

Article

Image Steganography Using LSB and Hybrid Encryption Algorithms

May Alanzy , Razan Alomrani , Bashayer Alqarni and Saad Almutairi * 

Faculty of Computers and Information Technology, University of Tabuk, Tabuk 71411, Saudi Arabia;
431009225@stu.ut.edu.sa (M.A.); 431010255@stu.ut.edu.sa (R.A.); 431000026@stu.ut.edu.sa (B.A.)

* Correspondence: s.almutairi@ut.edu.sa

Abstract: In today's era of widespread web technology and cloud computing, ensuring data security has become a crucial concern across various industries. Instances of data breaches and vulnerabilities in cloud storage have emphasized the need for robust data protection and communication protocols, particularly in sectors like social media, military, and research. This research proposes a Multi-Level Steganography (MLS) algorithm that employs two encryption algorithms, AES and Blow-Fish, to secure the cover image and embed encryption keys as key images within the stego image. The proposed MLS algorithm incorporates a robust pixel randomization function to enhance the security of the encrypted data. Experimental results demonstrate that the proposed algorithm effectively protects data with high Peak Signal-to-Noise Ratio (PSNR) and low Mean Square Error (MSE) values, ensuring superior image quality, reliable encryption, and decryption of secret messages. The utilization of hybrid encryption with AES and BlowFish algorithms further strengthens the algorithm's security by augmenting the complexity of the encryption process.

Keywords: AES; steganography; encryption; decryption; peak signal-to-noise ratio



Citation: Alanzy, M.; Alomrani, R.; Alqarni, B.; Almutairi, S. Image Steganography Using LSB and Hybrid Encryption Algorithms. *Appl. Sci.* **2023**, *13*, 11771. <https://doi.org/10.3390/app132111771>

Academic Editor: Luis Javier Garcia Villalba

Received: 19 September 2023

Revised: 19 October 2023

Accepted: 22 October 2023

Published: 27 October 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

In today's digital landscape, the escalating threat of malicious attacks targeting businesses, government entities, and private individuals has prompted a growing need for robust information security measures. As a result, developers and researchers are actively seeking technical solutions to ensure the privacy and confidentiality of documents transmitted over communication channels [1,2]. With the rapid shift of numerous services from local networks to the Internet, the significance of information security and data protection has reached new heights. To counteract the evolving processing capabilities of cryptanalysis, encryption algorithms have undergone significant advancements to bolster their complexity, thereby deterring attackers from swiftly compromising encrypted data [3,4]. It should be remembered that encrypted data always take an attacker's attention to try to crack the encrypted data as a challenge. Complex steganography techniques hide the data's existence, leading to fewer attacking possibilities. Steganography represents the technique of concealing data inside a cover medium, the origin of the word 'Steganography' is Greek, and it means 'hidden or covered writing'. Steganography mainly aims at concealing the very presence of the message inside the cover medium [5–7]. Its technique contains many secret communication methods that hide the mere fact of concealed data.

Conventional methods include the usage of microdots, invisible inks, etc. The recent techniques of steganography attempt to take advantage of video files, digital media images, audio files, etc. Steganography can combine hiding and encryption mechanisms. This makes finding the data hidden in the object much more complicated since the data are unreadable, and any attacking techniques see the results as unexpected and confusing [8,9]. Therefore, much research has been conducted to enhance the hiding mechanisms, particularly as a message exchange mechanism for top-secret data. Some of the newest trends

are to use steganography as the initial phase of opening the secure tunnels instead of predefined certificates or private and public keys. As discussed earlier, steganography handles concealing data in a cover source. Moreover, steganalysis represents the science and art of revealing messages hidden through steganography, identical to cryptanalysis utilized in cryptography [10–12].

The objectives of steganalysis are to detect suspicious packages, find out whether there is a payload that is encoded into the packages and retrieve that payload. Therefore, the main challenges of efficient steganography are as follows: Many researchers have been working on steganography algorithms to make it difficult to detect/extract secret data by steganalysis and to make it difficult for the Human Visual System (HVS) to find a slight difference that happens on cover data such as audio, image, and video after the hiding process. In addition, the use of multi-level steganography has been increasing in recent years [6,13]. The hiding efficiency and the hiding payload secret message are two crucial considerations that every effective and potent steganography system should consider. Researchers developed the first factor to satisfy the efficiency of the steganography scheme by making the visual quality of the stego image match with the cover image; when viewers notice any distortion that raises the likelihood of the attacker's suspicion, signalization is used. The user's requirements and the type of steganography scheme change these two [14–16].

This research aims to develop and design a very effective and efficient data hiding mechanism using the steganography technique with encryption algorithms to ensure confidentiality and integrity and to increase the security of the stego image by a method that does not show any difference in the image using visual attack tools. Also, the proposed approach is designed to generate a stego image with the lowest quality changes to avoid any visual attacks that can lead to the hidden message. The model also has an encryption solution using AES and Blowfish to the hidden message to protect the content of the secret message from being exposed and used by unauthorized individuals. Disinformation represents intentionally inaccurate or false information that is deliberately spread. This research mainly addresses the problem of detecting an attacker's alteration of a concealed confidential message. It also addresses the issue of improving the unauthorized individual's steganography of a personal protection technique by attaching an unauthorized individual to verify integrity. This layer assists in recognizing possible amendments to a confidential message that is not a constituent of the original message.

The main contributions of the research paper are summarized as follows:

1. Development of an effective and efficient data hiding technique using steganography: The research paper proposes a method that combines steganography and encryption algorithms to ensure the confidentiality and integrity of the transmitted data. The goal is to hide the message inside a cover medium to remain undetectable to attackers.
2. Enhancement of steno image security: The proposed approach aims to increase the security of the steno image by minimizing any visual differences between the cover image and the steno image. This helps to prevent visual attacks that may reveal the presence of hidden data.
3. Integration of encryption algorithms: The research paper utilizes advanced encryption algorithms such as AES (Advanced Encryption Standard) and Blowfish to protect the content of the hidden message. Encrypting the message prevents unauthorized individuals from accessing and using confidential information.

The remainder of the paper is organized as follows. Section 2 discusses the related work, and Section 3 presents the methods. Section 4 describes the result and discussion, and, finally, we conclude the paper with future research directions in Section 5.

2. Related Work

The symmetric encryption technique is one of the oldest and most famous methods of maintaining data security; the secret key can be a text or several random characters. The secret key is implemented by a text message to change its content [17]. The method

of encryption used in this technique is to convert each character to several alphabetic characters when the sender and recipient know the keys of all parties and then use the secret key to encrypt and decrypt the message. Blowfish is an encryption technique, more specifically a block cipher. It is frequently referred to as a cipher. Blowfish uses keys ranging from 3 to 2448 bits and has a 64-bit block size. Its creator, Bruce Schneier, claims it is free to use, open source, and royalty free. Although Blowfish is utilized in several cipher suites and encryption methods, AES is often employed. Blowfish is secure since no cryptanalysis attempt has succeeded [18,19].

The tool (AES) was chosen because it meets our objectives. We need a powerful encryption mechanism without the complexity of sharing multiple keys as asymmetric encryption, especially when demanding to send the parameter required for extracting the data on a secure tunnel. AES is a symmetric block encryption that uses a 128-bit encryption key, which is very hard to break. Also, the block encryption mechanism makes it possible to predict the encryption data using their language characteristic since it replaces the same data block with different coding types and sizes each time. The AES overcomes the short key use by 3DES and other symmetric encryption, which is technically the best choice for our proposed algorithm [20]. Text steganography principles can be applied to a standard text file by hiding the message in the header information of the file. Using it this way helps maintain the original text file and keep it the same without any change in the content itself; on the other hand, this mechanism increases the size of the file. Another mechanism replaces bits of the text file content and changes the original text, but it is not widely used since it makes the text unreadable. Text steganography can also be applied to PDF documents or other text standards [21].

The Least Significant Bit (LSB) is implemented by replacing the least significant bit in the cover image with the bit from a secret message; the LSB method hides the binary values '101100101' in a 24-bit image. The algorithm starts by uploading the cover image and the secret message, and then an end marker represented by an array of characters is added to the secret message [22]. This is performed to allow the awareness of the recovery phase of when to stop recovering in case the secret message bit's numbers do not need the full cover image pixels to be hidden since, in this case, the recovery tool continues to extract wrong data if no ending marker is found. After that, the algorithm receives each character in the secret message using a loop. It converts it to a binary value and selects three sequence pixels from the cover image based on the index of the count parameter, which starts from zero and is incremented each time a pixel is selected. Later, the algorithm extracts the three-colour components, R, G, and B, for each pixel chosen and converts each colour component to a binary value. It masks the least bit of each colour component to zero by applying (AND with 11111110). This allows the replacement of the secret character binary bits by the least bit in each colour component, which is performed later by applying XOR with one bit from the selected character bits. It is worth mentioning that the least significant bit (LSB) algorithm has been improved using the selected least considerable bit (SLSB); these techniques proposed to enhance the performance of the LSB method by hiding information only in one of the three colours at each pixel of the cover image to reduce the chance of the confidential data being detected [23,24].

Peak signal-to-noise ratio (PSNR) measures the quality of the stego image compared with the cover image in decibels. The higher the PSNR, the better the quality. Where MAX is the maximum possible pixel value of the image, this metric describes the proportion of a signal's maximal strength to the power of corrupting noise that compromises the accuracy of its representation. This metric determines signal reconstruction quality, like video coding and data encoding [25].

Visual attack is the only stego attack that allows attackers visual analysis of the stego image. The most common attack of this type is the display of the least significant bit of an object as a binary image and analysis of the resulting image for differences between pixel shows. This attack is too slow and expensive [26]. A statistical attack assumes that the least significant bit of the cover file is random. This attack aims to compare the frequency

distribution of the potential cover file with the expected distribution of the cover file. If the new data are not the same as the statistical data expected to contain the standard data, then it probably contains confidential data. It is worth mentioning that the distribution analysis is performed via mathematical methods like the standard deviation of the image histogram, which makes the analysis much faster and widely used [27]. Compared to some state-of-the-art techniques, the proposed method has demonstrated improved perceptual transparency measures, such as peak signal-to-noise ratio and the structural similarity index. Additionally, the proposed method has exhibited high resistance to stego attacks, such as pixel difference histograms and regular and singular analysis. The out-of-boundary pixel issue in many current data-hiding techniques has also been effectively addressed in work [28]. The study of information hiding holds great significance in data security. With the advancements in computational technology, covert communication methods have become widely recognized among researchers and common data communication participants.

Image steganography is one of the top choices among experts in data hiding. The biggest challenge in designing a steganographic system is to balance measures such as the quality of the cover image, capacity, and robustness to various attacks [29]. This study aims to comprehensively review various existing image steganography techniques concerning their performance evaluation standards. The challenges faced and the future directions of this field are also discussed [30]. A comprehensive performance evaluation of reversible image steganography techniques was conducted. Techniques from the past two decades were compared using standard test images, with PSNR and embedding capacity as the evaluation parameters. The results of each technique were tabulated, analyzed, and compared to provide a clear understanding of their performance. Descriptive statistics and an in-depth analysis were also performed to assess these past techniques of the standard test [31]. A study was conducted on the scaling parameter, alpha, in the context of image steganography. Various cover and payload images, including live images from a webcam, were preprocessed and normalized. The cover and payload images were then subjected to Haar Discrete Wavelet Transformation (DWT).

The payload image was encrypted and combined with the cover image to form the stego image. The performance of the stego image was evaluated using metrics such as PSNR, MSE, and Entropy [32]. This article highlights the importance of establishing a secure organization facing significant industrial and regulatory demands. The widespread use of Wi-Fi networks for remote access to various resources and devices makes them an essential component of modern organizations. Security measures must be taken to mitigate Wi-Fi risks and prevent hacking attempts. This article provides an overview of essential security measures for different organizational contexts to ensure a secure organizational environment.

A case study is also analyzed to illustrate the minimal measures that organizations require to build network security [33]. This study presents a hybrid shorthand approach that combines the LSB steganography technique with the RSA and Caesar Cipher encryption algorithms. This combination aims to increase the security of protected information and ensure the confidentiality of secret communications. The effectiveness of the proposed scheme has been demonstrated through experimental results, which have shown that the quality of the cover image remains intact and is indistinguishable from the original image while providing a high level of security [34]. As a result of the tremendous advances in digital communications and media, 3D models have become the core of various applications in diverse fields. Consequently, these models can be utilized in steganography, acting as secure and innocent host media for sheltering covert data. In this paper, the Blowfish encryption algorithm is performed on confidential data for higher security [28,35–38]. The work described in the related works fails to include the benefits of LSB and AES advantage. Therefore, we combined and developed a hybrid approach.

3. Method

The cover images serve as containers for concealing classified multimedia information from potential attackers. In this approach, the hidden capacity of the cover image is divided, with 50% of the storage area allocated for the stego file. Within this allocation, 25% is utilized for inserting the secret message, while the remaining 25% is dedicated to storing decoy data, which is used to test credibility. The stego value, obtained from the image during the upload function, acts as a key for encryption/decryption and serves as a basis for a specific algorithm. The secret message is encrypted using Blowfish and AES methods and embedded in the cover image during the embedding process. The encryption key is derived from the stego value, ensuring that any alterations to the image are capable of preventing successful key extraction and message decryption. The length of the encryption and decryption keys varies depending on the size of the cover image, as it is derived from the mask value obtained from the image. To counter visual and statistical attacks, the secret message is divided into multiple parts and strategically inserted into different segments of the cover image. To minimize noise and maintain the integrity of the embedded message, it undergoes compression before insertion into the image. The process involves calculating the message and image size and determining the segment number and split used within the image. When comparing the cover image with the resulting stego image, the Peak Signal-to-Noise Ratio (PSNR) is used as a measure of similarity. If the PSNR is not identical, the secret message extraction is not performed, as it is contingent on the encryption key derived from the mask value. Additionally, the histogram and weight of the image are calculated to ensure the integrity and confidentiality of the stego image and the embedded secret message.

3.1. Implementation Phase

Steganography is cloaking a hidden message inside an image or cover message. One way to achieve this is to use the Least Significant Bit (LSB) approach, which entails swapping out the least significant bits of the cover picture with those from the hidden message. Figure 1 depicts the Least considerable method. We have a 480×480 colour image with the dataset, and we want to hide a secret message of 100 bits within the image using LSB steganography. The LSB approach replaces the least significant bit of each pixel in the image with a bit from the secret message. This results in a slight change in the pixel values that is not easily noticeable to the human eye, but the difference is sufficient to hide the message. To ensure the secret message's confidentiality, we encrypt it using AES encryption. For example, AES operates on data in bytes rather than bits. The cipher processes 128 bits of the incoming data at a time because each block is 128-bit long. The embedding process can be described mathematically as follows using Equation (1).

We let the original pixel value of the i th pixel be denoted by P_i , and we let the modified pixel value after embedding the secret message be represented by P'_i . The modified pixel value can be calculated using Equation (1),

$$P'_i = P_i + (2^n * m_i), \quad (1)$$

where n is the number of least significant bits used for embedding (for example, $n = 1$ for LSB), m_i is the i th bit of the secret message, and the addition is performed in modulo 2^8 (since each colour component of a pixel is typically stored as an 8-bit value). The process is similar for grayscale images, but the pixel values are 8-bit values instead of 24-bit values. Similarly, if we want to use Blowfish encryption instead of AES, the secret message would be encrypted using Blowfish, and the encrypted ciphertext would be hidden within the image using LSB steganography. This example shows how LSB steganography and encryption algorithms can be used together to hide a secret message within an image, providing both confidentiality and imperceptibility to the hidden message. Steganography and cryptography are commonly used to manipulate information and mask their presence. Intentionally, cryptography messages up to make it understood.

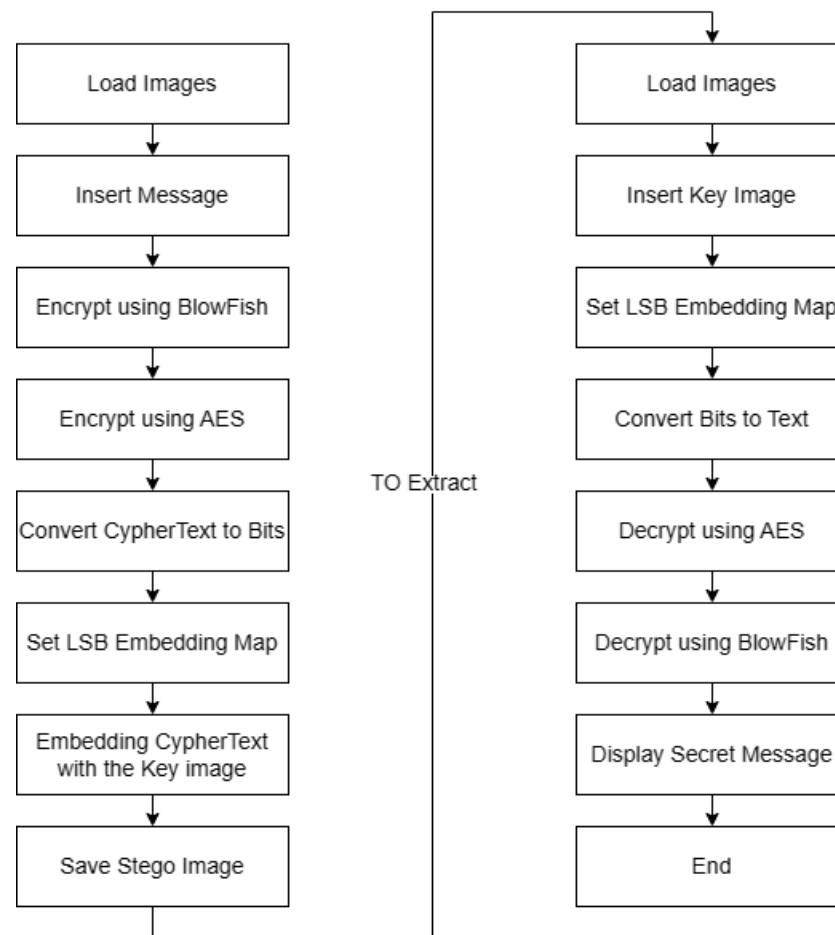


Figure 1. Least significant approach encryption and decryption process.

On the other hand, steganography masks or dissimulates the text and renders it unnoticed. Steganography is very useful if it is forbidden to use cryptography, where strong encryption is usually prohibited. Steganography can, therefore, stop these laws and transfer a text anonymously. Our research focuses on the ways a strong defensive mechanism can be developed. In cryptanalysis and steganalysis, a great effort has been made to overcome the hiding skills, so our role is to create a new technique that is more difficult to discover or defeat. The proposed model has two main functions, Embedding the Message into Cover Image and Extraction the Message from the Cover Image. The following processes are discussed: The data are securely embedded into the cover image at multiple levels using compress and encryption algorithms AES and BlowFish. The final output image combines a secret message and an image created using a dynamic transfer model.

This model adapts the key image method to calculate a cipher key and implements various data-hiding techniques to enhance security. The result is a smoothed stego image that is difficult to detect, ensuring the confidentiality of the hidden information.

The stego image accompanies a key idea as the decryption key. Upon successful upload, the decryption phase commences, followed by the decoding process, revealing the hidden message. An integrity check ensures that any changes to the image, such as an attack, did not alter the mask value and compromised the key for decryption. This helps to ensure the accuracy and security of the recovered information. The flow diagram of embedding images is shown in Figure 2. The LSB Approach:

1. The LSB approach is an essential and widely used technique in steganography.
2. It involves replacing the least significant bits of the cover media with secret data to embed information. The altered bits are typically invisible to the human eye or ear,

making it difficult to detect the hidden message. Supposing we have an image with pixel values ranging from 0 to 255, we can modify the least significant bit of each pixel to hide a secret message using the LSB approach. For instance, if the pixel value is 110 (in binary: 01101110), and we want to embed a bit of 1, we can change the LSB to 1 (01101111). This slight modification is often visually indistinguishable, especially with large cover media such as images or audio files.

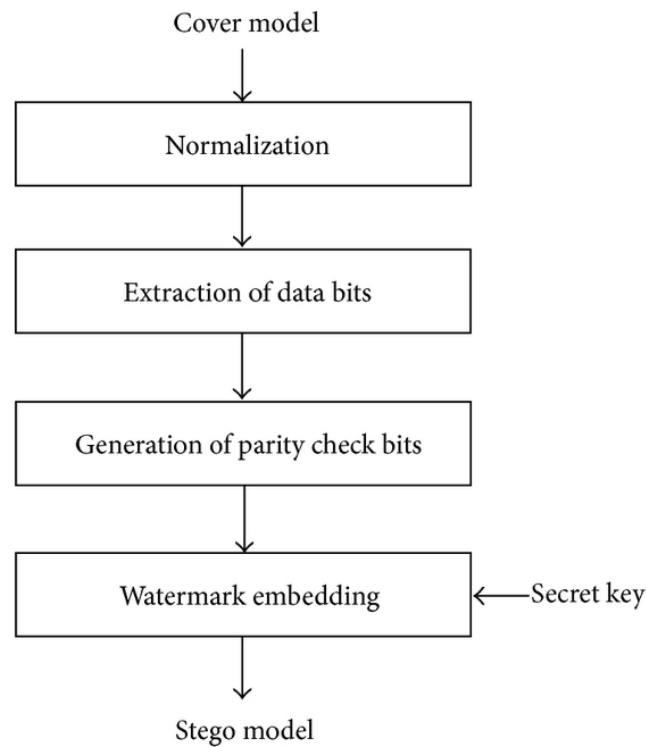


Figure 2. Flow diagram of embedding images.

3.2. The Hybrid Approach with LSB

A hybrid Image Encryption Using Cryptography Steganography (Image Steganography using LSB and Hybrid Encryption Algorithms (Algorithm 1)) combines two techniques: Least Significant Bit (LSB) steganography and hybrid encryption. LSB steganography is a commonly used technique for hiding secret messages within images. It works by replacing the least significant bits of the cover image with the secret message bits. The least significant bits of an image is the least important bits of the colour values of each pixel, and changing them is unlikely to cause a noticeable change in the image. This makes LSB steganography a good option for hiding secret messages within images without altering the appearance of the cover image. Hybrid encryption is a method of encryption that combines two or more encryption techniques to provide a higher level of security. In this research, using LSB steganography, the hybrid encryption approach is used to encrypt the secret message before it is hidden within the cover image. This means that the secret message is encrypted using a combination of encryption algorithms, providing higher security than when using only one encryption algorithm.

For example, we consider a scenario where an individual wants to send a secret message to a friend. The individual can use LSB steganography to hide the secret message within a cover image and then use hybrid encryption to encrypt the hidden message. The individual can send the cover image to a friend, who can then use the decryption key to decode the encrypted secret message and extract it from the cover image using the LSB steganography technique. The LSB approach would replace the least significant bits of the cover image with the encrypted secret message. For example, if the pixel values of a colour

image are represented in an 8-bit format, the least significant bit could be replaced with the corresponding bits of the encrypted secret message. Figure 3 depicts the hybrid approach with LSB. The hybrid approach with LSB encryption is given below.

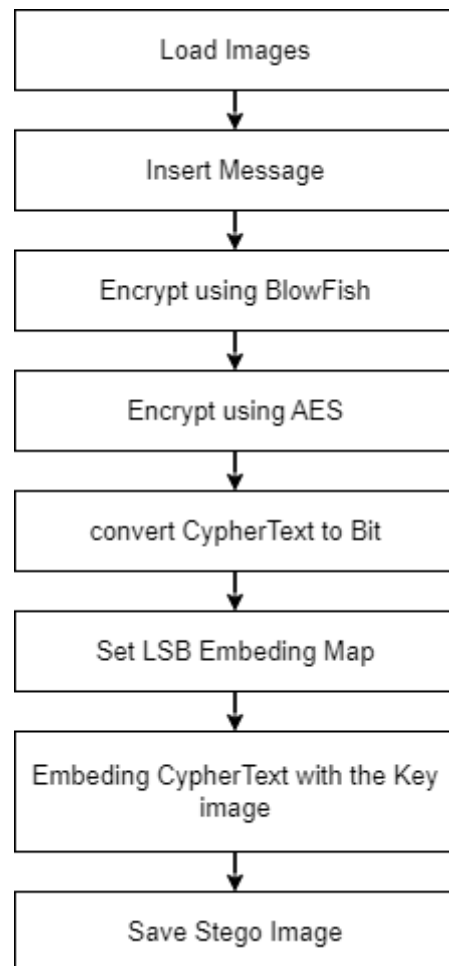


Figure 3. Hybrid approach with LSB encryption and Embedding image process.

The resulting stego image appears visually similar to the cover image while concealing the secret message within the least significant bits. To further improve the security of the hidden message, AES and Blowfish algorithms could be used in a hybrid encryption scheme. The secret message is first encrypted using AES, and the resulting ciphertext is then encrypted using Blowfish. The final encrypted message is then hidden within the LSBs of the cover image. This hybrid approach offers the advantages of both AES and Blowfish, with AES providing strong encryption for sensitive data and Blowfish providing fast and secure encryption for large amounts of data. The process is similar to a grey-scale image, with the difference being that the pixel values are represented in an 8-bit or a 16-bit format, depending on the image resolution. The encrypted secret message is then hidden within the LSBs of the grayscale image.

Algorithm 1 Hybrid approach with LSB encryption.

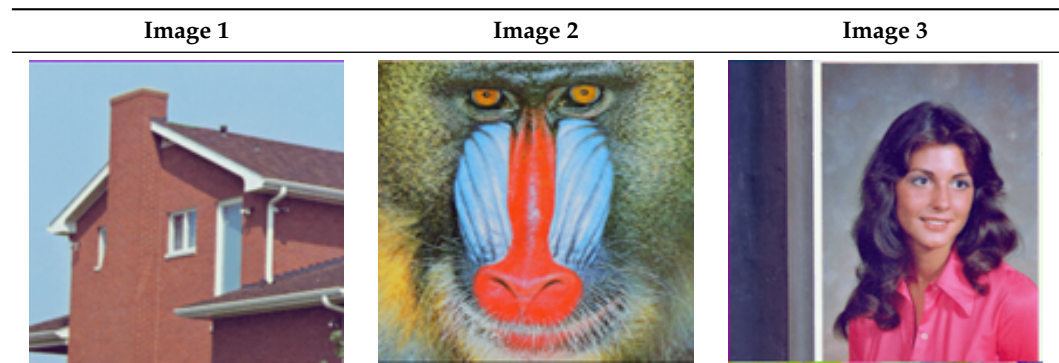
```

1.  function hybridImageEncryption(originalImage, secretMessage):
    encryptedMessage = hybridEncryptionAlgorithm(encrypt(secretMessage))
    stegoImage = embedMessageLSB(originalImage, encryptedMessage)
    return stegoImage
2.  function hybridImageDecryption(stegoImage):
    extractedMessage = extractMessageLSB(stegoImage)
    decryptedMessage = hybridDecryptionAlgorithm(decrypt(extractedMessage))
    return decryptedMessage
3.  function embedMessageLSB(originalImage, message):
    stegoImage = copy(originalImage)
    binaryMessage = convertToBinary(message)
    bitIndex = 0
    for each pixel in originalImage:
        if bitIndex >= length(binaryMessage):
            break
        pixelLSB = getLeastSignificantBit(pixel)
        modifiedPixel = setLeastSignificantBit(pixel, binaryMessage[bitIndex])
        stegoImage.setPixel(modifiedPixel)
        bitIndex = bitIndex + 1
    return stegoImage
4.  function extractMessageLSB(stegoImage):
    extractedMessage = ""
    for each pixel in stegoImage:
        pixelLSB = getLeastSignificantBit(pixel)
        extractedMessage = extractedMessage + pixelLSB
    return extractedMessage
5.  function hybridEncryptionAlgorithm(plaintext):
    symmetricKey = generateSymmetricKey()
    encryptedSymmetricKey = asymmetricEncryptionAlgorithm(symmetricKey)
    ciphertext = AES.encrypt(plaintext, symmetricKey)
    return encryptedSymmetricKey + ciphertext
6.  function hybridDecryptionAlgorithm(ciphertext):
    encryptedSymmetricKey = extractEncryptedSymmetricKey(ciphertext)
    symmetricKey = asymmetricDecryptionAlgorithm(encryptedSymmetricKey)
    encryptedMessage = extractEncryptedMessage(ciphertext)
    decryptedMessage = AES.decrypt(encryptedMessage, symmetricKey)
    return decryptedMessage
7.  function encrypt(message):
8.  Perform encryption on the message using a specific Hybrid encryption algorithm
9.  function decrypt(ciphertext):

```

3.3. Data Example

An evaluation of the three significant properties of any image steganography technique, undetectability, level of security, and capacity, was obtained to characterize the strengths and weaknesses of the proposed method. Table 1 presents the cover images used to test the proposed technique.

Table 1. The cover images that were used to evaluate the proposed method.

4. Results and Discussion

The embedding and extracting algorithms were implemented using Python 3.6 on VScode IDE utilising a web page and applied to bitmapped images with 256 colours of the same size (500×500) with a 24-bit depth. Different secret texts were embedded to evaluate the impact of the embedding process on the images. It has to be noted that the analysis included three cover images, which were partitioned into different blocks, and two images were used as encrypted messages and secret patterns.

4.1. Implementation Results

Different secret message sizes with different hidden patterns were used to test the embedding ability of the proposed technique. Moreover, the quantity of imperceptibility and the consistency of the stego image were determined for each Peak signal-to-noise ratio (PSNR) and Mean square error (MSE). PSNR and MSE statistics with a range of secret message sizes were compared with other steganography methods and results. The test was conducted on the data example images with the same size and segment–secret message sizes. The model showed stable results with increasing the size of the secret message on the images due to the chosen high-frequency areas in each block and hiding the secret message with the spectrum disruption of the message in each block.

Table 2 presents the proposed method's results applied to three images. The secret message used in this experiment had a capacity of 480 bits. The results show that the mean squared error (MSE) and peak signal-to-noise ratio (PSNR) varied between the three images. The MSE value of Image 1 was 0.00061387, and that of the PSNR was 80.2500. Image 2 had a lower MSE value of 0.00019995 and a higher PSNR value of 85.1216. Similarly, Image 3 had an MSE value of 0.0002002 and PSNR had a value of 85.1163.

Table 2. Results on Images (Capacity, PSNR, and mean Error score)—First Message.

Secret Message	The Message		
	Capacity	MSE	PSNR
Image 1	480	0.00061387	80.2500
Image 2	480	0.00019995	85.1216
Image 3	480	0.0002002	85.1163

Table 3 presents the results of the second secret message on three different images. The results are reported in terms of capacity (bits), mean squared error (MSE), and peak signal-to-noise ratio (PSNR). Image 1's capacity was 2400 bits, and the MSE was 0.00060364, resulting in a PSNR of 80.3230. Image 2's capacity was 2400 bits, and the MSE was 0.00018866, resulting in a PSNR of 85.3740. Image 3's capacity was 2400 bits, and the MSE was 0.00018717, resulting in a PSNR of 85.4083. It can be observed from the results that for all three images, the capacity remained the same for the second message. However, the MSE and PSNR values varied among the images. A lower MSE value indicates that

the difference between the original image and the stego image (with an embedded secret message) is small, and a higher PSNR value indicates that the quality of the stego image is more elevated.

Table 3. Results on Images (Capacity, PSNR, and mean Error score)—Second message.

Secret Message	The Message		
	Capacity	MSE	PSNR
Image 1	2400	0.00060364	80.3230
Image 2	2400	0.00018866	85.3740
Image 3	2400	0.00018717	85.4083

Table 4 presents the results of the third secret message on the three images regarding capacity, mean squared error (MSE), and peak signal-to-noise ratio (PSNR). All three images had the same capacity of 4800 bits. The results show that Image 2 had the lowest MSE and highest PSNR, while Image 3 had the highest MSE and the lowest PSNR. This indicates that Image 2 had the best image quality and the slightest degradation in terms of distortion after the steganographic process was applied compared to the other two images. These results provide insights into the performance of the steganographic method for different images and can be used to improve future steganographic algorithms.

Table 4. Results on Images (Capacity, PSNR, and mean Error score) – Third Message.

Secret Message	The Message		
	Capacity	MSE	PSNR
Image 1	4800	0.0004425	81.6717
Image 2	4800	0.0001677	85.8855
Image 3	4800	0.00017741	85.6411

In Table 5, it can be seen that the first, second, and third messages were embedded in Images 1, 2, and 3. After the secret message was embedded, the results showed the PSNR and MSE values of each image. It can be observed that the PSNR values for Images 1, 2, and 3 were 80.2500, 85.1216, and 85.1163, respectively, for the first message. For the second message, the PSNR values were 80.3230, 85.3740, and 85.4083, respectively. For the third message, the PSNR values were 81.6717, 85.8855, and 85.6411, respectively. The MSE values, on the other hand, reflected the quality of the stego images. It can be seen that the MSE values decreased as the PSNR values increased, indicating that the quality of the stego images improved with the increasing PSNR values. Figure 4 depicts the summary of the proposed PSNR method results with existing methods.

Table 5. The proposed Method Result Summary.

Image	PSNR and MSE		
	First Image	Second Image	Third Image
Image 1	80.2500	80.3230	81.6717
Image 2	85.1216	85.3740	85.8855
Image 3	85.1163	85.4083	85.6411

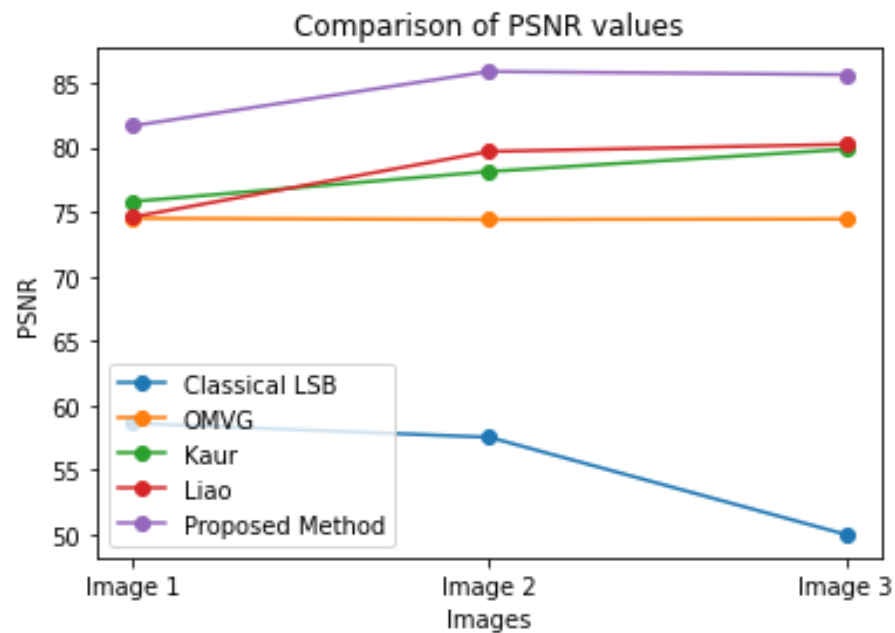


Figure 4. The Proposed Method PSNR result summary with existing methods.

4.2. Comparison with Existing Works

Table 6 presents a comparison between the proposed method and previous related works in the field of image steganography. The performance of the proposed method was evaluated and compared to those of the classical least significant bit (LSB) method, the over-multiplexed Vega (OMVG) method, the Kaur method, and the Liao method based on the Peak Signal-to-Noise Ratio (PSNR) of cover images. The results show that the proposed method outperforms the other ways regarding PSNR, with the highest values observed in Images 2 and 3, where the PSNR reached 85.8855 and 85.6411, respectively. In contrast, the classical LSB method had the lowest PSNR values among the comparison methods, with PSNR values ranging from 50 to 58.62 in Images 1 to 3.

Table 6. Comparison between the proposed model and the related work for PSNR .

Image	Classical LBS [39]	OMVG Method [40]	Kaur [41]	Liao [42]	The Proposed Method
	PSNR	PSNR	PSNR	PSNR	PSNR
Image 1	58.62	74.50	75.8	74.6	81.6717
Image 2	57.53	74.41	78.13	79.68	85.8855
Image 3	50.00	74.45	79.85	80.24	85.6411

4.3. Run Time Results

The run time results and comparison between the proposed method and those of other researchers are displayed below. The results are based on the average run time across all image types. The proposed method, which uses encryption algorithms BlowFish and AES, demonstrates impressive run time performance on average. The results are as follows.

Table 7 compares the run time of the proposed method with those of the related work in terms of encryption and decryption processes. The proposed method has a shorter run time than the classical LSB and OMVG methods, with a run time of 0.83 s for encryption and 1.5 s for decryption. It also has a slightly shorter run time compared to the Kaur and Liao methods, which have run times of 1.254 s and 1.54 s, respectively, for encryption and 1.642 s and 1.5 s, respectively, for decryption. This demonstrates the proposed method's

efficiency in terms of security and speed. Figure 5 compares the proposed model and the related work for run time.

Table 7. Run time comparison proposed model and related work (seconds).

Process type	Classical LBS [39]	OMVG Method [40]	Kaur [41]	Liao [42]	The Proposed Method
Encryption	1.874	1.012	1.254	0.98	0.83
Decryption	2.018	1.492	1.642	1.54	1.5

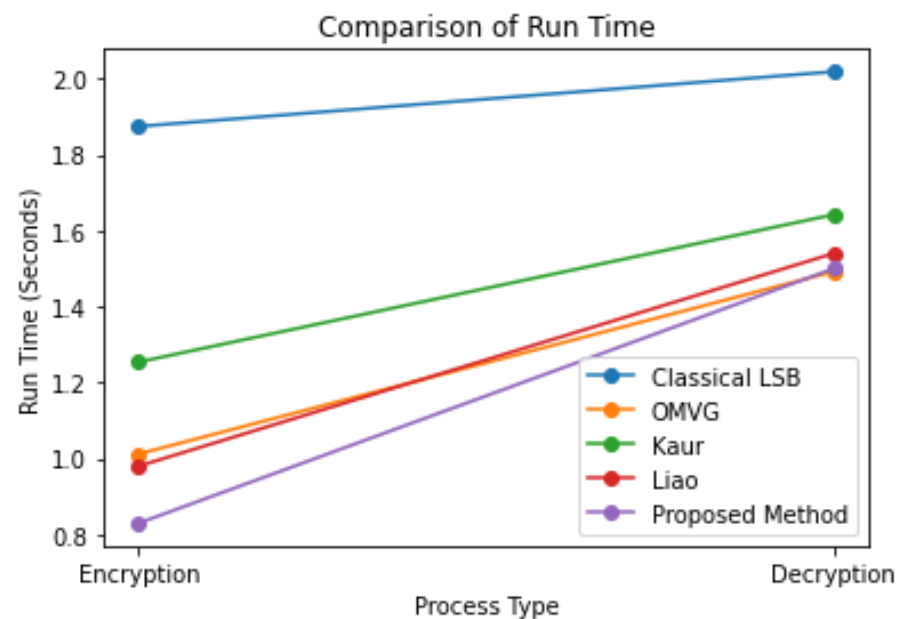








Figure 5. Comparison between the proposed model and the related work for run time.

4.4. Visual and Statistical Test

The small colour changes between the cover and stego images are nearly invisible to the human eye, which is a crucial aspect of successful picture steganography. This ability to conceal the changes is a testament to the effectiveness of the technology proposed. Table 8 depicts the visual effects on the data example images. The subtle colour shifts in a stego image can often remain unnoticed, making it challenging to detect the presence of hidden information. To overcome this challenge, a histogram comparison technique is utilized to distinguish between the cover and stego images. This is achieved by comparing the histogram of the cover image with that of the stego image.

The experiments conducted and the individual histograms drawn for both the cover and stego images demonstrate the effectiveness of this technique. Figures 6–11 display the histograms of the RGB channels of both the cover image and the stego image, as opposed to the histograms of just the Red, Green, and Blue channels, as their forms tend to remain similar even with the highest amount of secret data input.

Table 8. Display of visual effects on the data example images.

Cover Image	Stego Image
Image 1	Image 1
	
Image 2	Image 2
	
Image 3	Image 3
	

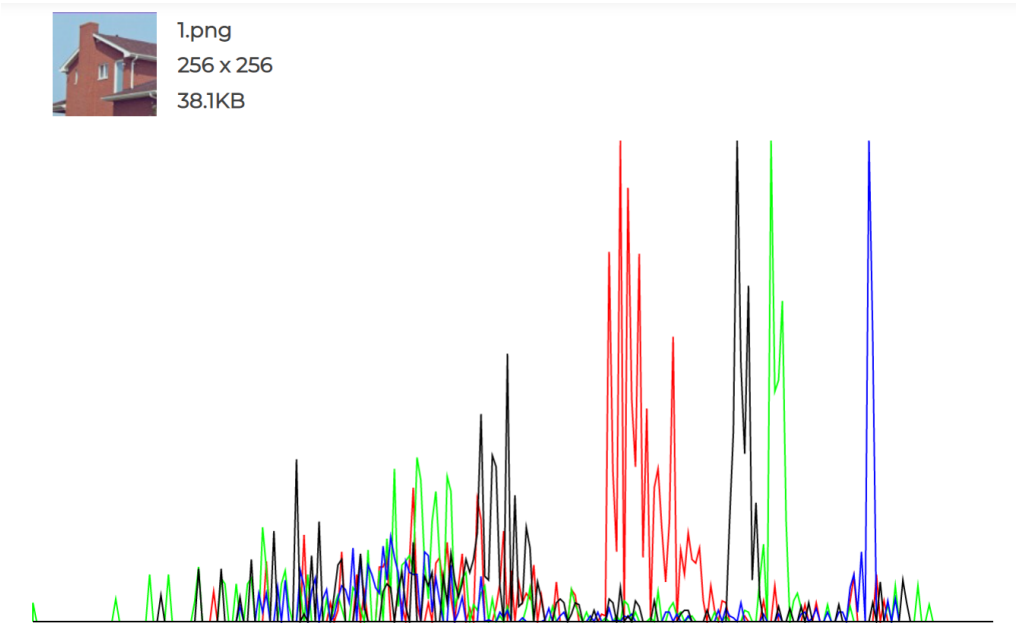


Figure 6. Original Image 1 histogram.

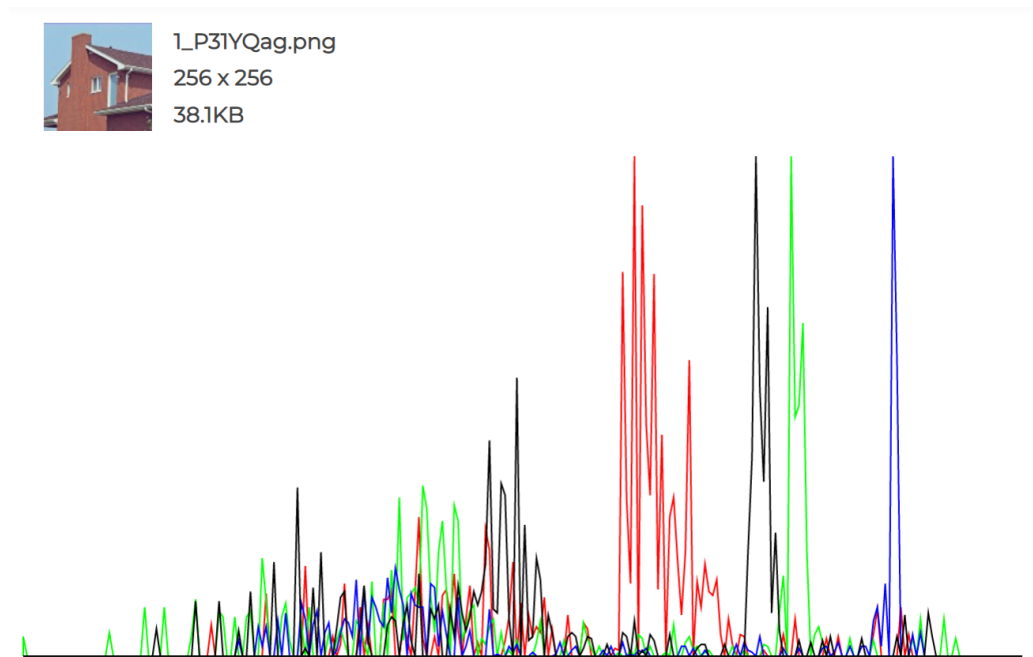


Figure 7. Cover Image 1 histogram.

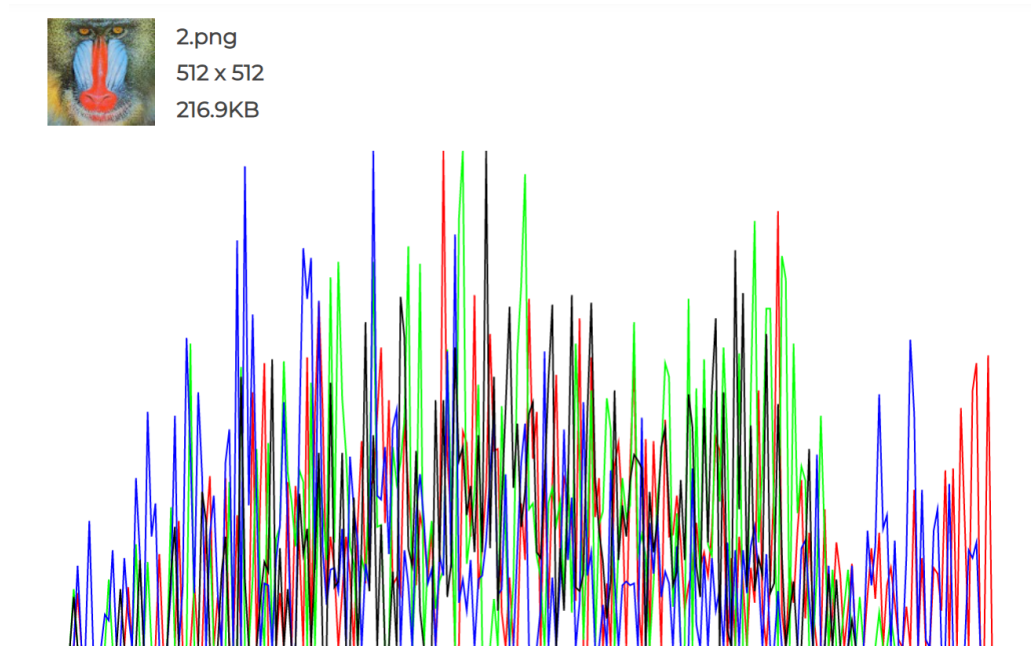


Figure 8. Original Image 2 histogram.

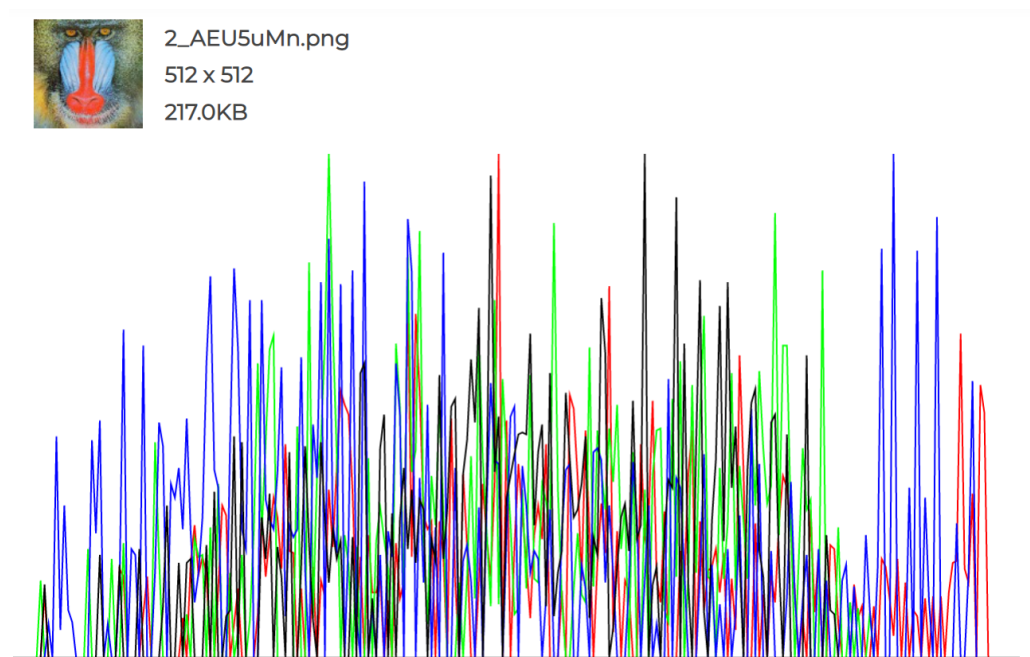


Figure 9. Cover Image 2 histogram.

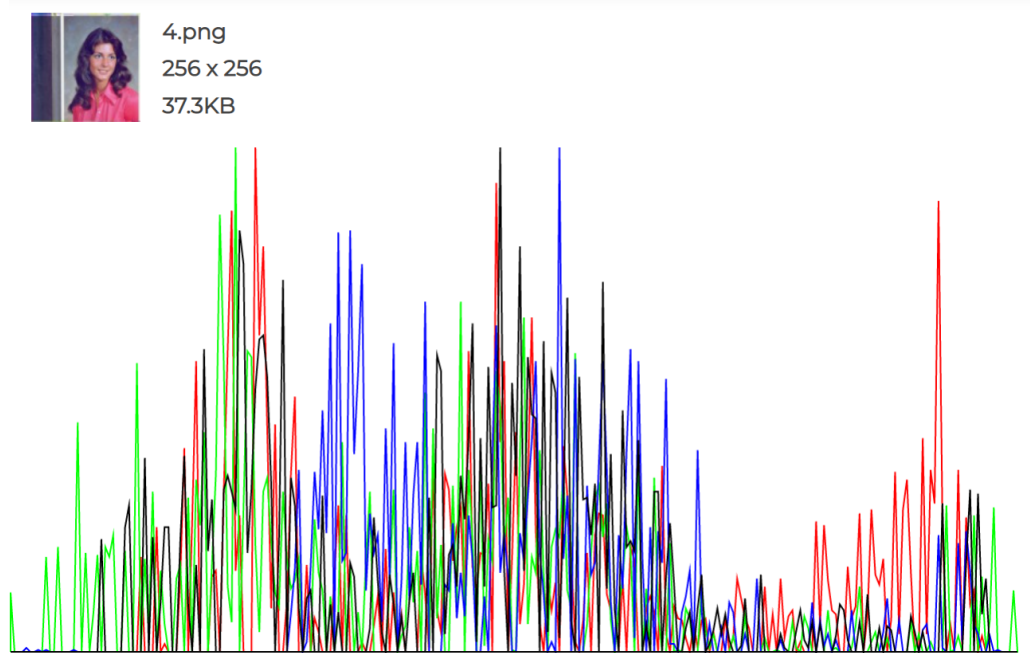


Figure 10. Original Image 3 histogram.

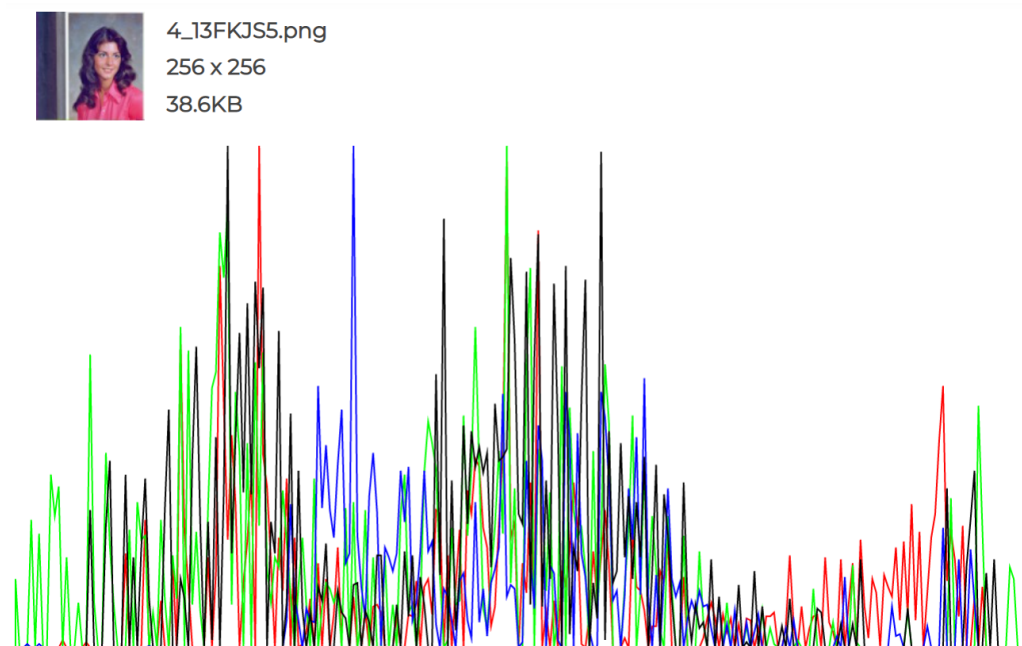


Figure 11. Cover Image 3 histogram.

4.5. Level of Security

A brutal force attack is one of the common image technique attacks. It means thoroughly monitoring all possible stego keys until a correct one is recognized. The first element of the Stego key, a predefined pattern, can be selected from an unlimited number of images over the web, mobile telephones, computers, etc., in the steganography technique suggested. Hence, the number of distinct hidden patterns is very high. In addition to the secret pattern, the attacker should be aware of the secret message size to insert the secret text, given that the secret pattern size is connected with the secret message size. The text is also inserted in a random order based on a colour range distribution of the hidden design and the number of pixels matched. However, using a stego key, it is hard to retrieve the hidden text by searching for a particular example in a picture in stego in which the embedded order is executed, because the text is concealed in different addresses on each block according to the cover attributes and the secret pattern used. This research presents a new approach to steganography based on the LSB technique, which uses AES and BlowFish encryption algorithms to conceal text inside an image. The proposed method takes into account the limitations of the LSB process. It improves upon them through randomization in pixel selection and a mask as a password encryption key. This method is expected to be further improved with advancements in encryption and compression algorithms, as well as the implementation of machine learning and AI to enhance its resistance against cryptanalysis and steganalysis attacks. The user interface should also be improved to make it more user-friendly and customizable for different users. The proposed method effectively addresses the two limitations of traditional LSB (Least Significant Bit) processes by incorporating a secret key based on the image and dividing the image into smaller blocks. This not only adds an extra layer of security to the hidden text through the use of a mask as both a password encryption key and as a minimum bit shift during data hiding, but also reduces the visual impact of the embedded text. Furthermore, by splitting the image into N frames and disconnecting it from its sequential order, the proposed method increases its resistance to attacks and enhances its overall security. This approach can be improved in future work by adjusting the dimensions of the masks used. The current limitation of the proposed method is that it needs to be enhanced by a more complex encoding method. The improvement should focus on the encryption and decryption algorithms, making them faster using a lightweight algorithm. Additionally, a compression algorithm should be applied to more significant messages to reduce the message size. Machine learning and AI

should test the method against cryptanalysis and steganalysis attacks. The model's GUI should also be enhanced to be more user friendly and usable, with added options to control desired processes.

5. Conclusions

This research introduces a novel steganography approach based on the Least Significant Bit (LSB) technique, employing AES and Blowfish encryption algorithms to conceal text within an image. The proposed method addresses the limitations of traditional LSB processes by incorporating randomization in pixel selection and utilizing a mask as a password encryption key. Future advancements in encryption and compression algorithms, along with machine learning and AI integration, are expected to enhance the method's resistance against cryptanalysis and steganalysis attacks. The user interface will also be improved to enhance user friendliness and customization for different user needs. The proposed method effectively overcomes two limitations of traditional LSB processes by incorporating a secret key derived from the image and dividing the image into smaller blocks. This enhances security by using a mask as both a password encryption key and a minimum bit shift during data hiding while minimizing the visual impact of the embedded text. By splitting the image into multiple frames and eliminating sequential order, the proposed method enhances resistance to attacks and overall security. Future work aims to optimize the dimensions of the masks used in the method. The current limitation lies in the complexity of the encoding method, which will be addressed by introducing faster, lightweight encryption and decryption algorithms. A compression algorithm will also be applied to more significant messages to reduce size. Machine learning and AI techniques will evaluate the method's robustness against cryptanalysis and steganalysis attacks. The graphical user interface (GUI) will be enhanced to be more user friendly, offering additional options for controlling desired processes.

Author Contributions: Formal analysis, M.A.; Data curation, B.A.; Writing—original draft, R.A.; Supervision, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: No animals/humans were used for studies that are the basis of this research.

Data Availability Statement: Not applicable.

Acknowledgments: The authors express their gratitude to the Deanship of Research and Graduate Studies and the Faculty of Computers and Information Technology at the University of Tabuk for their invaluable support to this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rizi, M.H.P.; Seno, S.A.H. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet Things* **2022**, *20*, 100584. [\[CrossRef\]](#)
2. Saini, R.; Joshi, K.; Punyani, K.; Yadav, R.; Nandal, R.; Kumari, D. Interpolated Implicit Pixel-based Novel Hybrid Approach Towards Image Steganography. *Recent Adv. Electr. Electron. Eng. (Former. Recent Patents Electr. Electron. Eng.)* **2023**, *16*, 851–871. [\[CrossRef\]](#)
3. Vaishnavi, A.; Pillai, S. Cybersecurity in the Quantum Era-A Study of Perceived Risks in Conventional Cryptography and Discussion on Post Quantum Methods. *J. Phys. Conf. Ser.* **2021**, *1964*, 042002. [\[CrossRef\]](#)
4. Anthoniraj, S.; Karthikeyan, P.; Vivek, V. Weed Detection Model Using the Generative Adversarial Network and Deep Convolutional Neural Network. *J. Mob. Multimedia* **2022**, *18*, 275–292. [\[CrossRef\]](#)
5. Majeed, M.A.; Sulaiman, R.; Shukur, Z.; Hasan, M.K. A review on text steganography techniques. *Mathematics* **2021**, *9*, 2829. [\[CrossRef\]](#)
6. Belagali, P.; Udupi, V. Robust Image Steganography Based on Hybrid Edge Detection. *Tuijin Jishu/J. Propuls. Technol.* **2023**, *44*, 1509–1521.

7. Bilgaiyan, S.; Ahmad, R.; Sagnika, S. Adaptive image steganography using rotating color channels and inverted LSB substitution. *SN Comput. Sci.* **2023**, *4*, 565. [\[CrossRef\]](#)
8. ALRikabi, H.T.S.; Hazim, H.T. Enhanced data security of communication system using combined encryption and steganography. *ijIM* **2021**, *15*, 145. [\[CrossRef\]](#)
9. Nasution, R.I.H.; Fauzi, A.; Khair, H. Hybrid Cryptosystem Algorithm Vigenere Cipher and Base64 for Text Message Security Utilizing Least Significant Bit (LSB) Steganography as Insert into Image. *J. Artif. Intell. Eng. Appl. (JAIEA)* **2023**, *2*, 89–98. [\[CrossRef\]](#)
10. Manimurugan, S. IoT-Fog-Cloud model for anomaly detection using improved Naïve Bayes and principal component analysis. *J. Ambient. Intell. Humaniz. Comput.* **2021**, 1–10. [\[CrossRef\]](#)
11. Pelosi, M.; Easttom, C. Identification of LSB image steganography using cover image comparisons. *J. Digit. Forensics Secur. Law* **2021**, *15*, 6. [\[CrossRef\]](#)
12. Velliangiri, S.; Manoharn, R.; Ramachandran, S.; Venkatesan, K.; Rajasekar, V.; Karthikeyan, P.; Kumar, P.; Kumar, A.; Dhanabalan, S.S. An efficient lightweight privacy-preserving mechanism for industry 4.0 based on elliptic curve cryptography. *IEEE Trans. Ind. Inform.* **2021**, *18*, 6494–6502. [\[CrossRef\]](#)
13. Oswal, D.; Parmar, G.; Patidar, H.K.; Badbadwal, K.; Shukla, P. Secure File Using Steganography. 2022.
14. Shyla, M.; Kumar, K.S.; Das, R.K. Image steganography using genetic algorithm for cover image selection and embedding. *Soft Comput. Lett.* **2021**, *3*, 100021. [\[CrossRef\]](#)
15. Yang, A.; Bai, Y.; Xue, T.; Li, Y.; Li, J. A novel image steganography algorithm based on hybrid machine learning and its application in cyberspace security. *Future Gener. Comput. Syst.* **2023**, *145*, 293–302. [\[CrossRef\]](#)
16. Manimurugan, S.; Al-Mutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access* **2020**, *8*, 77396–77404. [\[CrossRef\]](#)
17. Rajasekar, V.; Premalatha, J.; Dhanaraj, R.K.; Geman, O. Introduction to Classical Cryptography. In *Quantum Blockchain: An Emerging Cryptographic Paradigm*; John Wiley & Sons, Inc.: Hoboken, NJ, USA, 2022; pp. 1–29.
18. Aumasson, J.P. *Crypto Dictionary: 500 Tasty Tidbits for the Curious Cryptographer*; No Starch Press: San Francisco, CA, USA, 2021.
19. Saad Almutairi, S. Manimurugan, M.A. A new secure transmission scheme between senders and receivers using HVCHC without any loss. *EURASIP J. Wirel. Commun. Netw.* **2019**, 2019, 1–15.
20. Altigani, A.; Hasan, S.; Barry, B.; Naserelden, S.; Elsadig, M.A.; Elshoush, H.T. A polymorphic advanced encryption standard—a novel approach. *IEEE Access* **2021**, *9*, 20191–20207. [\[CrossRef\]](#)
21. Semenchenko, O.; Iakovenko, O.; Lekakh, A.; Parkhomenko, M.; Podlesny, S.; Karaban, O. The Analysis of the Codes in the Textual Steganography Technologies. In Proceedings of the 2021 IEEE 3rd International Conference on Advanced Trends in Information Theory (ATIT), Kyiv, Ukraine, 15–17 December 2021; pp. 31–35.
22. Pandey, D.; Wairya, S.; Al Mahdawi, R.S.; Najim, S.A.D.M.; Khalaf, H.A.; Al Barzinji, S.M.; Obaid, A.J. Secret data transmission using advanced steganography and image compression. *Int. J. Nonlinear Anal. Appl.* **2021**, *12*, 1243–1257.
23. Xian, Y.J.; Wang, X.Y.; Zhang, Y.Q.; Wang, X.Y.; Du, X.H. Fractal sorting vector-based least significant bit chaotic permutation for image encryption. *Chin. Phys. B* **2021**, *30*, 060508. [\[CrossRef\]](#)
24. Yang, D. Correlogram, predictability error growth, and bounds of mean square error of solar irradiance forecasts. *Renew. Sustain. Energy Rev.* **2022**, *167*, 112736. [\[CrossRef\]](#)
25. Anjum, U.; Hussain, A.; Ali, C.B.; Afzal, U.; Hussain, I.; Noorwali, A.; Shah, S.A. JPEG Image Compression Using Multiple Core Strategy in FPGA achieving High Peak Signal to Noise Ratios. In Proceedings of the 2021 International Congress of Advanced Technology and Engineering (ICOTEN), Taiz, Yemen, 4–5 July 2021; pp. 1–6.
26. Vennam, P.; TC, P.; BM, T.; Kim, Y.G.; BN, P.K. Attacks and preventive measures on video surveillance systems: A review. *Appl. Sci.* **2021**, *11*, 5571. [\[CrossRef\]](#)
27. Mustafa, M.S. An Effect Image Steganography System Based on Pixels Disparity Value and Secret Message Compression. Master's Thesis, Altınbaş Üniversitesi/Lisansüstü Eğitim Enstitüsü, Istanbul, Turkey, 2022.
28. Sahu, M.; Padhy, N.; Gantayat, S.S.; Sahu, A.K. Local binary pattern-based reversible data hiding. *CAAI Trans. Intell. Technol.* **2022**, *7*, 695–709. [\[CrossRef\]](#)
29. Sahu, M.; Padhy, N.; Gantayat, S.S.; Sahu, A.K. Performance analysis of various image steganography techniques. In Proceedings of the 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA), Gunupur, India, 8 September 2022; pp. 1–6.
30. Malarvizhi, N.; Priya, R.; Bhavani, R. Reversible Image Steganography Techniques: A Performance Study. In Proceedings of the 2022 7th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 22–24 June 2022; pp. 780–787.
31. Tevaramani, S.S.; Ravi, J. Image steganography performance analysis using discrete wavelet transform and alpha blending for secure communication. *Glob. Trans. Proc.* **2022**, *3*, 208–214. [\[CrossRef\]](#)
32. Sundaram, B.B.; Kannaiya Raja, N.; Sreenivas, N.; Mishra, M.K.; Pattanaik, B.; Karthika, P. RSA algorithm using performance analysis of steganography techniques in network security. In Proceedings of the International Conference on Communication, Computing and Electronics Systems: Proceedings of ICCES 2020, Coimbatore, India, 21–22 October 2021; pp. 713–719.

33. Diop, I.; Tall, K. A New hybrid approach of Data Hiding Using LSB Steganography and Caesar cipher and RSA algorithm (S-ccr). In Proceedings of the 2022 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 25–27 January 2022; pp. 1–4.
34. Hummady, M.M.; Morad, A.H. Enhancement of System Security by Using LSB and RSA Algorithms. *Al-Khwarizmi Eng. J.* **2022**, *18*, 26–37. [[CrossRef](#)]
35. Farrag, S.; Alexan, W. A high capacity geometrical domain based 3d image steganography scheme. In Proceedings of the 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, 12–14 April 2019; pp. 1–7.
36. Min-Allah, N.; Nagy, N.; Aljabri, M.; Alkharraa, M.; Alqahtani, M.; Alghamdi, D.; Sabri, R.; Alshaikh, R. Quantum Image Steganography Schemes for Data Hiding: A Survey. *Appl. Sci.* **2022**, *12*, 10294. [[CrossRef](#)]
37. Tariq, S.; Shoukat, I.A.; Iqbal, U.; Faheem, M.R. Hybrid Image Steganography Method with Random Embedding of Encrypted Message.
38. Belagali, P.; Udupi, V. Image Steganography based on Enhanced Payload Capacity using Hybrid Edge Detection and Least Significant Bit Steganography. *J. Harbin Eng. Univ.* **2023**, *44*, 1953–1960.
39. Yao, J.L.; Yang, H.M.; Jiang, D.H.; Yan, B.; Pan, J.S.; Wang, M.X. A Novel Quantum Image Steganography Algorithm Based on Double-Layer Gray Code. *Int. J. Theor. Phys.* **2023**, *62*, 52. [[CrossRef](#)]
40. Yousefzadeh, A.; Jabłoński, M.; Iakymchuk, T.; Linares-Barranco, A.; Rosado, A.; Plana, L.A.; Serrano-Gotarredona, T.; Furber, S.; Linares-Barranco, B. Multiplexing AER asynchronous channels over LVDS links with flow-control and clock-correction for scalable neuromorphic systems. In Proceedings of the 2017 IEEE International Symposium on Circuits and Systems (ISCAS), Baltimore, MD, USA, 28–31 May 2017; pp. 1–4.
41. Kaur, S.P.; Singh, S. A Digital Steganography Technique Using Hybrid Encryption Methods for Secure Communication. In Proceedings of the International Conference on Information Technology and Applications: ICITA 2022, Lisbon, Portugal, 20–22 October 2022; pp. 481–489.
42. Yang, Y.G.; Wang, B.P.; Zhou, Y.H.; Shi, W.M.; Liao, X. Efficient color image encryption by color-grayscale conversion based on steganography. *Multimed. Tools Appl.* **2023**, *82*, 10835–10866. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.