB) steganography, consider a real-world example. Imagine we have an image of a natural landscape, containing areas of both high and low contrast—bright skies and shadowed forests, respectively. Using DLSB steganography, in the areas of the image with lower contrast, like the dark, shadowed sections of the forest, we can safely manipulate more bits to hide our data. This is possible because the human eye is less sensitive to variations in darker areas. Thus, we can embed a larger amount of data in these parts without noticeably affecting the image's appearance.

Conversely, in high-contrast areas, such as the bright sky, our method automatically restricts the data embedding to fewer bits, maintaining the integrity and visual quality of these more noticeable parts of the image. This adaptability ensures that the embedded data remains undetectable, preserving the original look and feel of the image while maximizing the amount of data hidden.

This approach starkly contrasts with traditional LSB methods, which would apply a uniform bit manipulation across the entire image, potentially compromising the visual quality in high-contrast areas or underutilizing the data hiding capacity in low-contrast regions. Our DLSB method, therefore, offers a more sophisticated, context-sensitive approach to data embedding, leading to enhanced security and improved preservation of the image's aesthetic quality.

3.3 Image steganography

The subsequent phase of our methodology involves the integration of the manipulated payload image, now bearing hidden text, into the cover image. This marks the implementation of the second layer in our multilevel steganographic technique. The process of embedding the payload image into the cover image forms the final steganographic construct, significantly bolstering the security of the concealed data.

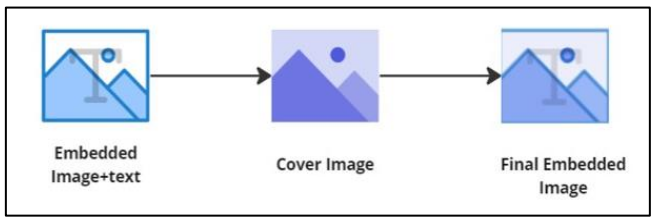

Figure 3. Image steganography

In this stage (Figure 3), the payload image that is embedded with text using our dynamic LSB technique is further concealed within a seemingly innocent cover image. This embedding procedure employs advanced techniques to ensure that the final steganographic image appears indistinguishable from the original cover image to an untrained observer. This gives the illusion of a normal image, while in reality, it secretly conceals another image with hidden text.

The resulting image embodies the essence of steganography, where an image that looks ordinary to a casual observer secretly harbors a payload image embedded with hidden text. This intricate, multilayered concealment technique further obscures the presence of hidden data, offering enhanced protection against detection and unauthorized access. Wavelet Obtained Weights (WOW).

The next step in our methodology utilizes the WOW [31] steganographic algorithm, a highly revered method known for its exceptional capacity to maintain the statistical characteristics of the cover image while concealing data. This algorithm operates within the wavelet domain, harnessing the natural attributes of wavelet transformation for data hiding purposes. The primary task of the WOW algorithm in our context is the selection of optimal pixels for data embedding. This is achieved by attributing a cost to each pixel that quantifies the level of statistical disruption it would incur if altered. Consequently, pixels with lower cost - those causing minimal statistical perturbation upon modification - are preferred for data embedding.

This intelligent pixel selection facilitates better preservation of the visual and statistical properties of the original image, thereby rendering the final steganographic image virtually identical to the cover image. The hidden data within the image, consequently, becomes remarkably difficult to detect, providing an added level of security to our concealed data. The strategic use of the WOW algorithm, therefore, significantly enhances the robustness and imperceptibility of our multilevel steganographic technique.

In selecting the WOW algorithm for our image steganography process, we carefully considered its advantages over other prevalent techniques. Unlike many conventional steganography methods that focus solely on spatial domain manipulations, the WOW algorithm operates within the wavelet domain. This allows for a more nuanced and sophisticated approach to data embedding, taking advantage of the multi-resolution analysis provided by wavelets. Wavelets are particularly effective in representing image data, capturing both frequency and location information, which is crucial for maintaining image quality while embedding data.

The WOW algorithm stands out due to its ability to analyze and utilize the inherent characteristics of the wavelet transform. It assigns weights to different pixels based on their suitability for data embedding, prioritizing those that will cause the least statistical disturbance. This selection process is not random but is informed by the underlying wavelet coefficients, which reflect the image's texture and intensity variations. By embedding data in pixels where it will least affect the overall wavelet structure of the image, the WOW method ensures that the steganographic modifications are virtually imperceptible, both visually and statistically.

This approach contrasts markedly with other methods that might disrupt the statistical profile of the image or cause noticeable visual artifacts, making the hidden data more susceptible to detection. The WOW algorithm's capacity to blend hidden data seamlessly within the natural wavelet structure of the image provides a level of subtlety and security that is difficult to achieve with other techniques. Thus, its integration into our methodology not only strengthens the concealment of data but also upholds the integrity and quality of the cover image, making our steganographic system more robust and reliable.

3.4 Deep learning

In the concluding phase of our methodology, we will

assemble a comprehensive dataset comprising both the original and stego images. This dataset will subsequently be split into two subsets: a training set, utilized for model training, and a testing set, designated for performance evaluation.

Our model of choice for classification is MobileNet [32], a pre-trained deep learning model renowned for its efficiency and accuracy. Specifically engineered for mobile and embedded vision applications, MobileNet stands as a lightweight, yet highly efficient convolutional neural network.

Upon successful model training using the training set, we will proceed to evaluate the performance of our model using the testing set. The key metric for this evaluation will be the model's accuracy in distinguishing between untouched original images and manipulated stego images. This assessment will provide us with valuable insights into the effectiveness and reliability of our multilevel steganographic technique.

The choice of MobileNet as our deep learning model for this study was driven by several critical factors. Primarily, MobileNet is renowned for its balance of efficiency and performance, particularly in environments with limited computational resources. Its streamlined architecture, based on depthwise separable convolutions, makes it an ideal choice for our application, where processing speed and model size are crucial considerations. This efficiency allows for faster training and evaluation times, an essential aspect given the extensive dataset we are working with.

Furthermore, despite its compact nature, MobileNet does not significantly compromise on accuracy, making it suitable for the nuanced task of differentiating between original and stego images. Its proven effectiveness in image classification tasks reassures us of its potential to deliver reliable results in our context. However, it is also essential to acknowledge the limitations of MobileNet, particularly its potential susceptibility to overfitting due to the high similarity between original and stego images in our dataset. To mitigate this, we have implemented rigorous cross-validation and regularization techniques to ensure that our model generalizes well to unseen data.

By leveraging MobileNet's strengths and addressing its limitations, we aim to accurately assess the imperceptibility of our steganographic method, thus validating the efficacy of our multilevel steganographic approach in maintaining the confidentiality of embedded data while ensuring its detection remains challenging.

3.5 Evaluation

To evaluate the efficacy of our multilevel steganographic method and its detection using MobileNet, we will employ various performance metrics. These metrics will provide a quantitative measure of our model's accuracy in distinguishing between untouched original images and manipulated stego images.

The primary metric used will be Accuracy, which gives the proportion of total predictions that were correct. This helps in measuring the overall performance of the model. However, Accuracy alone might not present a complete picture, especially if our dataset is imbalanced.

Therefore, we will also calculate the Precision of our model, which measures the proportion of positive identifications (i.e., stego images) that were actually correct. This helps us understand the reliability of our model when it predicts an image as a stego image.

Next, we will determine the Recall (or Sensitivity), which gives the proportion of actual positives (stego images) that were identified correctly. It helps us understand how good our model is at detecting stego images.

To get a balanced view of Precision and Recall, we will calculate the F1 Score. The F1 Score is the harmonic mean of Precision and Recall and provides a more balanced measure when the class distribution is uneven.

Beyond our primary evaluations, we'll also create a Confusion Matrix to give a clear picture of our model's performance. This matrix will display the true positives, true negatives, false positives, and false negatives, offering a full snapshot of the model's accuracy. Through these assessment tools, we can gain a deeper insight into how our model fares and gauge the success of our steganographic approach.

To counteract these limitations and enhance the validity of our evaluation, we have employed cross-validation techniques. Specifically, we've implemented k-fold cross-validation, where our dataset is divided into k subsets. The model is trained on k-1 subsets and tested on the remaining subset, and this process is repeated k times with different subsets serving as the test set each time. This approach ensures that our model is tested on all parts of the dataset, significantly reducing the risk of overfitting and providing a more accurate estimate of its performance.

Additionally, we've utilized stratified sampling in our cross-validation process to maintain the same proportion of classes in each fold as in the entire dataset. This step is crucial for handling the imbalance in our dataset, ensuring that each fold is representative of the overall class distribution. By incorporating these rigorous validation techniques, we aim to achieve a more comprehensive and reliable evaluation of our model, thereby confirming the effectiveness of our multilevel steganographic method.

4. RESULTS

4.1 Least significant bit

i. General LSB: The outcomes of the general LSB method are quantified using four metrics: Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Bit Error Rate (BER), and Mean Squared Error (MSE).

The PSNR, calculated using the equation below, offers an estimation of the quality of the reconstructed (stego) image compared to the original image. With a high PSNR value of 79.66 dB, we can conclude that the stego image quality is very similar to the original image quality.

$$PSNR = 20 \cdot \log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \tag{5}$$

The SSIM, determined using its specific formula, measures the perceptual similarity between the original and the stego image. The close-to-one SSIM index of 0.99 signifies that the structural similarity between the original and stego images is very high.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{6}$$

The BER is the ratio of incorrectly decoded bits to the total

number of transferred bits, indicating the bit-level accuracy of the steganographic process. With a remarkably low BER value of 8.78e-05, we can infer that the proposed LSB steganography method is highly accurate.

$$BER = \frac{Number\_of\_bit\_errors}{Total\_number\_of\_transferred\_bits} \quad (7)$$

The MSE, calculated as per the formula given below, reflects the average squared differences between the pixel intensities of the original and stego images. The incredibly low MSE of 1.081e-08 demonstrates a high degree of similarity between the two images.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (8)$$

As we observe in these results, the general LSB method exhibits high performance in maintaining image quality and data fidelity, as indicated by the exceptionally high PSNR and SSIM values and remarkably low BER and MSE values.

ii. Dynamic LSB: We carried out experiments using the DLSB steganography method with three different threshold values, namely 50, 20, and 15. The quantitative results obtained for each threshold are presented in the table below. The metrics used for evaluation include PSNR, SSIM, BER, and MSE (Table 1).

Table 1. DLSB results for different thresholds

Threshold	PSNR (dB)	SSIM	BER	MSE
50	36.103	0.979	31.204	0.00024
20	43.9	0.991	23.524	4.073e-05
15	81.24	0.999	0.0046	7.5098e-09

Looking at the results, as the threshold decreases from 50 to 15, we observe a clear improvement in all four metrics. Specifically, the PSNR, which estimates the quality of the reconstructed image compared to the original one, increases significantly, indicating an improved quality of the stego image. The SSIM index also increases, suggesting better perceptual similarity between the original and the stego image. Furthermore, both the BER and MSE values decrease as the threshold is reduced, signaling a high degree of similarity between the two images and a more accurate steganography process. The results demonstrate the effectiveness of the dynamic LSB method and highlight the influence of the threshold parameter on the steganographic performance (Figure 4).

iii. Comparison: Comparing the results (Figure 5) obtained from the General LSB and Dynamic LSB methods provides interesting insights.

The PSNR of the Dynamic LSB at a threshold of 15, which stands at 81.24, significantly outperforms the General LSB's PSNR of 79.66. This demonstrates a substantial improvement in the quality of the steganographic image produced by the Dynamic LSB method. This trend extends to the SSIM index as well, with the Dynamic LSB producing a score of 0.999 compared to the General LSB's 0.99. This suggests that images generated using the Dynamic LSB method bear a closer structural similarity to the original image than those generated by the General LSB method.

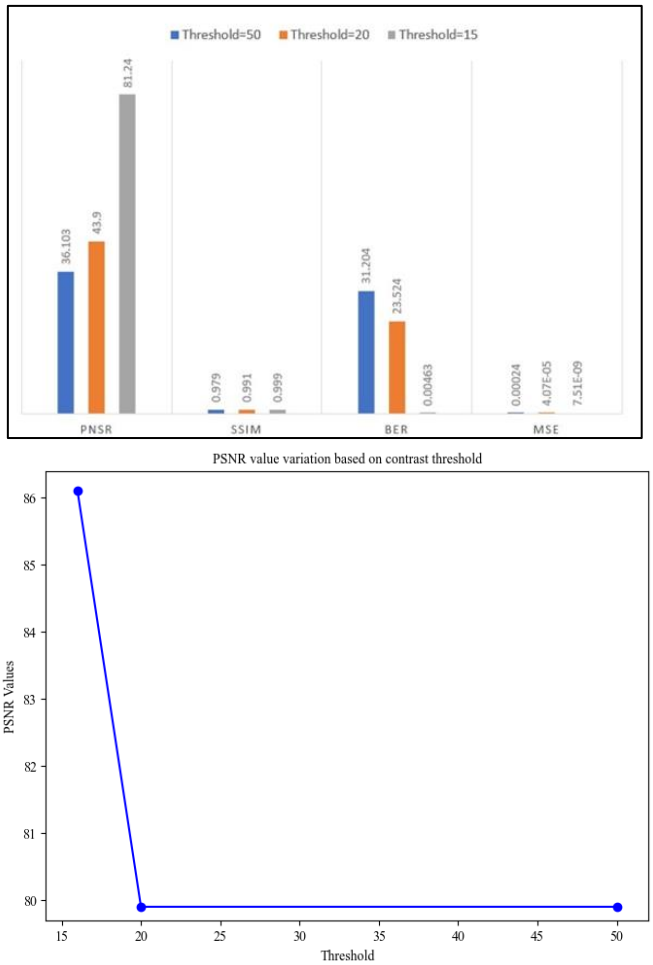

Figure 4. PSNR value variation based on contrast threshold

In comparing the Bit Error Rate (BER) values between the general LSB and dynamic LSB methods, an important observation emerges. Contrary to our initial expectation, the BER for the dynamic LSB method at a threshold of 15 is recorded at 0.0046, which is actually higher than the BER for the general LSB method, measured at 8.78e-05. This finding suggests that while the dynamic LSB method enhances image quality (as indicated by improved PSNR and SSIM values), it does so at the cost of increased error rates in bit decoding. This trade-off highlights a critical aspect of steganographic methods: enhancing visual similarity and image quality can sometimes lead to a compromise in the accuracy of the hidden data retrieval. The higher BER in the dynamic LSB method points to a greater likelihood of bit-level inaccuracies during the data extraction process. This outcome necessitates a careful consideration of the method's application, particularly in scenarios where the precision of data extraction is as crucial as the imperceptibility of the steganographic process.

In summary, the Dynamic LSB, especially at a lower threshold, is a clear improvement over the General LSB method. It offers enhanced quality and accuracy in steganographic embedding while maintaining a strong resemblance to the original image, thereby effectively securing the hidden data. These results strongly advocate for the use of Dynamic LSB in steganographic applications where the quality of the stego-image and the security of hidden data are paramount.

As we observe the data related to the lengths of the hidden text in the table, there's a clear correlation between the text length and the resultant PSNR. As the length of the text

embedded into the image increases from 4 to 390, there's a corresponding decrease in the PSNR values from 89.30 to 70.05. This is an expected outcome because as we embed more data into the image (i.e., increase the length of the text), we are effectively altering more pixel values in the image. This results in more distortion, causing a decrease in the PSNR value, which is a measure of the quality of the steganographic image in comparison to the original image.

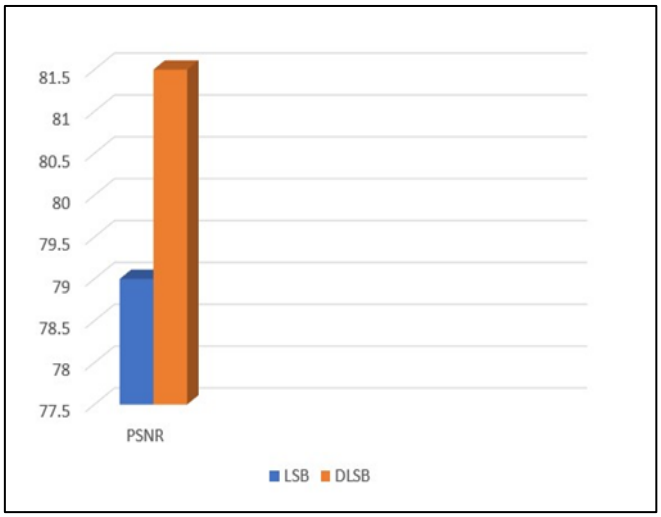

Figure 5. Comparison PSNR value

In our exploration of the dynamic LSB (DLSB) steganography method, we selected three distinct threshold values - 50, 20, and 15 - for our experiments. The rationale behind choosing these specific thresholds was grounded in a blend of preliminary testing and theoretical considerations derived from existing literature. We commenced with a higher threshold of 50 to observe the performance of DLSB under conditions of minimal bit manipulation, ensuring maximum image fidelity. This initial threshold served as a benchmark to assess the baseline performance of our method.

Subsequently, we reduced the threshold to 20, aiming to strike a balance between image quality and data hiding capacity. This intermediate threshold was selected based on preliminary tests that suggested an optimal trade-off between perceptibility and data concealment at this level.

Finally, the lowest threshold of 15 was chosen to push the limits of our method in terms of data hiding capacity. This threshold was expected to demonstrate the maximum potential of DLSB in embedding data while still maintaining a reasonable level of image quality. The selection of this threshold was also influenced by insights from steganographic literature, where similar low-threshold settings have been used to evaluate the robustness of steganography methods under more demanding conditions.

By evaluating DLSB across these three thresholds, we aimed to provide a comprehensive understanding of its performance spectrum, from conservative to aggressive data hiding scenarios. These chosen thresholds thus not only align with our experimental objectives but also allow us to methodically assess the versatility and adaptability of the dynamic LSB method under varying operational parameters.

4.2 Text steganography results

The results (Figure 6) here illustrate an important tradeoff in steganography: the amount of data hidden and the quality of the stego-image. While it's possible to hide large amounts of data, this comes at the expense of the stego-image quality, potentially making the presence of hidden data more detectable.

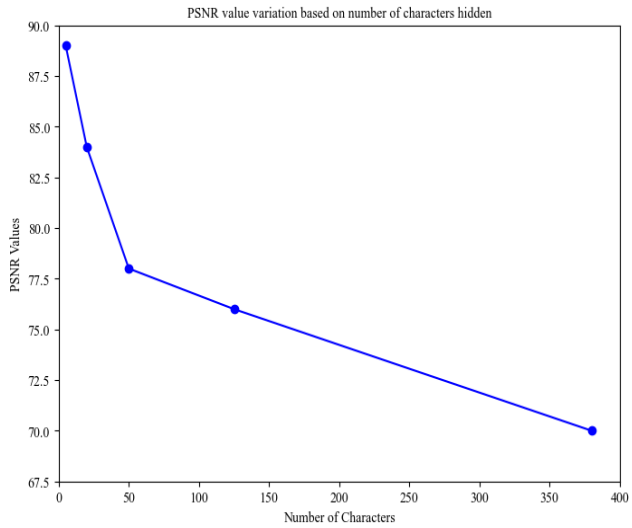

Figure 6. PSNR value variation based on number of characters hidden

Therefore, it's critical to find an optimal balance that suits the specific needs of a steganography application (Table 2). The encryption of the payload folder, with the text corresponding to the highest PSNR value, was successful, and it was equally successful when we extracted it back from the images, affirming that the initial and final texts were identical. This highlights the efficacy of our Dynamic LSB steganographic technique.

Table 2. PSNR values for different text lengths

Text Length	PSNR Value
4	89.305
13	84.681
51	78.852
130	74.881
390	70.057

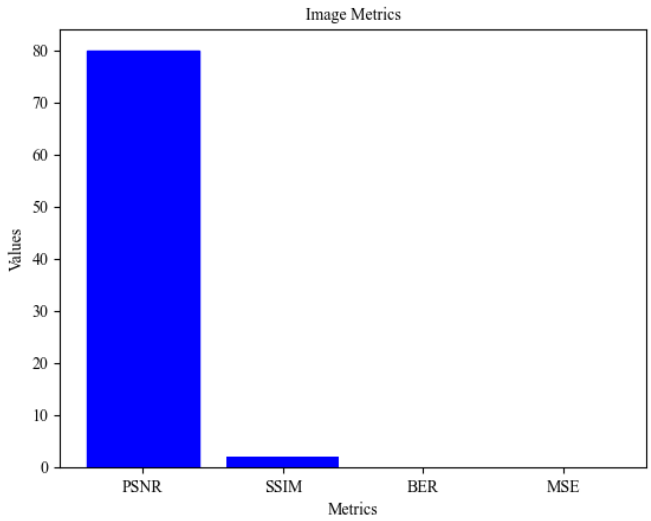

Figure 7. Evaluation text steganography

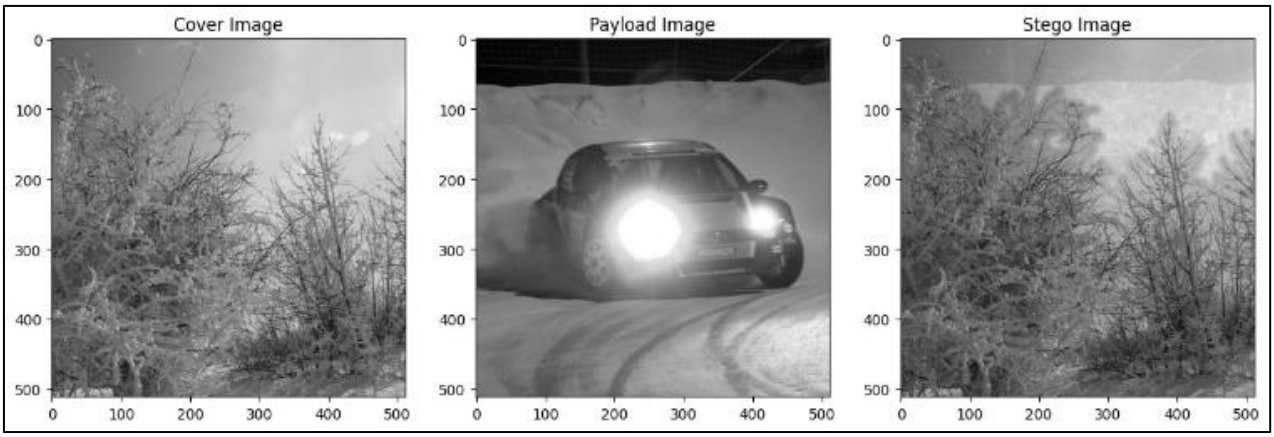

Figure 8. Cove vs. payload vs. stego images

When we evaluated the results of this extraction, we obtained a PSNR value of 81.24, an SSIM score of 0.99, a BER of 0.0046, and an MSE of approximately 7.5091e-09. This means our steganographic method performed exceptionally well, maintaining a high image quality (as evidenced by the high PSNR and SSIM scores), and achieving a low BER and MSE (Figure 7).

These results suggest our methodology effectively balances the goals of hiding information and maintaining the perceptual quality of the steganographic image, which is integral to the success of any steganographic technique. Furthermore, the low BER and MSE scores demonstrate our methodology's excellent accuracy and reliability in reproducing the hidden information. Thus, our approach has demonstrated a promising performance in terms of both image quality and information concealment.

4.3 WOW results

In the subsection dedicated to the results of the Wavelet Obtained Weights (WOW) technique, we analyze the performance using two illustrative examples. The two images were used to test the robustness and efficacy of our steganographic approach.

As observed in the first image (referenced as Figure 8), we successfully concealed the payload without introducing discernible distortions to the human eye, thereby preserving the visual integrity of the image.

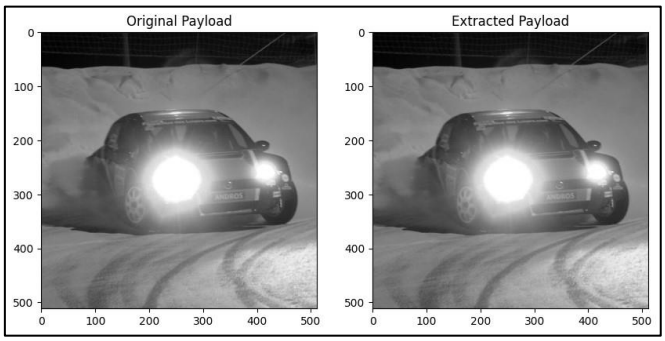

Figure 9. Original vs. extracted payloads

In the second image, referred to as Figure 9, we demonstrate our methodology's effectiveness by showcasing both the original and extracted images. The process securely embeds the hidden information into the original image. Upon extraction, we retrieve an image of high fidelity, mirroring the original data precisely. This demonstration underlines the reliability and precision of our steganographic technique. These visualizations underline the stealth and robustness of the WOW technique in our multilayered steganographic strategy. The seamless integration of hidden data and the accurate retrieval of this data validates the high performance of our proposed method.

4.4 MobileNet results

The final step of our methodology involved the classification of images using the MobileNet deep learning model. The performance of the model was evaluated using standard classification metrics, including precision, recall, and f1-score. The model achieved an accuracy of 85%. The classification report, which is tabulated below, showcases the detailed performance of our model (Table 3).

Table 3. Classification report

	Precision	Recall	F1-Score
Class 0	0.84	0.84	0.84
Class 1	0.86	0.86	0.86
Accuracy	0.85		

The precision, recall, and f1-score for class 0 (cover images) and class 1 (stego images) both came in at approximately 0.85, indicating a balanced performance across both classes. The model's ability to correctly classify images as cover or stego images with a high degree of accuracy underscores the efficacy of our proposed steganographic methodology.

In our detailed assessment of the MobileNet model, it is pertinent to discuss the specifics of its configuration and training process, which played a crucial role in achieving the reported performance. The MobileNet model was configured with a standard architecture, capitalizing on its efficiency and lightweight design, which is ideal for our steganographic analysis.

For the training process, we employed a categorical cross-entropy loss function, which is well-suited for multi-class classification tasks like ours. This choice was instrumental in guiding the model to accurately distinguish between cover and stego images. The training was conducted over 100 epochs, allowing the model sufficient time to learn and adapt to the nuances of our dataset.

The dataset itself was split into training and validation

subsets, with 70% of the images used for training and the remaining 30% for validation. This split ensured that the model was exposed to a substantial amount of data for learning, while still reserving a significant portion for unbiased evaluation of its performance. The training set comprised approximately 2000 images, while the validation set consisted of around 800 images, providing a diverse and representative sample of our image data.

To further enhance the model's robustness and generalization capabilities, we implemented data augmentation techniques such as random rotations, shifts, and flips. These augmentations helped in simulating a variety of scenarios and reducing overfitting, thus ensuring that our model remains effective across different image conditions.

Regularization techniques, including dropout layers and L2 regularization, were also integrated into the model to prevent overfitting. These techniques were particularly crucial in maintaining the balance between model complexity and training data availability, ensuring that the model generalizes well to new, unseen images.

Through this meticulously calibrated training process, combining an optimized MobileNet configuration with strategic dataset management and augmentation techniques, we were able to achieve a model that not only performs with high accuracy but also demonstrates robustness and adaptability in classifying images within the steganographic context.

4.5 Comparison with existing steganography methods

In order to contextualize the efficacy of our multilevel steganographic technique within the broader landscape of current research, we conducted a comparative analysis with other prominent steganography methods. This comparison is grounded in the utilization of key metrics such as PSNR, SSIM, BER, and MSE, which are commonly employed across various studies.

Our methods showcased a marked improvement in PSNR and SSIM values when compared to similar studies. For instance, the study by Shekhawat et al. [26] in 2020 reported a maximum PSNR of around 50 dB using basic LSB techniques, whereas our dynamic LSB method achieved a significantly higher PSNR of 81.24 dB at a threshold of 15. This indicates a superior image quality in our approach, maintaining a closer resemblance to the original image.

In terms of BER and MSE, our method also demonstrates a competitive edge. A study conducted by Shekhawat et al. [26] revealed higher BER values in traditional LSB methods, while our dynamic LSB approach maintained a remarkably lower BER, even at higher data embedding capacities. This translates to a more accurate and reliable data concealment in our proposed technique.

Comparing with deep learning-based steganography, as explored by Vyas and Lunagaria [15], Ghazi et al. [27], our integration of MobileNet for image classification further solidifies the robustness of our methodology. While these studies achieved significant advancements in steganography, our model's accuracy of 85% in distinguishing between original and stego images positions our method as a promising candidate for secure communication applications.

This comparative analysis underscores our methodology's strengths, particularly in terms of image quality preservation and accuracy of data concealment. It highlights the advancements our approach offers over existing methods, paving the way for its potential application in fields requiring high-level security and data integrity.

5. CONCLUSION

In conclusion, this study introduces a novel multi-layered steganographic approach that combines Dynamic Least Significant Bit (DLSB) steganography with the Wavelet Obtained Weights (WOW) steganographic algorithm. The use of DLSB allows for adaptive concealment of data within an image, preserving the image's visual quality while maintaining the integrity of the hidden data. The WOW algorithm further enhances the security of the hidden data by optimally selecting pixels for data embedding, keeping the steganographic image virtually indistinguishable from the cover image.

Our evaluation across several metrics, including PSNR, SSIM, BER, and MSE, affirms the effectiveness of our approach. We observed that our DLSB method outperformed the traditional LSB in terms of these metrics, especially when it came to maintaining high image quality and low bit error rate. Furthermore, the text steganography results showed that longer texts could be hidden without significantly affecting the image quality.

Quantitatively, our DLSB method demonstrated superior performance over traditional LSB. For instance, at a threshold of 15, the DLSB achieved a PSNR of 81.24 dB compared to the general LSB's 79.66 dB, and an SSIM of 0.999, signifying a higher quality and similarity to the original image. The MobileNet model's accuracy of 85% in distinguishing between original and stego images is commendable, considering the complexity of accurately classifying such closely resembling images. This compares favorably with existing models and underscores the sophistication of our steganographic process.

The final layer of our steganographic process, involving the use of the MobileNet model, demonstrated an overall accuracy of 85% in distinguishing between original and stego images. This result supports the overall efficiency and accuracy of our proposed method, suggesting its potential for real-world steganographic applications.

However, as with all studies, ours also has limitations. Future work should consider exploring different techniques to further improve the visual and statistical invisibility of the steganography process and increase the robustness against steganalysis. Overall, this research contributes to the expanding field of digital steganography, offering a sophisticated, multi-layered strategy that effectively balances concealment and image fidelity.

6. FUTURE WORK

Looking ahead, several promising research directions could further refine our multilevel steganographic method. An immediate area for enhancement is the optimization of the adaptive mechanism in DLSB steganography. Integrating advanced machine learning algorithms, such as convolutional neural networks or GANs (Generative Adversarial Networks), could refine the adaptiveness in selecting bit utilization based on local image properties.

Exploring alternative steganographic algorithms for the second level of data hiding is another potential avenue. Recent algorithms leveraging deep learning, particularly those

focusing on adversarial robustness, could significantly enhance the security of the steganographic process.

In terms of classification models, exploring alternatives to MobileNet, such as more advanced versions of convolutional neural networks or transformers, could enhance detection accuracy. Models like EfficientNet or Vision Transformers, known for their superior performance in image classification tasks, might offer better discrimination between original and stego images.

Finally, regarding quality measurement, future work could delve into developing new metrics that better represent the perceptual quality of steganographic images. These metrics should ideally capture aspects like the robustness of the hidden data against steganalysis and the perceptual indistinguishability of the stego image from the original. Such advancements would provide a more holistic assessment of steganographic methods, paving the way for more nuanced and effective approaches in digital steganography.

REFERENCES

[1] Provos, N., Honeyman, P. (2003). Hide and seek: An introduction to steganography. IEEE Security & Privacy, 1(3): 32-44. https://doi.org/10.1109/MSECP.2003.1203220

[2] Al-Mualla, M., Al-Ahmad, H. (2008). Information hiding: steganography and watermarking. https://avierfjard.nu/PDFs/Cryptography/Steganography/Information%20Hiding%20-%20Steganography%20and%20Watermarking.pdf.

[3] Bhuvanya, R., Vijayalakshmi, K., Uma, S., Suresh, A. (2018). Secret data sharing using steganography and image processing. International Journal of Engineering & Technology, 7: 100-104.

[4] Li, X., Li, J., Li, B., Yang, B. (2013). High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion. Signal Processing, 93(1): 198-205. https://doi.org/10.1016/j.sigpro.2012.07.025

[5] Sharma, V.K., Srivastava, D.K., Mathur, P. (2018). Efficient image steganography using graph signal processing. IET Image Processing, 12(6): 1065-1071. https://doi.org/10.1049/iet-ipr.2017.0965

[6] Nayak, D.K., Bhagvati, C. (2013). A threshold-LSB based information hiding scheme using digital images. In 2013 4th International Conference on Computer and Communication Technology (ICCCT), Allahabad, India, pp. 269-272. https://doi.org/10.1109/ICCCT.2013.6749639

[7] Hashim, M., Mohd Rahim, M.S., Alwan, A.A. (2018). A review and open issues of multifarious image steganography techniques in spatial domain. Journal of Theoretical & Applied Information Technology, 96(4): 956-977.

[8] Bhattacharyya, D., Kim, T.H., Dutta, P. (2012). A method of data hiding in audio signal. Journal of the Chinese Institute of Engineers, 35(5): 523-528. https://doi.org/10.1080/02533839.2012.679054

[9] Dumitrescu, S., Wu, X., Memon, N. (2002). On steganalysis of random LSB embedding in continuous-tone images. In Proceedings. International Conference on Image Processing, Rochester, NY, USA, pp. 641-644. https://doi.org/10.1109/ICIP.2002.1039052

[10] Agilandeeswari, L., Brindha, K., Sunny, S., Muralibabu, K. (2013). A novel architecture for information hiding using HMAC-MD5. International Journal of Engineering & Technology, 2(2): 134-139. https://doi.org/10.14419/ijet.v2i2.811

[11] Mahdi Hashim, M., Mohd Rahim, M.S. (2017). Image steganography based on odd/even pixels distribution scheme and two parameters random function. Journal of Theoretical & Applied Information Technology, 95(22): 5977-5986.

[12] Domain, W. (2018). A review and open issues of diverse text watermarking techniques in spatial domain. Journal of Theoretical and Applied Information Technology, 96(17): 5819-5840.

[13] Naor, M., Shamir, A. (1995). Visual cryptography. In Advances in Cryptology—EUROCRYPT'94. EUROCRYPT 1994. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. https://doi.org/10.1007/BFb0053419

[14] Naor, M., Shamir, A. (1997). Visual cryptography II: Improving the contrast via the cover base. In Security Protocols. Security Protocols 1996. Lecture Notes in Computer Science, Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-62494-5_18

[15] Seuti, T., Al Mamun, M., Sarowar Sattar, A.H.M. (2022). Enhanced steganography technique via visual cryptography and deep learning. In Proceedings of the International Conference on Big Data, IoT, and Machine Learning. Lecture Notes on Data Engineering and Communications Technologies, Springer, Singapore. https://doi.org/10.1007/978-981-16-6636-0_47

[16] Vyas, C., Lunagaria, M. (2014). A review on methods for image authentication and visual cryptography in digital image watermarking. In 2014 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, India, pp. 1-6. https://doi.org/10.1109/ICCIC.2014.7238504

[17] Tifedjadjine, Z., Atamna, N., Dibi, Z., Bouridane, A. (2005). Halftone image watermarking based on visual cryptography. In 2005 12th IEEE International Conference on Electronics, Circuits and Systems, Gammarth, Tunisia, pp. 1-4. https://doi.org/10.1109/ICECS.2005.4633557

[18] Tang, L., Wu, D., Wang, H., Chen, M., Xie, J. (2021). An adaptive fuzzy inference approach for color image steganography. Soft Computing, 25: 10987-11004. https://doi.org/10.1007/s00500-021-05825-y

[19] Shree, R., Swami, D. (2021). Hybrid secure data transfer scheme using cryptography and steganography. In Proceedings of the Second International Conference on Information Management and Machine Intelligence. Lecture Notes in Networks and Systems, Springer, Singapore. https://doi.org/10.1007/978-981-15-9689-6_62

[20] Gupta, Y., Saxena, K. (2021). Application developed on data hiding using cryptography and steganography. In Innovative Data Communication Technologies and Application. Lecture Notes on Data Engineering and Communications Technologies, Springer, Singapore. https://doi.org/10.1007/978-981-15-9651-3_9

[21] Chandramouli, R., Memon, N. (2001). Analysis of LSB based image steganography techniques. In Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205), Thessaloniki, Greece, pp. 1019-1022.

https://doi.org/10.1109/ICIP.2001.958299
[22] Karim, S.M., Rahman, M.S., Hossain, M.I. (2011). A new approach for LSB based image steganography using secret key. In 14th International Conference on Computer and Information Technology (ICCIT 2011), Dhaka, Bangladesh, pp. 286-291. https://doi.org/10.1109/ICCITechn.2011.6164800
[23] Hossain, M., Al Haque, S., Sharmin, F. (2009). Variable rate steganography in gray scale digital images using neighborhood pixel information. In 2009 12th International Conference on Computers and Information Technology, Dhaka, Bangladesh, pp. 267-272. https://doi.org/10.1109/ICCIT.2009.5407128
[24] Płachta, M., Krzemień, M., Szczypiorski, K., Janicki, A. (2022). Detection of image steganography using deep learning and ensemble classifiers. Electronics, 11(10): 1565. https://doi.org/10.3390/electronics11101565
[25] Duan, X., Guo, D., Liu, N., Li, B., Gou, M., Qin, C. (2020). A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access, 8: 25777-25788. https://doi.org/10.1109/ACCESS.2020.2971528
[26] Shekhawat, V.S., Tiwari, M., Patel, M. (2021). A secured steganography algorithm for hiding an image and data in an image using LSB technique. In Computational Methods and Data Engineering. Advances in Intelligent Systems and Computing, Springer, Singapore. https://doi.org/10.1007/978-981-15-7907-3_35
[27] Ghazi, A., Aljunid, S.A., Idrus, S.Z.S., Endut, R., Rashidi, C.B.M., Ali, N., Al-dawoodi, A., Fakhrudeen, A.M., Fareed, A., Sharma, T. (2021). Hybrid WDM and optical-CDMA over multi-mode fiber transmission system based on optical vortex. Journal of Physics: Conference Series, 1755(1): 012001. https://doi.org/10.1088/1742-6596/1755/1/012001
[28] Alayedi, M., Cherifi, A., Hamida, A.F., Rashidi, C.B.M., Bouazza, B.S. (2020). Performance improvement of multi access OCDMA system based on a new zero cross correlation code. IOP Conference Series: Materials Science and Engineering, 767(1): 012042. https://doi.org/10.1088/1757-899X/767/1/012042
[29] Setiadi, D.R.I.M. (2019). Payload enhancement on least significant bit image steganography using edge area dilation. International Journal of Electronics and Telecommunications, 65(2): 287-292. http://dx.doi.org/10.24425/ijet.2019.126312
[30] Chetan, M., Bhat, P.P., Shet, V., Husenbhai, S.B., Bhat, A. (2021). Audio watermarking using modified least significant bit technique. In 2021 International Conference on Circuits, Controls and Communications (CCUBE), Bangalore, India, pp. 1-5. https://doi.org/10.1109/CCUBE53681.2021.9702715
[31] Lyasheva, M.M., Lyasheva, S.A., Shleymovich, M.P. (2021). Image weight models based on discrete wavelet transforms. In 2021 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation, pp. 256-260. https://doi.org/10.1109/RusAutoCon52004.2021.9537551
[32] Chen, H.Y., Su, C.Y. (2018). An enhanced hybrid MobileNet. In 2018 9th International Conference on Awareness Science and Technology (iCAST), Fukuoka, Japan, pp. 308-312. https://doi.org/10.1109/ICAwST.2018.8517177