SEMARAK ILMU PUBLISHING

Journal of Advanced Research in Applied Sciences and Engineering Technology

Journal homepage:
https://semarakilmu.com.my/journals/index.php/applied_sciences_eng_tech/index
ISSN: 2462-1943

A Modified Lsb Image Steganography Method Using Msb-Based Pixel Filtering Algorithm

Sheikh Thanbir Alam[1,2], Md. Maruf Hassan[1,2,*], R. Badlishah Ahmad[2,3], Naimah Yaakob[2,3], Munira Tabassum Mou[1], Ong Bi Lynn[2,3], Nur Farhan Kahar[2,3]

[1] Department of Software Engineering, Daffodil International University, Dhaka, Bangladesh
[2] Department Faculty of Electronic Engineering & Technology, Universiti Malaysia Perlis, Arau, 02600, Perlis, Malaysia
[3] Centre of Excellence for Advanced Computing (ADVCOMP), Universiti Malaysia Perlis, Arau, 02600, Perlis, Malaysia

ABSTRACT

Data is one of the most crucial resources for organizations today, and it must be safeguarded against the increasing threats in cybersecurity. Furthermore, information is often intercepted and altered when transmitted online, which necessitates robust protective measures. Thereupon, to strengthen safety when broadcasting, aside from the two accessible ways, one is cryptography, and the second is steganography. In the cryptography system, info is programmed to cryptogram text by non-public key, yet the data's corporeality is apparent to others, regardless of how impenetrable they are. Meanwhile, steganography hides private data in a common confidential file to escape eye recognition. This study offered a unique information-concealing approach leveraging Least Significant Bit (LSB) image steganography, in which concealed data employs only user-selected picture elements. On the contrary, image element info is employed to strain the complete picture to find the seeker image element, and a stoner-defined word is utilized to protect the LSB steganography. To enhance safety, the XOR scheme secures confidential information, and the AES system encrypts the text before steganography. In the case study, quality metrics are multiplied to evaluate the Stego Image (SI). The SI shows improved Peak Signal Noise Ratio and lower Mean Square Error, indicating the robustness of the recommended scheme compared to other methods.

Keywords:
LSB; AES; XOR; image steganography; MSB pixel filtering

1. Introduction

The exponential progress of cyberspace use in the modern period has emerged as a distinguishing feature. The security of online interactions and communication is a crucial area that receives much attention in the modern environment. People interact with one another in various situations in a socially oriented society. Notably, every individual has a unique communication style; occasionally, disclosing sensitive information to a certain recipient becomes vital. However, it is not always easy and might be a cause for worry when guaranteeing the safe and secure delivery of information to the intended destination. Thus, to maintain honest communication, it has become necessary to hide

* *Corresponding author.*
E-mail address: ancssf@gmail.com

https://doi.org/10.37934/araset.62.1.3248

information. Due to this, implementing information encryption has become crucial for creating safe communication routes between organizations.

The most popular form of information encryption has evolved, and that is cryptography. However, it is essential to note that cryptography may be insufficient to guarantee total security, as the sheer existence of encrypted information might invite skepticism and inference. Steganography, on the other hand, uses a cover medium to covertly envelop confidential communication. This procedure ensures that the transmission is still visibly undetectable. In addition, steganography's capacity to mask information inside a cover medium, making it nearly invisible to anybody other than the intended receiver, is a key benefit it offers. This approach has the unique ability to provide high degrees of security, often going beyond what encryption by itself can do.

In an age when digital information is continuously in danger of unwanted access and cyberattacks, the necessity of robust information security cannot be stressed enough. As accurately pointed out, cryptography has been the cornerstone of information encryption for decades. It has grown and adapted to the ever-changing world of technology, becoming the standard for safeguarding data in transit and at rest. However, despite its efficiency, encryption is not a silver bullet. The sheer existence of encrypted data might draw attention and suspicion, perhaps inciting efforts to crack the encryption. In rare situations, competent attackers may even succeed in decrypting the material. Accordingly, this vulnerability has pushed the quest for alternate means of securing sensitive data. This is when steganography comes into play.

Steganography is a creative and innovative methodology that goes beyond typical encryption methods. Instead of depending exclusively on mathematical techniques to jumble information, it uses the principle of concealing data under an apparently harmless cover medium. This concealment is performed in such a manner that, to the untrained sight, the presence of any concealed information is essentially unnoticeable. Note that the capacity of steganography to disguise information into the very fabric of a cover medium is its distinguishing strength. It provides an extra degree of protection, making it very difficult for prying eyes to notice a concealed message. In essence, it provides a clandestine route of communication that functions directly under the nose of possible eavesdroppers.

Steganography's unique value resides in its ability to complement and improve standard encryption technologies. By integrating these strategies, companies and individuals may construct a security plan that is significantly more resilient. While encryption protects the security of the information, steganography adds an element of concealment that is, in many situations, unequaled. As we discussed the complicated realm of digital security, the union of cryptography and steganography provides a tremendous synergy. It is the confluence of mathematics and art, guaranteeing that our information stays both secret and covert, defending against not just brute-force assaults but also the prying eyes of those who may be inclined to dig into our most intimate interactions. In an age when data is a valued asset, this cooperation is the key to safeguarding the purity of our digital lives.

Steganography works by disguising a message's real content such that it blends in with the original cover medium. This trait effectively prevents unauthorized access since it stops intruders from speculating that clandestine communication is occurring. Note that this technology is based on transferring information over a covert route while enclosing sensitive information. In summary, steganography proves to be a potent technology that works well in conjunction with encryption techniques. As such, sensitive information is kept secure from prying eyes by completely obscuring communication's presence. This technology uses a confidential channel to function, effectively protecting the privacy of sent information.

The realm of steganography encompasses a wide array of potential mediums, as demonstrated in Figure 1. This encompassing assortment of techniques enables the concealment of sensitive data within various carrier media, such as images, audio, text, and videos. Among these options, images emerge as a particularly versatile and adaptable means of safeguarding confidential information. Therefore, it is essential to recognize that human visual perception is more attuned to detecting changes in brightness (luminance) rather than color (chrominance). This intrinsic sensitivity to luminance variations forms the foundation for steganography's effectiveness. Steganography leverages this fundamental aspect of human vision to operate discreetly, ensuring that concealed elements within images remain imperceptible to the human eye. In addition, the choice of images as a carrier medium for steganography is not arbitrary but strategic. Thus, by aligning with the inherent characteristics of human vision, steganography maximizes its concealment capabilities, making it a powerful tool for securing confidential data.

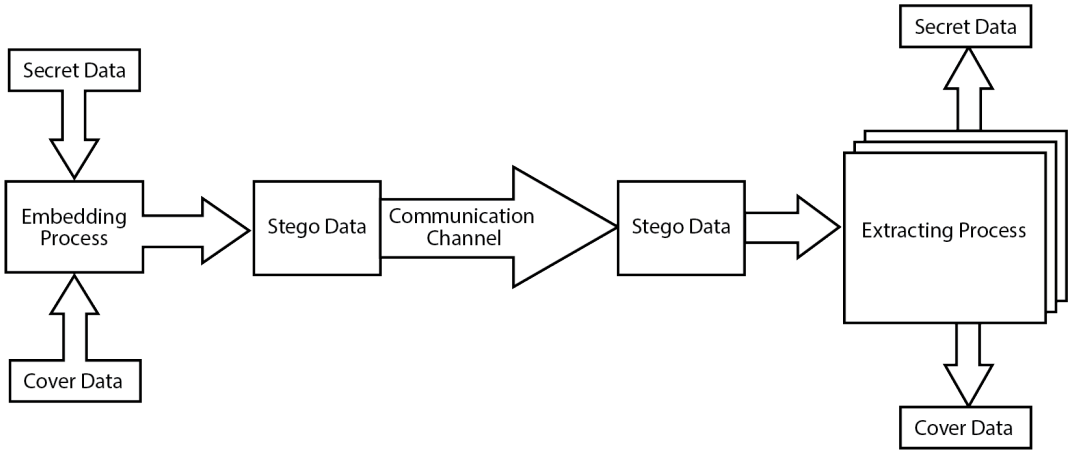


Fig. 1. Steganography block diagram in general

A color picture has been selected as the cover carrier, which is 24-bit for this publication. Systems for hiding information in images may be divided into two primary categories: frequency and spatial. The frequency domain method changes the picture into a new domain by performing mathematical operations on the cover image. Meanwhile, the cover picture is directly altered using the spatial domain approach. The LSB approach, denoted as the Least Significant Bit (LSB), is an extensively used and simple spatial domain process [1]. At the same time, the confidential message's bits are substituted for the picture pixel's LSB in LSB steganography.

Non-filtering and filtering LSB steganography are two separate subtypes. Each pixel of the picture is used in the non-filtering approach to hide critical information. On the other hand, the filtering process carefully selects pixels for steganography while considering the image's quality. This decision ensures that the picked pixels do not degrade the image's visual quality. The work uses LSB filtering picture steganography, which entails carefully selecting certain pixels to insert.

Nevertheless, steganography alone may not provide total protection for sensitive information. Advanced AES encryption technology is used with the recommended steganography technique to increase security [2, 3]. In this study, a user-defined word is included as an enhancement to the traditional LSB approach. Instead of merely changing the LSB of an image pixel, the suggested approach uses logical operations that affect both message bits and word bits. Additionally, an evaluation of the complete picture is performed at the pre-processing step to choose the best pixels to employ for the steganography method. The subsequent is a summary of this manuscript's main contribution.

i. The system uses an improved and tailored pixel filtering method that dynamically adjusts to each unique picture. As a result, there is no way to identify which image pixels are being utilized to conceal private messages.
ii. The recommended solution employs the XOR mathematical operation to integrate the relevant bit rather than explicitly switching LSB bits.
iii. The technique leverages the AES technology for cryptography prior to embedding the confidential information message into the image for better security precautions.

The rest of this article has been fragmented into the following sections. The related work of video steganography is discussed in section two. Section three provides a complete description of the architecture of our suggested approach. The projected technique benefits the two-level security by combining cryptographic algorithm and steganography with the use of random frame selection to LSB-based embed confidential information in the defined pixels. Additionally, the chapter discusses the phases of our method. Section four will confer the findings of our experimental work and provide a comprehensive analysis of the performance assessment criteria especially used in the steganography scheme. We also conduct a comparative study by contrasting our strategy with several different techniques. The last part of this paper summarizes our conclusions and key learnings from the study we conducted.

2. Related Works

There are several approaches that use steganography with various cover medium types. A method that merges visual steganography with digital encoding was proposed by Islam *et al.,* [3]. The authors employed the AES encryption technology to encode the hidden message prior to inserting it into the image. They also utilized a filtering approach in which not every pixel in the picture was used to hide information. Meanwhile, in order to safeguard private communication, Mukhedkar *et al.,* [4] suggested a method that combines information encoding with picture concealment. They used the Blowfish Algorithm for picture encryption and hid information bits in the LSB position. At the same time, in a technique provided by Singh *et al.,* [5], information was concealed by applying the LSB approach and hiding it in non-adjacent pixel locations within the selected picture. This made it impossible for attackers to find any hidden information bits on the borders of images. In addition, Joshi and Yadav [6] proposed a unique method that used grayscale pictures for both spatial domain image steganography and cryptography. They encrypted the message using the Vernam cipher method, and then, after performing the left shift and XOR operations, they placed the ciphered information in LSB bit locations. A measurement-based LSB steganographic strategy centered on pixel values was investigated by Li *et al.,* [7].

A Rubik's cube-based picture encryption technique was developed by Loukhaoukha *et al.,* [8]. Establishing a precise connection between the original and ciphered pictures is challenging due to the XOR operations they conducted after scrambling the image. A text format stenography technique was proposed by Majeed *et al.,* [9]. Meanwhile, Ghosal [10] used a technique that counted the red channel's 1s and 0s and hid bits according to their contrast. Kaur *et al.,* [11] proposed a strategy that utilized Lempel–Ziv–Welch (LZW) compression for information optimization and the higher LSB bit for information concealment. Prior to implementing LSB image steganography, Ren-Er *et al.,* [12] employed the Data Encryption Standard (DES) encryption technique for private information. A steganography method employing grayscale and Red, Green, and Blue (RGB) cover pictures and image encryption discovered that the square block concept was recommended [13]. Steganography and cryptography were merged by Phadte and Dhanaraj [14], who used chaotic encryption for the stego picture.

In order to evade information loss throughout the conversion of RGB color space to YCbCr color space, Broda *et al.,* [15] projected a scheme that used an image color prototypical to conceal information as text. With Caesar cipher encryption first, Charan *et al.,*'s [16] proposal for an LSB replacement technique to conceal information in color photographs. Segmentation and information concealing were integrated by Sulaiman and Khalaf [17], who used two RGB frequencies to store hidden information. For grayscale picture steganography, Emad *et al.,* [18] suggested using Integer Wavelet Transform (IWT). Artificial Neural Networks (ANN) and LSB systems were employed by Deeba *et al.,* [19] for digital watermarking, embedding a hidden picture using the LSB method and displaying it using ANN. Furthermore, Alam *et al.,* [20] presented an 8-directional pixel selection method for embedding confidential information. Meanwhile, Bhuiyan *et al.,* [21] presented a data-hiding method in image steganography to address security issues with the LSB replacement technique. Employing XOR operation with the seventh bit of RGB components and embedding the output within the eighth bit enhances security without external keys. Empirical validation exhibits a high Peak Signal-to-Noise Ratio (PSNR) (55.90 dB) and low Mean Square Error (MSE), indicating good imperceptibility and security. However, limited evaluation and lack of theoretical justification raise questions about real-world applicability and robustness, necessitating further investigation. Almaliki *et al.,* [22] presented a systematic approach to categorizing carrier images in digital steganography based on their noise levels, utilizing the Canny filter.

Notably, the strength of the paper lies in its advancement towards automatic image classification, which optimized the selection of substitution methods for embedding secret information. By eliminating the need for human intervention in the classification process, the proposed method enhances the efficiency and efficacy of steganographic techniques. Nevertheless, while the paper highlighted the effectiveness of the approach through empirical testing and algorithm development, it lacks a comprehensive discussion on potential limitations or challenges associated with the proposed method. Additionally, further elaboration on how this method compares to existing techniques could provide valuable insights into its novelty and applicability. Noroozi *et al.,* [23] presented an approach integrating digital signature into image steganography to enhance its robustness against attacks, particularly focusing on maintaining security and authenticity. Thus, by embedding the signature directly into the cover image, the proposed scheme minimizes additional bandwidth requirements and enhances computational efficiency. However, while the paper outlines the methodology and benefits of the proposed algorithm, it lacks in-depth discussion on potential vulnerabilities or limitations of the approach, such as susceptibility to specific types of attacks or the impact on image quality. Therefore, further empirical validation or comparative analysis with existing methods could provide stronger evidence of the scheme's effectiveness and practical applicability.

We describe a technique that uses the one-bit LSB method in the spatial field to incorporate confidential information in order to overcome the drawbacks of the aforementioned techniques. We use the AES method, an encryption technique with a 128-bit key prior to embedding, to increase security. In addition, we combine the LSB technique with a user-selected pixel recognition mechanism during embedding to provide effective performance even with random permutations. Since Portable Network Graphics (PNG) files have good visibility, we utilize them as cover pictures. For assessment, quality measurements, such as PSNR is denoted as Peak Signal-to-Noise Ratio, MSE is presented as Mean Square Error, and RMSE is denoted as Root Mean Square Error, are used in the result section [24].

3. Methodology

In this study, an automatically generated two-layered encrypted information hiding method for picture steganography using single-bit LSB with a customer-particular customizable image element choosing technique exhibited where the algorithm for encryption and steganography conduct will be explained in depth in the subsections that follow. The confidential information must be inputted by the user using our proposed tool and will be decoded automatically after it has arrived. It is deciphered using the AES method, a largely popular and secured symmetric encoding standard [25] that can condense information chunks using various symmetric keys gradationally. Furthermore, it utilizes a similar encoding key for breaking and then encrypting and decoding confidential information. In this paper, 128-bit critical size was employed to encode the confidential information, which offers superior outcomes with fast speed besides using minimal random-access memory (RAM) [26]. The essential size of 128 bits is secure; however, [27, 28] it has been bypassed through direct automation. All AES methods are implemented using a function developed in C-Sharp language.

Subsequently encoding the confidential message, the encoded information waits to be placed into the original carriers and converted to PNG picture-organized images developed in C-Sharp language. This image element filtering is a dynamic user-selected technique where users have options to decide between two techniques. The first one is even based on pixel filtering operated by MSB bit. In the context of image processing, the "Even-Based Pixel Filtering Algorithm" is a method for selecting and filtering pixels within an image. In addition, it operates by examining the binary representation of the red segment of the RGB color values of each pixel in the image. Specifically, it focuses on the two most significant bits of the red channel, which are the highest-order bits that carry the most weight in determining the red component's value. The RGB color model is a widely used representation of digital images.

In this model, each pixel is described by three color channels: RGB. Each channel typically uses 8 bits to represent the intensity of its respective color component, resulting in a 24-bit color representation. To apply the algorithm, convert the red channel of each pixel into its binary representation. This involves expressing the red component as a sequence of 8 binary digits (0s and 1s), with the leftmost (most significant) bit having the highest weight. The algorithm focuses on the first and second most significant bits of the red channel's binary value. Note that these bits have the greatest influence on the overall intensity of the red component. The name "Even-Based Pixel Filtering Algorithm" derives from the specific criterion used for pixel selection. If the first and second most significant bits of the red component are the same (either both 0 or both 1), then the pixel is considered eligible for selection based on this evenness criterion. In other words, it filters out pixels whose red component's binary representation starts with 10 or 00. The algorithm selects and retains pixels in the image that meet this even-based criterion. These selected pixels typically exhibit a specific pattern in their red intensity and may be used for further processing or analysis.

The application of this algorithm can have various use cases, depending on the specific goals of the image processing task. The even-based criterion exploits the characteristics of the binary representation of the red component to filter and extract specific information or patterns from the image. This approach is displayed in Figure 2. The second one, the "Odd-Based Pixel Filtering Algorithm," is an image processing technique that revolves around the binary representation of the red channel in the RGB color model. This algorithm is designed to select and filter pixels within an image by examining the binary values of the red component, specifically focusing on the first and second most significant bits. The RGB color model is commonly used to represent digital images. In this model, each pixel is described by three color channels: red, green, and blue. Typically, each channel employs 8 bits to represent the intensity of its respective color component, resulting in a 24-

bit color representation for each pixel. To apply the algorithm, convert the red channel of each pixel into its binary representation. This involves expressing the red component as an 8-bit binary number, with the leftmost (most significant) bit holding the highest weight.

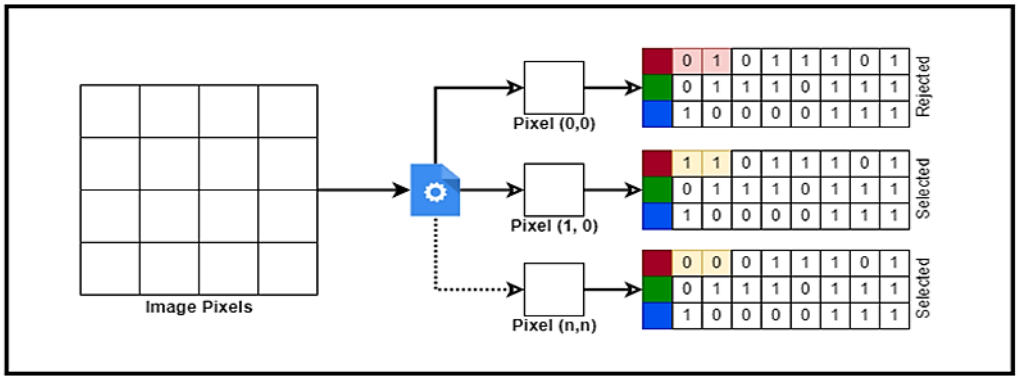


Fig. 2. Even pair-based pixel filtering system

The algorithm specifically targets the first and second most significant bits of the red channel's binary value since these bits carry the greatest significance in determining the overall intensity of the red component. The name "Odd-Based Pixel Filtering Algorithm" derives from the criterion used for pixel selection. In this case, if the first and second most significant bits of the red component are opposite (i.e., one is 0 and the other is 1), then the pixel is considered eligible for selection based on this oddness criterion. In other words, it filters out pixels whose red component's binary representation begins with 01 or 10. The algorithm selects and retains pixels in the image that meet this odd-based criterion. These selected pixels typically exhibit a specific pattern in their red intensity, and they can be used for further analysis or processing based on this unique characteristic. The application of the Odd-Based Pixel Filtering Algorithm can vary depending on the specific objectives of the image processing task. Notably, this technique is valuable in scenarios where selecting pixels based on the binary characteristics of their red component is crucial. This approach is illustrated in Figure 3. Here, we use (X_n, Y_m) [Where n= width, m= height] to visit all pixels to check.

$F_{yB}(F_{xr}(X, Y))[0][1]$ is used to find even or odd pairs from the 1st and 2nd MSB positions based on a user-selected approach. Note that F_{XB} denotes the function of binary conversion, and F_{xr} denotes the function of getting the value red.

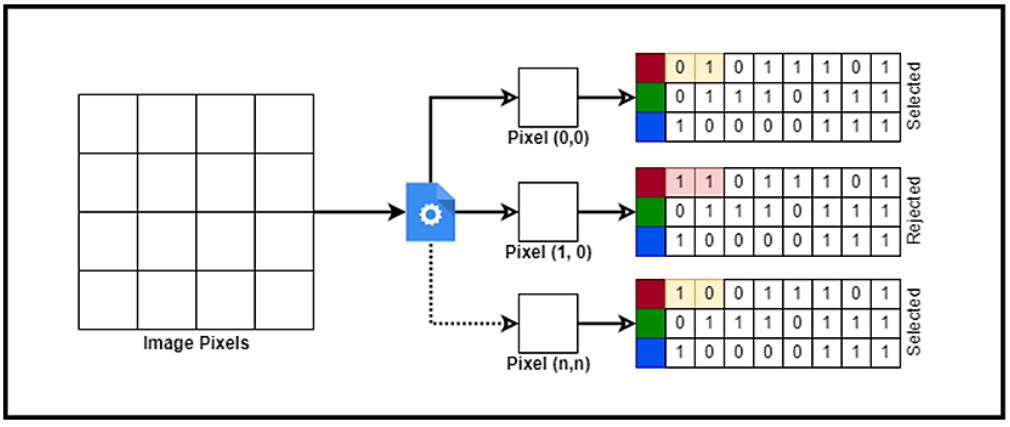


Fig. 3. Oddly pair-based pixel filtering system

The steganographic method is separated into dual corridors–the bone is the implanting approach, and the recovery technique is another one. Figure 4 depicts the implanting technique of the suggested system; it collects the hidden base content from the end user and encodes the information exchange through an AES technique with a key of 128-bit. In the second stage, photos are taken as the cover holder, and afterward, the corresponding image element-picking mechanism relates to the systems defined above.

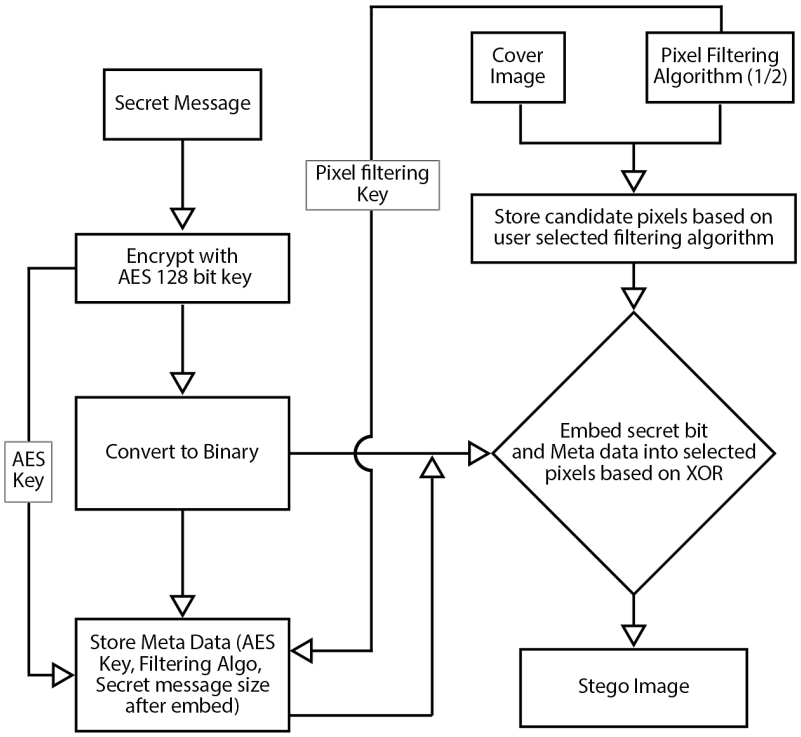


Fig. 4. Embedding process

In the third phase, the encoded information clandestine communication information will be translated into 8-bit-based binary data that subsequently is placed with a one-bit LSB location of selected pixels by the operation of XOR. Here, XOR will operate with the cloistered text bit and the sixth allocated bit, replacing the last indexed to RGB chunks. Figure 5 depicts the retrieving technique. To recover secret information, having an understanding of the facts such as private message embed key, text size, and image element selecting approach will accumulate the immobile four image element location using Eqs. (1) to (4).

$$\text{1st Pixel's Position: } (X_1, Y_1) = \left\{\left(\frac{W}{2} - 3\right), 1\right\} \tag{1}$$

$$\text{2nd Pixel's Position: } (X_2, Y_2) = \left\{W, \left(\frac{H}{2} - 3\right)\right\} \tag{2}$$

$$\text{3rd Pixel's Position: } (X_3, Y_3) = \left\{\left(\frac{W}{2} + 3\right), H\right\} \tag{3}$$

$$\text{4th Pixel's Position: } (X_4, Y_4) = \left\{1, \left(\frac{H}{2} + 3\right)\right\} \tag{4}$$

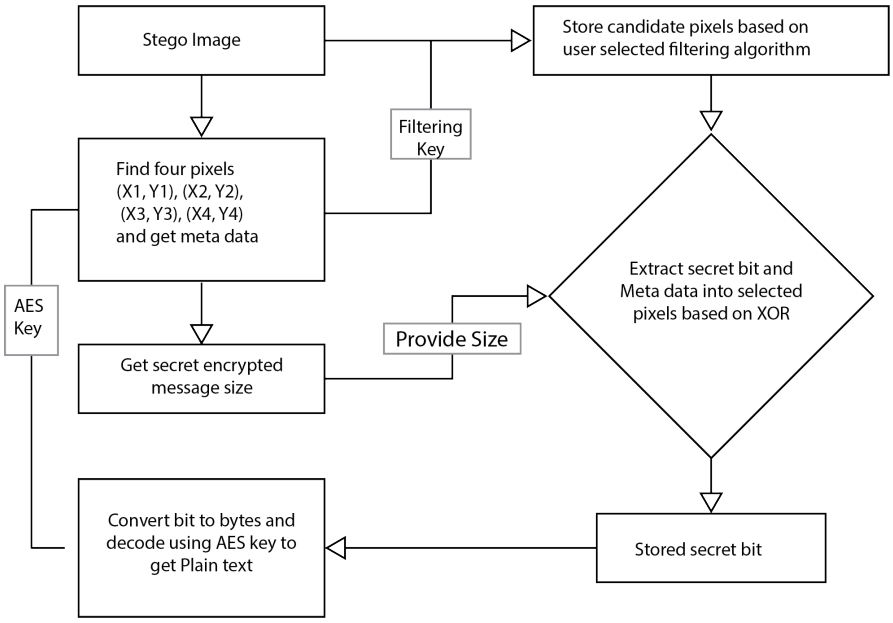


Fig. 5. Retrieving process

In Eq. (1), (X_1, Y_1) represents a pixel location in an image. In computer graphics and image processing, this notation is often used to define the coordinates of a specific point within an image. X_1 typically denotes the horizontal (or x-axis) coordinate, while Y_1 denotes the vertical (or y-axis) coordinate. Together, they specify the exact location of a pixel. Note that W represents the width of an image. The variable 'W' is used to define the image's width in terms of the number of pixels along the horizontal (x-axis) direction. This width is typically measured in pixels. (W/2 - 3) is the x-coordinate (horizontal position) of the pixel. It is calculated as follows: (W/2) represents the midpoint of the image in the x-axis since 'W/2' divides the width in half. Subtracting 3 from this midpoint shifts the pixel location 3 units to the left along the x-axis.

In other words, it moves three pixels to the left from the center. 1 is the y-coordinate (vertical position) of the pixel. In this case, the y-coordinate is a constant value of 1, which means the pixel is located at a fixed height in the image, likely at the top of the image. Therefore, the equation (X_1, Y_1) = (W/2 - 3, 1) specifies the pixel location within the image. It is located at a position that is W/2 - 3 pixels from the left edge of the image along the x-axis (horizontal) and at a fixed height of 1 pixel from the top of the image along the y-axis (vertical). The specific position of this pixel depends on the value of 'W,' which is the width of the image.

In Eq. (2), the equation (X_2, Y_2) = (W, H/2 - 3) specifies the pixel's location within the image. It is situated at the far-right edge of the image (W pixels from the left) along the x-axis and at a specific height (H/2 - 3 pixels from the center) along the y-axis. The actual position of this pixel is determined by the values of 'W' and 'H,' which represent the image's width and height, respectively. Similarly, Eqs. (3) and (4) are calculated.

The pixels are used to store meta information, which is used to retrieve techniques to know the AES key and message size and filter the pixels algorithm. After understanding the filtering method, the system utilized will be able to retrieve filtering image elements where the encoded confidential communication bits are kept in the implanting tactic. Consequently, the system will perform the XOR mathematical maneuver with each of the sixth and seventh indexed bits for RGB chunks to retrieve the confidential data bit. After collecting the bits depending on the payload text size, the system may decode the encrypted communication protocol based on the AES key. It would be able to acquire the plain text that was deliberately disguised.

Figure 6 represents the flowchart of the embedding and retrieval process of our proposed approach. In the embedding process, users must provide a clandestine message, cover image, and image element filtering algorithm. Then, the system will consign the provided information to the primary memory first. Afterward, the encoding key for AES is generated randomly based on 128-bit. Subsequently, the system will immediately begin finding image elements depending on the pixel processing method and save them as part of an image element list utilized in the implanting procedure. Those picture components are utilized to mask sensitive bits from the material being encoded, which is altered by the AES key. The provided embedding algorithm describes a method for employing steganography to conceal information inside a picture. The original carrier (CI), the confidential message (Sm), and supplementary information (FA) are the first inputs. It generates an AES Encryption Key (EK). Meanwhile, the encrypted confidential message (ESm) is created by first encrypting the Sm with the generated key using AES encryption.

Futhermore, the technique includes filtering operations to handle the cover picture and meta information (MD) creation for embedding. By performing a number of filtering operations on the cover picture at certain coordinates (X, Y), filtered pixel values are produced. The EK, FA, and the measurement of the ESm are combined to generate MD. The information is used to extract the location explained in Eqs. (1) to (4). The ESm is then further processed to produce a Stego Message Buffer (SMB). The process then repeats across each filtered pixel. The SMB is contained in the RGB value for each pixel utilizing the LSB XOR manipulation. The RGB value is updated to reflect the modifications after the embedding. This method encrypts the Sm, processes the cover picture, produces MD, builds an SMB, and then iteratively inserts the stego message into the image element values of the cover carrier using LSB XOR manipulation. The resultant picture, known as the Stego Image (SI), includes an S_m that is hidden.

Result: Stego Image
$S_m \leftarrow input;$
$C_l \leftarrow input;$
$F_A \leftarrow input;$
$E_K = AESKey();$
$ES_m = AESEncryption(S_m, E_K);$
$FilteredPixels[] = F_{XB}(Fxr(X,Y))[0][1](C_I);$
$M_D = F_{XB}(E_K + F_A + Size(ES_m));$
$(x1,y1),(x2,y2),(x3,y3),(x4,y4) \leftarrow M_D;$
$S_{MB} = F_{XB}(ES_m);$
for $a \leq FilteredPixels[]$ **do**
  $RGB = Read(FilteredPixel[n]);$
  $embedLSBXOR(RGB, S_{MB});$
  $UpdatedRGB();$
end

(a)

Result: Secret Message
$S_l \leftarrow input;$
$M_D \leftarrow (x1,y1),(x2,y2),(x3,y3),(x4,y4);$
$FilteredPixels[] = Fx(M_D, S_I);$
$M_S = M_D[Size(ES_m)];$
for $a \leq FilteredPixels[]$ **do**
  $SecretBit[] = retrieveLSBXOR(RGB, S_{MB})$
  if $(SecretBit[] >= M_S)$ **then**
    Break;
  end
end
$encryptedMessage = BitToBytes(SecretBit[])$
$Plaintext = Decode(encryptedMessage, Key)$

(b)

Fig. 6. Algorithm of the proposed approach (a) Embed process (b) Retrieve process

Another aspect of the extracting process is a completely different procedure comprising the embedding technique. The repossession procedure offered describes how to use steganography techniques to retrieve a hidden message from a stego picture. The SI serves as the first input. The

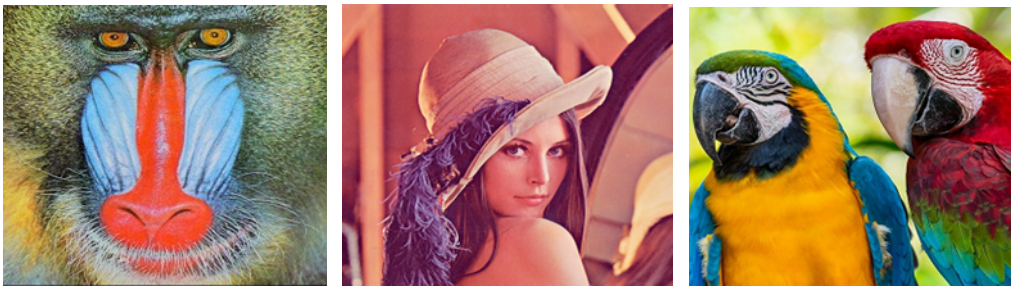
approach presupposes that the SI's MD, which consists of locations Eqs. (1) to (4), has been retrieved. Applying the function Fx, which requires these coordinates and the stego picture as inputs, yields the filtered pixel values. The meta information size (MS), in particular the size of the ESm, is also retrieved by the method from the MD. The program then repeats the process for every pixel that was filtered. Using a function called retrieve LSB XOR, the LSB of each image element's RGB values are obtained. These LSBs are kept in a Confidential Bit array. Until the total amount of bits is more than or equal to the MS, the method will continue to extract and store these bits. The loop is now broken at this point. Using the method BitToBytes, the obtained confidential bits (ConfidentialBit[]) are then changed into bytes to create an encrypted message (encryptedMessage). Finally, a decoding procedure utilizing a predetermined key is used to convert this encrypted message into plaintext. The original hidden message included inside the stego picture is obtained as a consequence of this decoding. In conclusion, the retrieval algorithm uses the information, processes the pixel values, and applies bitwise operations to retrieve the Sm concealed inside a stego picture methodically. The Sm previously concealed using steganography is eventually obtained by recovering the original encrypted message and then decrypting it using a supplied key.

4. Performance Analysis of the Proposed Framework

This section offers a thorough breakdown of the results via graphical depiction and compares the stego carrier to the unique cover carrier. The effectiveness of the suggested approach is further demonstrated by comparing its findings to those from well-known steganographic techniques. Three evaluations of quality criteria are incorporated in the statistical investigation portion of this study, including measures like PSNR, RMSE, and MSE.

In order to conduct a thorough and rigorous experimental evaluation, three specific images were thoughtfully chosen. These images, namely the "Baboon," "Lena," and "Parrot," were selected for their unique characteristics and diverse content. Each image was prepared in a standardized format with a resolution of 512 by 512 pixels. This uniformity in resolution ensures consistency in the evaluation process, allowing for meaningful comparisons and assessments. Additionally, the images were saved in the widely-used PNG format, known for its lossless compression, which preserves image quality and detail during storage.

Figure 7 provides a visual representation of how these carefully selected images are utilized in the evaluation of the proposed methodology. It serves as a pivotal reference point, offering a clear and concise overview of the experimental setup. This figure illustrates the specific roles of the "Baboon," "Lena," and "Parrot" images in assessing the methodology's performance. Their inclusion in the experimental framework allows for a comprehensive analysis of the suggested approach, revealing its strengths and limitations. To implement the proposed methodology, the development environment relied on the .NET Framework version 4.8. This choice of framework was deliberate, as it offers a stable and well-established platform for software development. Furthermore, the use of .NET Framework 4.8 ensured the reliability and compatibility of the implemented methodology. It also provided access to a wide range of libraries and resources that facilitated the development process. This technology selection underscores the commitment to a robust and efficient execution of the proposed methodology, aligning with industry best practices. In essence, the selection, preparation, and evaluation of these images, along with the choice of the .NET Framework version 4.8, collectively contribute to a comprehensive and meticulously planned approach for the experimental assessment of the methodology. This attention to detail and the utilization of proven technologies enhances the credibility and reliability of the research, allowing for meaningful insights and findings.



(a) (b) (c)

Fig. 7. Cover Images (a) Baboon, (b) Lenna, and (c) Parrot

Eq. (5) through Eq. (7) demonstrate the three specified quality measurement matrices (PSNR, RMSE, and MSE) as they are represented scientifically. Benchmarks for evaluating the effectiveness and security of the steganographic process are often used formulae.

$$PSNR = 10\log_{10}\frac{255^2}{MSE}dB \tag{5}$$

$$MSE = \frac{1}{n}\sum_{i-1}^{n}(y_i - \widetilde{y_i})^2 \tag{6}$$

$$RMSE = \sqrt{\sum_{i=1}^{n}\frac{\widehat{y_i} - y_i^2}{n}} \tag{7}$$

The mathematical representation for PSNR is provided by equation [29]. Historically, PSNR was measured in decibels (dB) and depends on MSE. Various studies indicate that a PSNR value exceeding 40 dB between the cover and stego frames is considered commendable. For the calculation of MSE and RMSE, as defined in references [30-32], the process involves taking the observed value, subtracting the predicted value, and squaring the difference. This procedure is repeated for all instances, with the squared values summed and then divided by the total instances.

The efficiency of the suggested system is examined with various payloads on the provided three photos. The discoveries of PSNR eminence evaluation measures for the provided frames are exposed in Table 1. Additionally, frames sized at 512 x 512 pixels, namely Baboon, Lenna, and Parrot, were utilized. With a payload of 15 kilobytes (15,000 bytes), the proposed system was able to conceal varying amounts of confidential information, ranging from 27,000 to 65,000 bytes across the various images in a graduated manner. Notably, the image of Parrot exhibited slightly sophisticated PSNR standards compared to the other frames.

This presented Table 1 focuses on Even Pair Pixels to test the model. Specifically, for the Lenna image, Even Pair Pixels account for 53% of the total, while the Baboon image comprises 28%, and the Parrot image leads with 64% Even Pair Pixels. When examining an image with dimensions of 512x512 and a payload of 512 bytes, the proposed model yields a PSNR value of 68.7456, an MSE value of 0.0027, and an RMSE value of 0.0519 for the Lenna image. Similarly, using the same dimensions but a payload of 256 bytes, the PSNR value increases to 71.9204, with an MSE of 0.0013 and an RMSE of 0.0363. Further, a payload of 128 bytes raises the PSNR value to 74.5643, while the MSE drops to 0.0007 and the RMSE falls to 0.0260 for the same Lenna image. Comparable results are observed for the Baboon image, with a PSNR value of 68.7655, an MSE of 0.0026, and an RMSE of 0.0512 for dimensions of 512x512 and a payload of 512 bytes. These metrics improve with decreasing payload size: a PSNR of 71.7456, MSE of 0.0013, and RMSE of 0.0356 with 256 bytes, and a PSNR of 75.5664, MSE of 0.0006, and RMSE of 0.0252 with 128 bytes. Turning to the Parrot image, with dimensions of

512x512 and a 512-byte payload, the metrics are PSNR 69.8645, MSE 0.0017, and RMSE 0.0417. With 256 bytes, the values become PSNR 72.5456, MSE 0.0010, and RMSE 0.0299. Finally, a 128-byte payload results in PSNR 75.9695, MSE 0.0005, and RMSE 0.0223. Conducting this experiment on three distinct images (Lenna, Baboon, and Parrot) with varied information types, it is evident that the Parrot image yields more effective results compared to Lenna and Baboon, as indicated by the performance metrics.

Table 1
Quality measuring metrics of the predicted technique

Frame	Resolutions	Pixels	Text Size	PSNR	MSE	RMSE
Lenna	512 X 512	53%	512 Bytes	68.7456	0.0027	0.0519
			256 Bytes	71.9204	0.0013	0.0363
			128 Bytes	74.5643	0.0007	0.0260
Baboon	512 X 512	28%	512 Bytes	68.7655	0.0026	0.0512
			256 Bytes	71.7456	0.0013	0.0356
			128 Bytes	75.5664	0.0006	0.0252
Parrot	512 X 512	64%	512 Bytes	69.8645	0.0017	0.0417
			256 Bytes	72.5456	0.0010	0.0299
			128 Bytes	75.9695	0.0005	0.0223

The comparison of various steganographic techniques using different metrics emphasizes the superior performance and efficiency of the proposed P-Model when compared to Models 1 and 2. Table 2 offers a comprehensive comparison, with the proposed PM outperforming the existing models in terms of payload (512 Bytes) and frame size (512x512), as denoted by the XOR substitution (M1) and the 8-directional based model (M2) [31, 32].

Table 2
A comparative study of recent steganography approaches

Photo	Approach	Text size (bytes)	PSNR	MSE	Time (milisec)
	M1	512	65.5456	0.0029	191
Lenna	M2	512	67.5615	0.0028	151
	PM	**512**	**68.7456**	**0.0027**	**125**
	M1	512	65.9655	0.0028	198
Baboon	M2	512	67.5315	0.0027	167
	PM	**512**	**68.7655**	**0.0026**	**134**
	M1	512	64.5154	0.0029	215
Parrot	M2	512	67.3265	0.0027	178
	PM	**512**	**69.8645**	**0.0026**	**154**

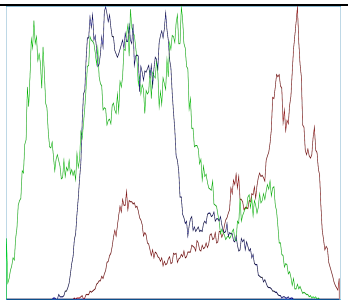
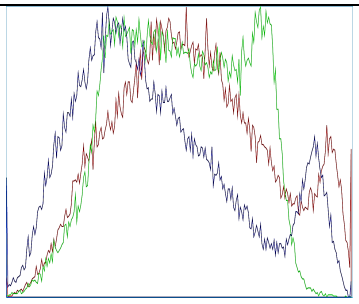
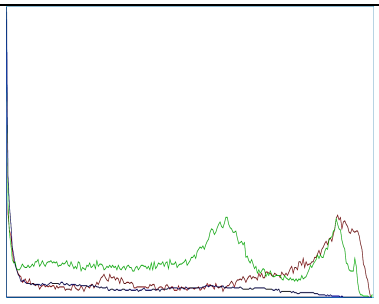
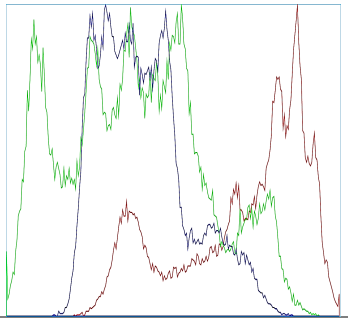
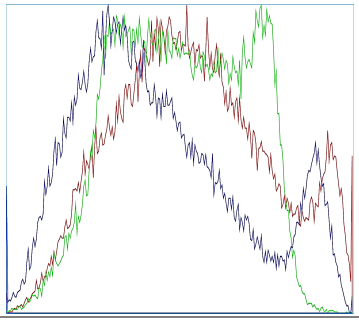
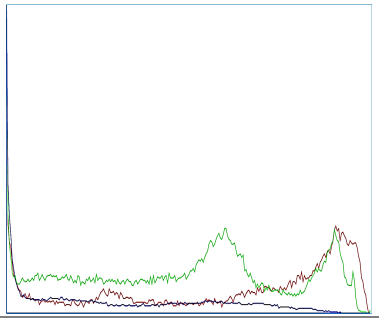
Using a variety of image performance measures as described in the respective paragraph, the projected scheme and two more existing approaches are thoroughly compared in the table above. Dimensions, payload, execution time, PSNR, and MSE values are all factors that are taken into account. The distinguishing characteristics of the different models are mentioned in the second attribute. The values for PSNR, MSE, and the duration of execution in milliseconds are displayed in the fifth attribute, sixth attribute, and seventh attribute, respectively. The third and fourth columns provide dimension and payload. Three unique images-Lenna, Baboon, and Parrot-are used in this research and are described in the first column of the table. Each picture has a standardized 512x512 pixel size and 512-byte payload. Model 1 produces a PSNR of 65.5456 and an MSE of 0.0029 for the Lenna picture in a time interval of 191 milliseconds. Meanwhile, Model 2 takes 151 milliseconds to achieve a PSNR of 67.5615 and an MSE of 0.0028. Notably, the suggested model (P-Model) completes

in only 125 milliseconds with a PSNR value of 68.7456 and an MSE of 0.0027. These findings highlight how much more effective the suggested methodology is compared to other methods.

Moving on to the Baboon picture, Model 1 produces it in 198 milliseconds with a PSNR of 65.9655 and an MSE of 0.0028. Nevertheless, within 167 milliseconds, Model 2 offers a PSNR of 67.5315 and an MSE of 0.0027. The proposed P-Model, in comparison, provides a PSNR of 68.7655 and an MSE of 0.0026 in only 134 milliseconds. These numbers demonstrate the suggested model's better performance vs the alternatives. Model 1 takes 215 milliseconds to process the Parrot picture and offers PSNR and MSE values of 64.5154 and 0.0029, respectively. In 178 milliseconds, Model 2 produced results with a PSNR of 67.3265 and an MSE of 0.0027. Surprisingly, the suggested P-Model accomplishes a PSNR of 69.8645 and an MSE of 0.0026, both in 154 milliseconds. These results demonstrate that the suggested paradigm is more successful than the other methods.

In summary, the suggested P-Model consistently outperforms both Models 1 and 2 when evaluating a variety of metric values in comparison to comparable methodologies. Additionally, Table 3 depicts histograms for the three aforementioned photos in 512 x 512 pixel sizes for the cover and SIs.

Table 3
A comparative study of steganographic methods through histograms

Type	Lenna	Baboon	Parrot
Cover			
Stego			

In the process of comparing histograms of numerous photos, the purpose is to statistically quantify the degree of similarity or dissimilarity between these images based on their pixel intensity distributions. The histogram analysis approach provides a mechanism for attaining this purpose. The findings of the histogram analysis have demonstrated that there is a minimal noticeable difference between the two photos under scrutiny. In essence, this indicates that the differences or inconsistencies noticed are so minor that they remain undetectable to human sight. Histogram analysis is a great method for picture comparison as it allows us to break down complicated visual information into a numerical representation. Each pixel's intensity contributes to the total histogram, enabling us to evaluate the distribution of pixel values. When the histograms of two photos display minimum differences, it suggests that the pixel intensity patterns in both photographs are surprisingly comparable. In addition, this inconspicuous amount of variance between the photos is

essential in numerous applications. For instance, in quality control and verification operations, the capacity to identify even the tiniest deviations is vital. Additionally, in sectors like picture compression or data concealing, recognizing that some adjustments are invisible to human sight guarantees that the visual quality of images stays preserved.

In essence, the findings of our histogram analysis provide valuable insights regarding the resemblance of the photos being compared. Although unnoticeable to the human viewer, the slight deviations discovered possess practical value in many sectors where maintaining picture quality and detecting minute changes are of essential interest.

4. Conclusions

This work proves the special advantages of the proposed approach for information steganography via careful investigation and result analysis. It appears to be a strong and trustworthy solution that offers cutting-edge security features. Furthermore, it is discovered that the approach outperforms a number of current information-concealing strategies in terms of imperceptibility or the capacity to produce changes that are invisible to human sight. Together, these findings highlight the greater security and decreased risk of discovery connected with this novel method of picture steganography. Furthermore, using a dual-layered approach, this research study provides an innovative and automated method for safely encoding information in photographs. The technology incorporates LSB replacement and XOR operations as well as a cutting-edge, dynamic pixel selection technique that customers may personalize. Accordingly, this technique effectively conceals sensitive information by encrypting it with 128-bit AES inside the original picture.

Acknowledgement

This research was partially funded by the Centre of Excellence for Advanced Computing (ADVCOMP), Universiti Malaysia Perlis.

References

[1] Chandramouli, Rajarathnam, and Nasir Memon. "Analysis of LSB based image steganography techniques." In *Proceedings 2001 International Conference on Image Processing (Cat. No. 01CH37205)*, 3, p. 1019-1022. IEEE, 2001. https://doi.org/10.1109/ICIP.2001.958299

[2] Mathur, Nishtha, and Rajesh Bansode. "AES based text encryption using 12 rounds with dynamic key selection." *Procedia Computer Science* 79 (2016): 1036-1043. https://doi.org/10.1016/j.procs.2016.03.131

[3] Islam, Md Rashedul, Ayasha Siddiqa, Md Palash Uddin, Ashis Kumar Mandal, and Md Delowar Hossain. "An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography." In *2014 International Conference on Informatics, Electronics & Vision (ICIEV)*, p. 1-6. IEEE, 2014. https://doi.org/10.1109/ICIEV.2014.6850714

[4] Mukhedkar, Moresh, Prajkta Powar, and Peter Gaikwad. "Secure non real time image encryption algorithm development using cryptography & steganography." In *2015 Annual IEEE India Conference (INDICON)*, p. 1-6. IEEE, 2015. https://doi.org/10.1109/INDICON.2015.7443808

[5] Singh, Kh Manglem, L. Shyamsudar Singh, A. Buboo Singh, and Kh Subhabati Devi. "Hiding secret message in edges of the image." In *2007 International Conference on Information and Communication Technology*, p. 238-241. IEEE, 2007. https://doi.org/ 10.1109/ICICT.2007.375384

[6] Joshi, Kamaldeep, and Rajkumar Yadav. "A new LSB-S image steganography method blend with Cryptography for secret communication." In *2015 Third International Conference on Image Information Processing (ICIIP)*, p. 86-90. IEEE, 2015. https://doi.org/10.1109/ICIIP.2015.7414745

[7] Li, Xiaolong, Tieyong Zeng, and Bin Yang. "Detecting LSB matching by applying calibration technique for difference image." In *Proceedings of the 10th ACM Workshop on Multimedia and Security*, p. 133-138. 2008. https://doi.org/10.1145/1411328.1411353

[8] Loukhaoukha, Khaled, Jean-Yves Chouinard, and Abdellah Berdai. "A secure image encryption algorithm based on Rubik' s cube principle." *Journal of Electrical and Computer Engineering* 2012, no. 1 (2012): 173931. https://doi.org/10.1155/2012/173931

[9] Majeed, Anas, Miss Laiha Mat Kiah, Hayan T. Madhloom, B. B. Zaidan, and A. A. Zaidan. "Novel approach for high secure and high rate data hidden in the image using image texture analysis." *International Journal of Engineering and Technology* 1, no. 2 (2009): 63-69.

[10] Ghosal, Sudipta Kr. "A new pair wise bit based data hiding approach on 24 bit color image using steganographic." *IEMCON* (2011): 123-129.

[11] Kaur, Dilpreet, Harsh Kumar Verma, and Ravindra Kumar Singh. "A hybrid approach of image steganography." In *2016 International Conference on Computing, Communication and Automation (ICCCA)*, p. 1069-1073. IEEE, 2016. https://doi.org/ 10.1109/CCAA.2016.7813901

[12] Ren-Er, Yang, Zheng Zhiwei, Tao Shun, and Ding Shilei. "Image steganography combined with DES encryption pre-processing." In *2014 Sixth International Conference on Measuring Technology and Mechatronics Automation*, p. 323-326. IEEE, 2014. https://doi.org/ 10.1109/ICMTMA.2014.80

[13] Raniprima, Sevierda, Bambang Hidayat, and Nur Andini. "Digital image steganography with encryption based on rubik's cube principle." In *2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC)*, p. 198-201. IEEE, 2016. https://doi.org/10.1109/ICCEREC.2016.7814972

[14] Phadte, Radha S., and Rachel Dhanaraj. "Enhanced blend of image steganography and cryptography." In *2017 International Conference on Computing Methodologies and Communication (ICCMC)*, p. 230-235. IEEE, 2017. https://doi.org/10.1109/ICCMC.2017.8282682

[15] Broda, Martin, Vladimir Hajduk, and Dušan Levický. "Image steganography based on combination of YC b C r color model and DWT." In *2015 57th International Symposium ELMAR (ELMAR)*, p. 201-204. IEEE, 2015. https://doi.org/ 10.1109/ELMAR.2015.7334530

[16] Charan, Gunda Sai, Nithin Kumar SSV, B. Karthikeyan, and V. Vaithiyanathan. "A novel LSB based image steganography with multi-level encryption." In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-5. IEEE, 2015. https://doi.org/10.1109/ICIIECS.2015.7192867

[17] Khalaf, Emad T., and Norrozila Sulaiman. "Segmenting and hiding data randomly based on index channel." *International Journal of Computer Science Issues (IJCSI)* 8, no. 3 (2011): 522.

[18] Emad, Elshazly, Abdelwahab Safey, Abouzaid Refaat, Zahran Osama, Elaraby Sayed, and Elkordy Mohamed. "A secure image steganography algorithm based on least significant bit and integer wavelet transform." *Journal of Systems Engineering and Electronics* 29, no. 3 (2018): 639-649. https://doi.org/10.21629/JSEE.2018.03.21

[19] Deeba, Farah, She Kun, Fayaz Ali Dharejo, and Hira Memon. "Digital image watermarking based on ANN and least significant bit." *Information Security Journal: A Global Perspective* 29, no. 1 (2020): 30-39. https://doi.org/10.1080/19393555.2020.1717684

[20] Alam, Sheikh Thanbir, Nusrat Jahan, and Md Maruf Hassan. "A New 8-Directional Pixel Selection Technique of LSB Based Image Steganography." In *Cyber Security and Computer Science: Second EAI International Conference, ICONCS 2020, Dhaka, Bangladesh, February 15-16, 2020, Proceedings 2*, p. 101-115. Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-52856-0_8

[21] Bhuiyan, Touhid, Afjal H. Sarower, Rashed Karim, and Maruf Hassan. "An image steganography algorithm using LSB replacement through XOR substitution." In *2019 International Conference on Information and Communications Technology (ICOIACT)*, p. 44-49. IEEE, 2019. https://doi.org/10.1109/ICOIACT46704.2019.8938486

[22] Almaliki, Alaa Jabbar Qasim, Sajad Muhil Abd, Inam Abdullah Lafta, Roshidi Din, Osman Ghazali, Jabbar Qasim Almaliki, and Sunariya Utama. "Application of the canny filter in digital steganography." *Journal of Advanced Research in Computing and Applications* 35, no. 1 (2024): 21-30. https://doi.org/10.37934/arca.35.1.2130

[23] Noroozi, E., S. M. Daud, and A. Sabouhi. "A security enhanced robust image hiding algorithm from digital signature." *Journal of Advanced Research in Applied Mechanics* 8: 1-12.

[24] Kaur, Sharanpreet, Surender Singh, Manjit Kaur, and Heung-No Lee. "A systematic review of computational image steganography approaches." *Archives of Computational Methods in Engineering* 29, no. 7 (2022): 4775-4797. https://doi.org/10.1007/s11831-022-09749-0

[25] Rathod, Chetan, and Atul Gonsai. "A Detailed Comparative Study and Performance Analysis of Standard Cryptographic Algorithms." In *Cyber Security and Digital Forensics: Proceedings of ICCSDF 2021*, p. 301-307. Springer Singapore, 2022. https://doi.org/10.1007/978-981-16-3961-6_26

[26] Umamaheswari, S., N. R. Vishal, N. R. Pragadesh, and S. Lavanya. "Secure Data Transmission using Hybrid Crypto Processor based on AES and HMAC Algorithms." In *2023 2nd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA)*, p. 1-6. IEEE, 2023.. https://doi.org/10.1109/ICAECA56562.2023.10200277

[27] Bedoui, Mouna, Hassen Mestiri, Belgacem Bouallegue, Belgacem Hamdi, and Mohsen Machhout. "An improvement of both security and reliability for AES implementations." *Journal of King Saud University-Computer and Information Sciences* 34, no. 10 (2022): 9844-9851. https://doi.org/10.1016/j.jksuci.2021.12.012

[28] Salman, Rasool S., Alaa K. Farhan, and Ali Shakir. "Lightweight modifications in the Advanced Encryption Standard (AES) for IoT applications: a comparative survey." In *2022 International Conference on Computer Science and Software Engineering (CSASE)*, p. 325-330. IEEE, 2022. https://doi.org/10.1109/CSASE51777.2022.9759828

[29] Christiana Abikoye, Oluwakemi, Roseline Oluwaseun Ogundokun, Sanjay Misra, and Akasht Agrawal. "Analytical study on LSB-based image steganography approach." In *Computational Intelligence in Machine Learning: Select Proceedings of ICCIML 2021*, p. 451-457. Singapore: Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-16-8484-5_43

[30] Tevaramani, Saleem S., and J. Ravi. "Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication." *Global Transitions Proceedings* 3, no. 1 (2022): 208-214. https://doi.org/10.1016/j.gltp.2022.03.024

[31] Luo, Jie, Peisong He, Jiayong Liu, Hongxia Wang, Chunwang Wu, Chao Yuan, and Qiang Xia. "Improving security for image steganography using content-adaptive adversarial perturbations." *Applied Intelligence* 53, no. 12 (2023): 16059-16076. https://doi.org/10.1007/s10489-022-04321-6

[32] Kuznetsov, Oleksandr, Emanuele Frontoni, and Kyrylo Chernov. "Beyond traditional steganography: enhancing security and performance with spread spectrum image steganography." *Applied Intelligence* 54, no. 7 (2024): 5253-5277. https://doi.org/10.1007/s10489-024-05415-z