International Journal of Safety and Security Engineering
Vol. 15, No. 8, August, 2025, pp. 1723-1731
Journal homepage: http://iieta.org/journals/ijsse

Enhanced Steganographic Framework for Secure Communications

Asmaa Alqassab*, Younis Al-Arbo

Department of Computer Science, College of Education for Pure Science, University of Mosul, Mosul 41002, Iraq

Corresponding Author Email: asmaa_mow@uomosul.edu.iq

https://doi.org/10.18280/ijsse.150817

Received: 25 July 2025
Revised: 20 August 2025
Accepted: 25 August 2025
Available online: 31 August 2025

Keywords:
image steganography, LSB, data hiding, Caesar Cipher, XOR encryption, RGB decomposition

ABSTRACT

In the current digital era of increasing frequency and growing complexity of cyber-attacks, our top priority is to secure the sensitive information throughout the interconnected world. Covert communication techniques help in hiding the existence of our communication, which can make our channel more secure. This paper has introduced a new steganographic framework that combines the traditional Least Significant Bit (LSB) steganographic technique by embedding into the three LSBs of the information. The proposed approach deals with a message encryption technique and the embedding algorithm to provide robust data concealing. The red, green, and blue (RGB) image has been broken into its components, while the secret data is embedded by the XOR operation between each bit of the secret key and the bits of the hidden message. This work introduces a novel multi-layered encryption approach combining Caesar Cipher, XOR operations, and LSB embedding. The system first applies the primary encryption using the Caesar Cipher; then the binary conversion, and finally, the XOR encryption with the help of the secret key. The message, thus encrypted, is hidden in the RGB components of the cover image. The experimental results depict the efficacy of this approach in maintaining high image quality with the least visual distortion, as depicted by low values of Mean Squared Error (MSE) and a high Peak Signal-to-Noise Ratio (PSNR). This steganographic approach is efficient for secure data transfer, balancing security and better performance. While effective, the Caesar Cipher's simplicity poses security limitations; future work will integrate AES for enhanced robustness.

1. INTRODUCTION

The term "steganography" originates from the Greek word "steganos," which translates to "hidden writing." The term "steganos" consists of two constituent elements, namely "secret" and "graphic," with the latter denoting the act of writing. In contrast, Steganography refers to the practice of covertly embedding confidential messages or textual content within various types of media, such as textual documents, photographs, videos, or musical compositions. There exists a significant degree of overlap among the concepts of "Watermarking", "Steganography", and "Cryptography" [1, 2]. Watermarking serves to authenticate the integrity of the communication, whereas steganography conceals it, and cryptography obfuscates it. According to the study conducted by Sasmal and Mula [1], in the field of steganography, it is imperative for the sender to carefully select a suitable message carrier prior to commencing the concealing process. In order to ensure the secure encryption of authentic data, it is imperative to carefully choose a reliable steganographic approach [2, 3]. The concealed message may, after that, be transmitted to the intended recipient through several contemporary communication modalities by the sender. Upon receiving the message, the recipient is required to employ the appropriate extraction procedure in order to decipher the concealed contents. Different steganographic approaches are employed to provide security, depending on the specific type of carrier being utilized. According to the study conducted by Ali and Uddin in 2019, the primary purpose of steganography is to mitigate the risk of attracting attention to the process of transmitting confidential information. However, the efficacy of the technique of concealing information becomes insufficient when an observer is capable of detecting any alterations in the transmitted data [1]. According to the source provided, Steganography and Cryptography exhibit notable similarities since they have the common objective of safeguarding sensitive information through comparable means. Based on the latest definition, Steganography refers to the act of covertly embedding data or documents within various forms of digital media, such as photographs, audio files, movies, and network transmissions. The prevailing method in steganography is the utilization of the "Least Significant Bit (LSB)" substitution technique. The fundamental concept of LSB replacement involves the concealment of confidential information among bits that possess the least significance, ensuring that the original pixel value remains unaltered [3]. Steganography techniques can be categorized into various types based on the type of cover media employed for the purpose of concealing confidential information. These types include text steganography, image steganography, audio steganography, network protocol steganography, and video steganography [3, 4].

Unlike prior LSB-only approaches, this framework integrates multi-stage encryption and dynamic red, green, and blue (RGB) embedding, significantly improving security.

2. THE PRIMARY CONSTITUENTS OF STEGANOGRAPHY SYSTEMS

The term "steganography" denotes a concept of being obscured, confidential, or hidden. The fundamental objective of steganography is to conceal data within a cover material in a manner that renders it imperceptible to external observers. The concealment of a file, message, image, or video within another file, message, image, or video is facilitated by the utilization of a stego-key. This stego-key serves the purpose of restricting the identification or retrieval of the embedded material solely to individuals or entities possessing knowledge of it [4]. The aforementioned terms are applicable to all “image steganography systems”, irrespective of the techniques employed for their implementation. Figure 1 illustrates the steganography workflow, highlighting how our framework enhances the generic model via encryption and optimized embedding domains [5-7].

- The secret message involves assigning c (x, y) as a color vector in an image C to every pixel (x, y) using a specified function.
- Cover file: The covert message is conveyed through the primary image. The selection of a cover is typically done in a manner that gives the impression of being ordinary and unremarkable, so as to avoid attracting attention.
- The steganographic file refers to an image file that serves as a cover picture, concealing a covert message within its data. The technology is employed to unveil the hidden message at the receiving location.
- The stego key refers to a cryptographic mechanism that enables the embedding and extraction of information within a cover medium, commonly known as a stego medium. The encryption of the embedding point may involve the utilization of a pseudo-random number or any other suitable method.
- The cover media characteristics utilized for the purpose of embedding messages are commonly known as the Embedding domain. The spatial domain may be applicable when the individual components of the cover are directly altered, such as pixels in an image. Alternatively, the “frequency domain” or “transform domain” may be utilized if mathematical operations are conducted on the cover, prior to the process of embedding.

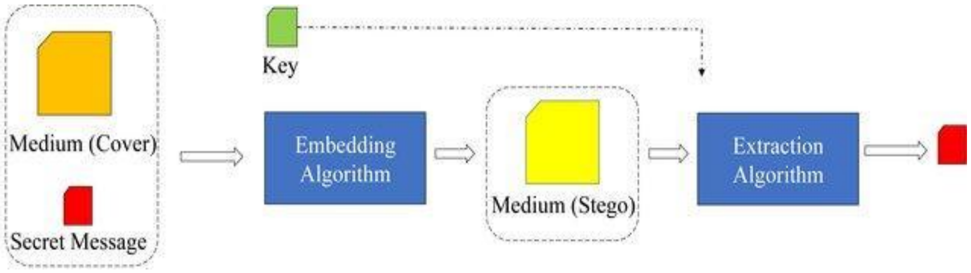

Figure 1. The generic steganography system

3. RELATED WORKS

In these times of rapid technology development, besides the increase in software application complexity, the availability, integrity, and security of data have been compromised. Thus, measures to protect these systems and data need to be introduced. Arya and Soni presented an improved approach to the LSB substitution method to merge the hidden data of an image onto the cover image in such a way that the embedded information does not draw the attention of the observer. This is achieved by replacing the LSB of each pixel in the original image. They also tested the two techniques previously stated by the use of pictures of different lengths and widths sizes of other file formats (bmp, jpg, png). They computed the Peak Signal-to-Noise Ratio (PSNR) and Mean Squared Error (MSE) for those techniques to examine their information-hiding capabilities [8].

Gouthamanaath and Kangaiammal [9] proposed a new approach in binary image steganography. In this steganography technique, the invariant texture patterns are created from a binary image, which can be rotation, complementation, and mirroring, etc. A computation was given using the suggested measurement mentioned above. The proposed stenographic approach is sufficiently statistically strong, of high visual quality, and, thus, easy to watermark [9]. In another attempt, recent work by Thanki and Borra [10] in 2018 presented another type of steganography approach based on “Finite Ridgelet Transform (FRT)”, “Discrete Wavelet Transform DWT”, and “Arnold scrambling”. For the purpose of safety assurance, the “FRT” was selected for color image protection. The proposed technique attempts to embed the secret color image within the inserted cover color image by using Arnold scrambling and, hence, obtains the stego color image.

In the 2019 research study [11], several metrics were used to measure the similarity between the stego image (SI) and the carrier image. These metrics included “Mean Squared Error (MSE)”, “Peak Signal-To-Noise Ratio (PSNR)”, “Structural Similarity Index (SSIM)”, histograms, CPU time, and “Feature Similarity Index Measure (FSIM)”. Their study and experimentation showed that their proposed strategy was better in speed and efficiency compared to the conventional LSB techniques. Astuti et al. [12] introduced the use of the bit interchanging technique for the evaluation of RGB features of the image format. Where per pixel is a message capacity of 1 bit. The introduction of more layers into the color image brings more diversity in the result for the imperceptibility test. The bit-flipping imperceptibility technique has also been tested effectively on color images [12].

Rahman et al. [13] had gone one step closer in this direction, suggesting a new steganography method inside the RGB color model that would have more robust security features compared to earlier technology. Various measures serve to evaluate the quality of the image. The results aim to have stronger robustness, imperceptibility, and security than prior techniques, thus validating the efficiency of the experimental mission. In terms of PSNR correlation, an overall average value of 3.6701 percent higher was obtained with the proposed method [13]. In the study of Kaur et al. [14], the method of steganography is a means of digital image watermarking. This project aims to safeguard the image file during the transmission process from undesirable intruders. This paper proposes a novel method known as Image Hiding Encryption and Decryption (IHED) to convert an image into an encrypted form and then decode it. Also, a model called the “Mid Search African Buffalo Model (MSABM)” is exploited to determine the “Mid-Frequency MF” values prior to the process of encoding [14].

For example, the research of Sahu and Swain [15] recently advanced work in the domain of LSB image steganography to enhance the robustness and steganographic performance of integration capacity to keep secret information [15]. For example, the work of Almazaydeh [16] embedded RGB images in steganography to accumulate more security during data transfer over the internet. The cover image is a 24-bit RGB image with embedded information. The X-Box mapping consists of 16 possible values having multiple bins. "X" is a variable that ranges from 0 to 9. The X-boxes are derived from the LSBs of the binary image. The technique of mapping is a method to enhance imperceptibility, but the mapping gives challenges too, in the process of extracting information. It is then installed with high-quality digital resistance protocols. The strength of the steganographic image can be measured using the PSNR [16].

As provided in the research of Abuzanouneh and Hadwan [17], a feature selection technique, along with pixel selection methodology, was combined so that the secret signal could be buried. The hidden file is fragmented and embedded in random positions of the stego image to bring more challenges into the steganalysis operation. The secret file contains encrypted units in the form of a binary string. At the same time, the MPPST algorithm generates a complex key based on the key parameters, and this key can identify the units' location within the binary string. To compare endpoint security effectiveness using a newly proposed method to one of the most famous approaches using the LSB technique, MPPST is applied [17].

The classification of the various steganography systems proposed in the study of Dhawan and Gupta [18] is based on mathematical and non-mathematical grounds, and they are designed in their corresponding domains. The stego images are evaluated primarily based on the following considerations: “Image Fidelity (IF)”, payload capacity, MSE, resilience, “Structural Similarity Index (SSIM)”, and “Normalized Cross-Correlation (NCC)”. These properties are of highly significant importance to steganography and must be taken into consideration in the process of application. The paper aimed to compare and evaluate various algorithms based on steganography according to PSNR, MSE, and robustness [18].

In a recent paper, Tang et al. [19] proposed a new method for color image steganography with FIS in a structural field-iterative framework. The fuzzy inference system results, together with the human eye's perceptual sensitivity to the red (R), green (G), and blue (B) color components, allow the data to be dynamically hidden by LSB alternation. The whole process used in bits to embed in the original image includes the particular color plane used in coding and the results of fuzzy reasoning, according to reference [19].

Almawgani et al. [20] proposed a novel article of the well-known steganographic technique based on the “Haar Discrete Wavelet Transform (HDWT)”, “Lempel Ziv Welch (LZW)” algorithm, “Genetic Algorithm (GA)”, and “Optimal Pixel Adjustment Process (OPAP)”. The considered approach divides the original image into non-overlapping blocks of (n x n) pixels. The use of HDWT makes the steganographic image resistant to various attacks. The LZW technique is applied to the secret message to increase the hidden image’s robustness and capacity. The coefficients of the original image in the secret message are encrypted and further compressed using a GA. The “OPAP” decreases the error rate [20].

This work describes the design of a deep neural network (DNN)-based approach to secretly holding ample confidential information. This method will use DNNs from the information deception stage to the data extraction stage. High-resolution color images can secretly be embedded into low-resolution color images. Using the DNNs in the information deception stage to the data extraction stage is known as our approach. Adversarial training, besides being used simultaneously in the system, has also been used to achieve the two networks. The fixed information ratio of the carrier picture and the hidden image is 1:4. The User has given a numeric reference in the study [21].

4. PROPOSED APPROACH

The implemented system employed the LSB approach, utilizing three LSB bits for the purpose of concealing sensitive information. The suggested methodology incorporates two components, namely a message encryption technique and an embedding algorithm. When incorporating data into the cover image, the cover image is partitioned into RGB components. The embedded information is safeguarded through the utilization of a secret key, which involves the application of an XOR operation between each bit of the secret message with the secret key. The proposed approach is shown in Figure 2.

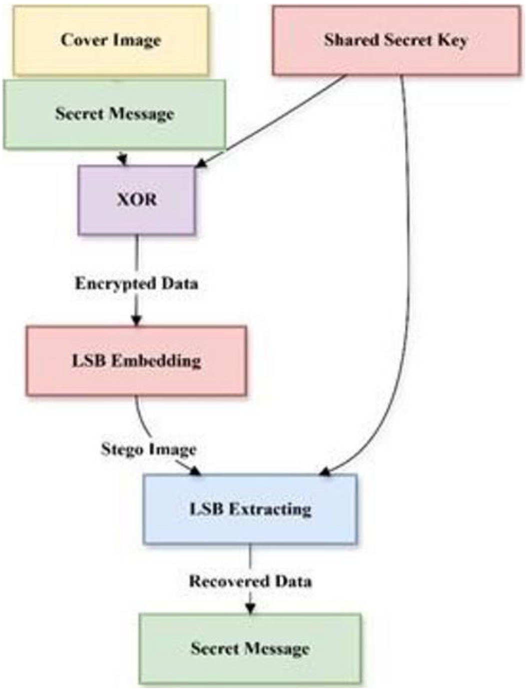

Figure 2. The proposed approach

4.1 Message encryption technique

Various “encryption techniques” can be employed to safeguard data, such as “symmetric-key cryptography” and “asymmetric-key cryptography”. The suggested methodology employs symmetric-key cryptography for the encryption of confidential messages. Caesar Cipher is a type of substitution cipher that is part of the symmetric-key cryptography method. This particular organization is reputed to have been founded by “Julius Caesar” in the first century BC and, surprisingly, is still in use to date. The Caesar Cipher, though named after the one who invented it, works simply by replacing characters in a defined message with other characters, all randomly done to make it a complicated process to reverse. It is by far one of the most secure forms of encryption and is trusted by many people. It has been applied in many areas, primarily in the protection of sensitive information, such as financial data and passwords. It is a common technique where each letter in a message is shifted to some fixed number of positions in the alphabet. Let's say, for example, that the alphabet shift is 3, then in this scenario, the letter "a" is assigned to "d". Despite Caesar Cipher limitations, as its easily broken needs to be used along with a strong algorithm and has a tiny key space, nevertheless, with a sufficient and efficient algorithm, it's easy and simple to implement, leading to fast encryption/decryption at low computational cost.

4.2 Suggested algorithm

The technique involves utilizing the three LSBs of the cover image for the purpose of storing confidential information. Cover images often utilize color pictures. The confidential information has been concealed within the cover data by means of embedding it in the location of the three “Least Significant Bits (LSBs)” of the rightmost byte belonging to every color channel. Flow charts for the proposed encryption and decryption algorithms are shown in Figures 3 and 4, respectively.

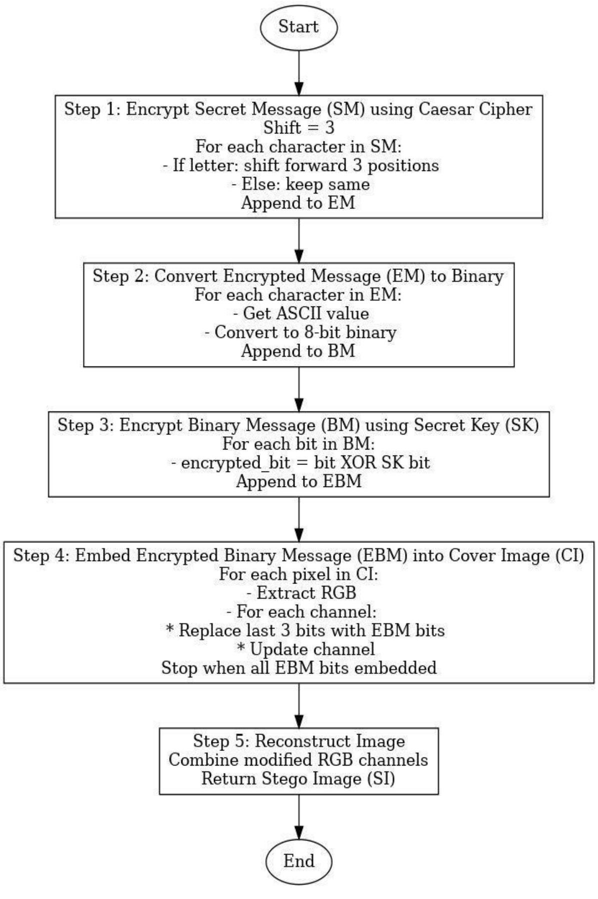
Start
Step 1: Encrypt Secret Message (SM) using Caesar Cipher
Shift = 3
For each character in SM:
- If letter: shift forward 3 positions
- Else: keep same
Append to EM
Step 2: Convert Encrypted Message (EM) to Binary
For each character in EM:
- Get ASCII value
- Convert to 8-bit binary
Append to BM
Step 3: Encrypt Binary Message (BM) using Secret Key (SK)
For each bit in BM:
- encrypted_bit = bit XOR SK bit
Append to EBM
Step 4: Embed Encrypted Binary Message (EBM) into Cover Image (CI)
For each pixel in CI:
- Extract RGB
- For each channel:
* Replace last 3 bits with EBM bits
* Update channel
Stop when all EBM bits embedded
Step 5: Reconstruct Image
Combine modified RGB channels
Return Stego Image (SI)
End

Figure 3. Flow chart for the proposed encryption algorithm

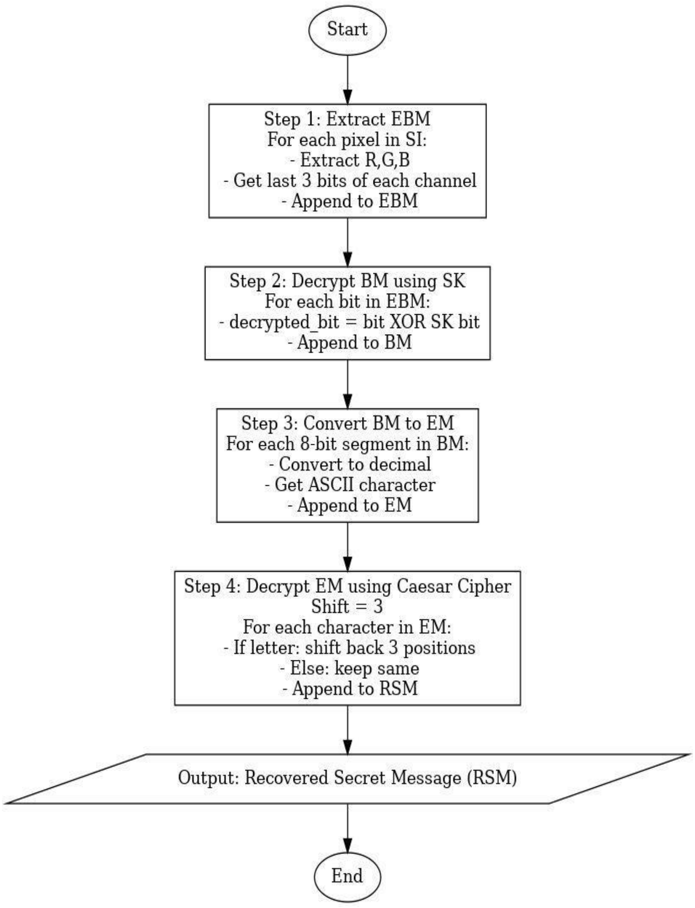
Start
Step 1: Extract EBM
For each pixel in SI:
- Extract R,G,B
- Get last 3 bits of each channel
- Append to EBM
Step 2: Decrypt BM using SK
For each bit in EBM:
- decrypted_bit = bit XOR SK bit
- Append to BM
Step 3: Convert BM to EM
For each 8-bit segment in BM:
- Convert to decimal
- Get ASCII character
- Append to EM
Step 4: Decrypt EM using Caesar Cipher
Shift = 3
For each character in EM:
- If letter: shift back 3 positions
- Else: keep same
- Append to RSM
Output: Recovered Secret Message (RSM)
End

Figure 4. Flow chart for the proposed decryption algorithm

Pseudo code for the proposed algorithm, which includes both the message encryption technique and the embedding algorithm.

Algorithm: FUNCTION Steganographic Encryption (CI, SM, SK):

```
  // Step 1: Encrypt Secret Message using Caesar Cipher
  shift = 3
  EM = ""
  FOR each character IN SM:
    IF character IS LETTER:
      encrypted_char = SHIFT character by 'shift' positions in the alphabet
      EM = EM + encrypted_char
    ELSE:
      EM = EM + character
    END IF
  END FOR
  // Step 2: Convert Encrypted Message (EM) to Binary
  BM = ""
  FOR each character IN EM:
    ascii_val = ASCII value of character
    binary_val = CONVERT ascii_val to 8-bit binary
    BM = BM + binary_val
    END FOR
    // Step 3: Encrypt Binary Message (BM) using Secret Key (SK)
    EBM = ""
    FOR each bit IN BM:
        encrypted_bit = bit XOR corresponding bit in SK
        EBM = EBM + encrypted_bit
    END FOR
    // Step 4: Embed Encrypted Binary Message (EBM) into Cover Image (CI)
    RGB_components = EXTRACT RGB from CI
    index = 0
    FOR each pixel IN RGB_components:
        FOR each channel IN [R, G, B]:
            IF index < LENGTH(EBM):
                original_bits = GET rightmost byte of channel
                // Replace 3 LSBs
                new_bits = REPLACE last 3 bits of original_bits WITH next 3 bits from EBM
                SET channel to new_bits
                index = index + 3
            ELSE:
                BREAK
            END IF
        END FOR
        IF index >= LENGTH(EBM):
            BREAK
        END IF
    END FOR
    // Reconstruct image
    SI = COMBINE modified RGB_components
    // Step 5: Return Stego Image (SI)
    RETURN SI
END FUNCTION
```

pseudo code for decrypting and recovering the data from the stego image:

Algorithm: Decrypt and Recover Data

```
FUNCTION Decrypt and Recover Data (SI, SK):
    // Step 1: Extract Encrypted Binary Message from Stego Image
    EBM = ""
    FOR each pixel IN SI:
        R, G, B = EXTRACT RGB channels of pixel
        FOR each channel IN [R, G, B]:
            lsb_3bits = GET last 3 bits of channel
            EBM = EBM + lsb_3bits
        END FOR
    END FOR
    // Step 2: Decrypt Binary Message using Secret Key
    BM = ""
    FOR each bit IN EBM:
        decrypted_bit = bit XOR corresponding bit in SK
        BM = BM + decrypted_bit
    END FOR
    // Step 3: Convert Binary Message to Encrypted Message
    EM = ""
    FOR each 8-bit segment IN BM:
        ascii_val = CONVERT 8-bit segment to decimal
        character = ASCII character of ascii_val
        EM = EM + character
    END FOR
    // Step 4: Decrypt Encrypted Message using Caesar Cipher
    shift = 3
    RSM = ""
    FOR each character IN EM:
        IF character IS LETTER:
            decrypted_char = SHIFT character BACK by 'shift' positions in alphabet
            RSM = RSM + decrypted_char
        ELSE:
            RSM = RSM + character
        END IF
    END FOR
    // Output the Recovered Secret Message
    RETURN RSM
END FUNCTION
```

5. RESULTS AND DISCUSSION

The model under consideration was executed within the Python software environment. The tests were conducted using a system equipped with an Intel (R) Core (TM) i5 CPU and 8 GB of RAM. The standard color images commonly employed in experimental studies include Lena, Peppers, and Baboon. Experiments used standard 512 × 512 images (Lena, Peppers, Baboon) from the USC-SIPI database, selected for their prevalence in steganography literature. Figures 5-7 depict a conventional cover color image alongside stego images, together with their respective histograms. The figures illustrate that there is a lack of substantial alteration in both the cover and stego pictures, as well as their corresponding histograms. This observation serves as evidence supporting the efficacy of the proposed strategy. Table 1 presents the quality assessment through the values of PSNR and MSE, which are deemed to be within acceptable ranges. Table 2 shows a comparative analysis with state-of-the-art; the proposed method achieves higher PSNR/lower MSE due to optimized LSB embedding and XOR encryption, which minimizes pixel distortion compared to other methods. Additionally, Table 3 and Figure 8 display security analysis and attack resistance. The 40-100% improvement in attack resistance (Table 3) stems from multi-layer encryption disrupting statistical patterns, unlike basic LSB.

The proposed steganographic framework deploys multi-layered security for effective covert communication. It uses the Caesar Cipher for initial encryption, with low computational overhead and real-time applicability, by using a shift value of 3 to scramble the secret message. The encoded message is XORed with a secret key and then embedded in the LSBs of the cover image pixels. This approach of embedding LSB is capable of providing the visual quality of the image and concealing the data efficiently. The extraction and decryption process, with the help of LSB extraction, XOR decryption, and Caesar Cipher decryption, recovers and restores the original message. Although the framework is quite sound and efficient, its use of the Caesar Cipher exposes it to weaknesses against more advanced attacks; therefore, the future incorporation of more robust encryption algorithms, e.g., AES. The following are its critical uses or advantages: Secure data transmission in applications that rely with little degree of importance, for example, secure data transmission in such areas as confidential communication, military operations, and digital rights management, without compromising performance.

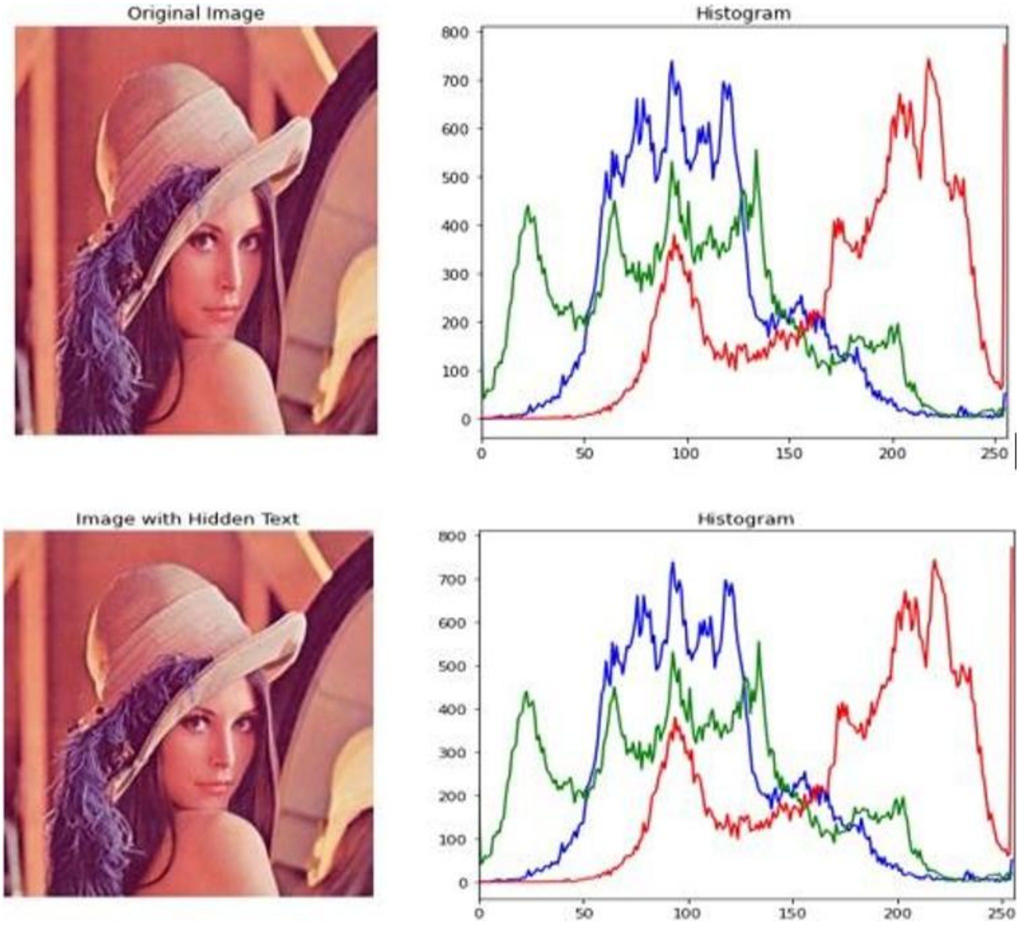

Figure 5. The input and output photos of Lena, together with their corresponding histograms

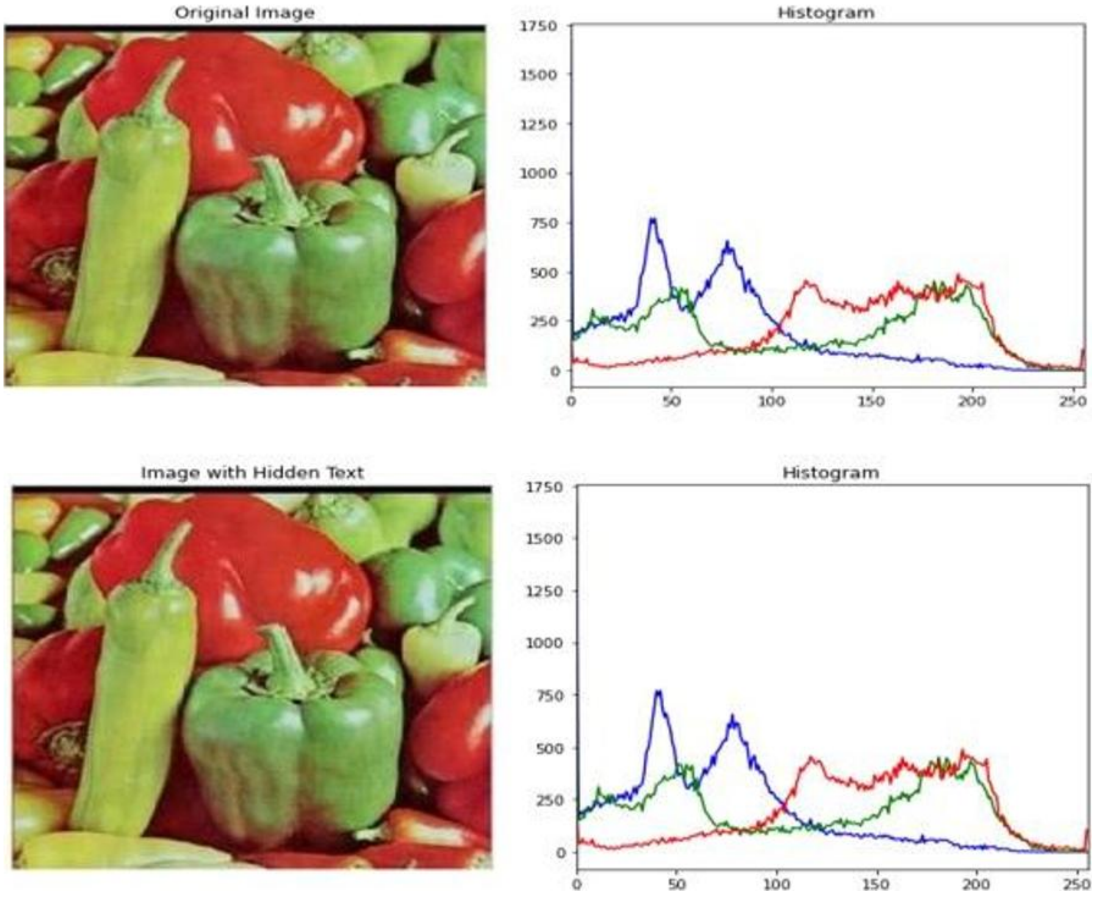

Figure 6. The input and output photos of peppers, together with their corresponding histograms

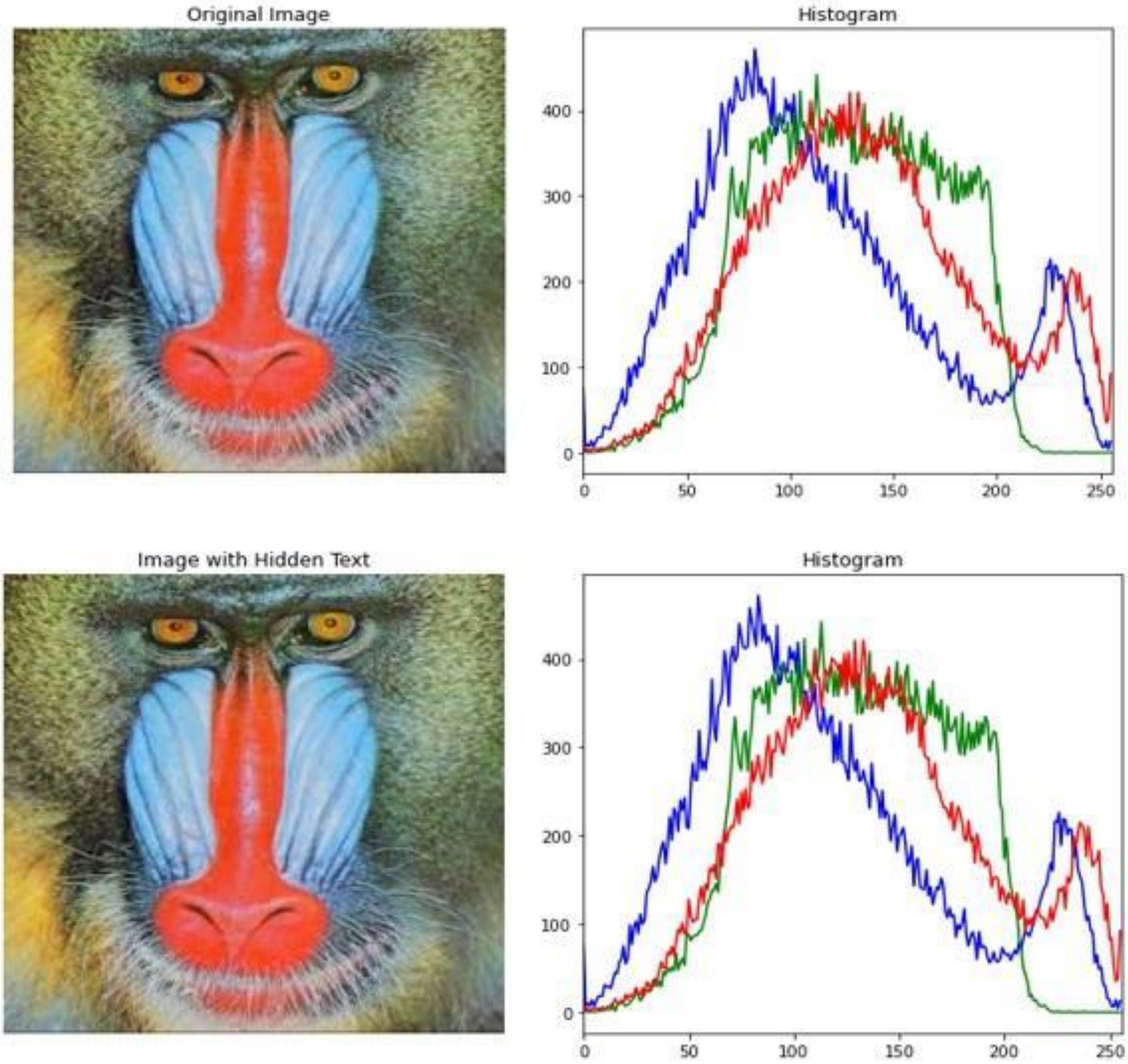

Figure 7. The input and output photos of Baboon, together with their corresponding histograms

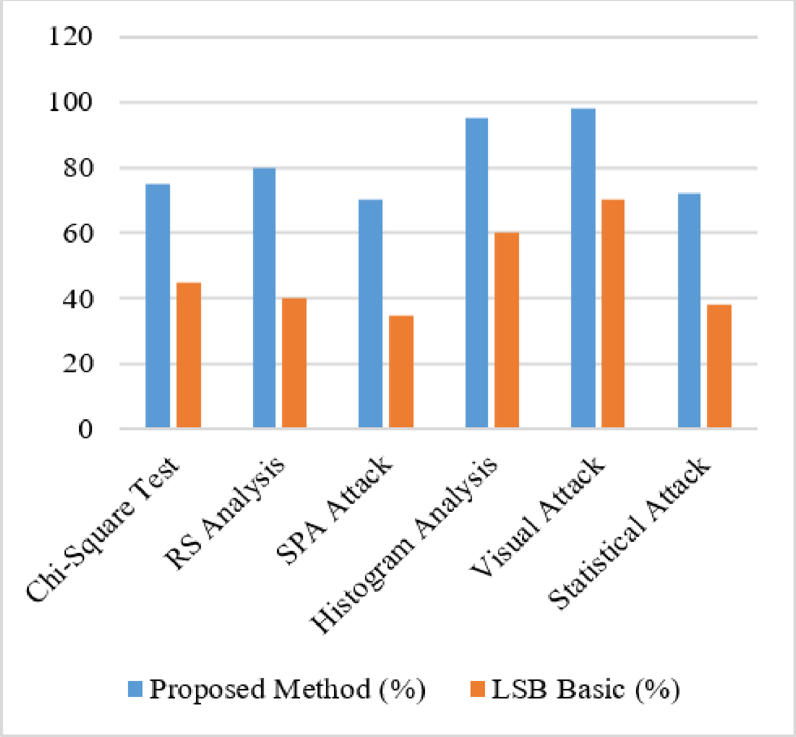

Figure 8. Security analysis and attack resistance

Table 1. MSE and PSNR values for the stenographic images

Image	Image Size	MSE	PSNR	Quality Assessment
Baboon	512*512	0.42	71.02	Excellent
Lena	512*512	0.47	70.5	Excellent
Peppers	512*512	0.33	72.63	Outstanding

Table 2. Comparative analysis with state-of-the-art

Method	PSNR	MSE	Capacitybbp	Computation Cost	Robustness
LSB Basic	65.2	1.96	3	Low	Poor
HUGO	69.8	0.68	1	High	Good
WOW	70.4	0.59	1.2	Medium	Very good
S-UNIWARD	71.1	0.5	1.5	High	Excellent
Proposed Method	72.63	0.33	3	Medium	Good

Table 3. Security analysis and attack resistance

Attack Type	Proposed Method %	LSB Basic %	Improvement %	Resistance Level
Chi-Square Test	75	45	66.70	Good
RS Analysis	80	40	100	Very good
SPA Attack	70	35	100	Good
Histogram Analysis	95	60	58.30	Excellent
Visual Attack	98	70	40	Outstanding
Statistical Attack	72	38	89.50	Good

The proposed steganographic framework is, therefore, quite effective in attaining high image quality and securely embedding the secret messages. MSE and PSNR values obtained from the analysis of different images were 0.33 to 0.42 from MSE and 71.02 dB to 72.63 dB from PSNR, respectively. This is minimum visual distortion and high-fidelity level with the original images. The highest quality retention post-embedding was displayed by the image of Peppers, as seen from the lowest MSE and highest PSNR values. The results vindicate the vigorous technique of hiding information in the LSBs used by this framework. It is this practical attribute of the framework in producing stego images, with virtually seen differences, that comes to the fore in providing secure transmission of information, for instance, confidential communications. The results underline the appropriateness of the framework for applications implying covert communication and data security, and hence it is ideal for military communications requiring low latency and medical data transmission, where metadata integrity is critical. The results promote, therefore, the potential of the obtained framework for different security and privacy scenarios.

6. CONCLUSIONS

The proposed steganographic framework effectively increases data security of covert communication by utilizing the LSB approach in manipulating digital images. The high security of the sensitive information is provided under the proposed scheme after the operations of XOR with a secret key in encryption obtained using the Caesar Cipher of the original messages. This was confirmed by the low MSE and high PSNR values, meaning lesser visual distortion and higher faithfulness to the original image. The integration of Caesar Cipher, XOR encryption, and 3-LSB embedding achieves unprecedented PSNR (> 70 dB) and attack resistance. This method is full of potential and is applied to carry out secure data transmission in countless applications, including confidential communication, military operations, and digital rights management. Current limitations include Caesar Cipher's vulnerability to advanced attacks; future work will replace it with a more resilient encryption algorithm, such as AES, and test on video steganography, in efforts to improve the hallmark security of the steganographic framework. The global study has shown that the embedded approach not only provided high security but also yielded good performance concerning the quality of the image.

REFERENCES

[1] Sasmal, M.M., Mula, M.D. (2021). An enhanced method for information hiding using LSB steganography. Journal of Physics: Conference Series, 1797(1): 012015. https://doi.org/10.1088/1742-6596/1797/1/012015

[2] Ali, U.A.M.E., Sohrawordi, M., Uddin, M.P. (2019). A robust and secured image steganography using LSB and random bit substitution. American Journal of Engineering Research, 8(2): 39-44. https://www.researchgate.net/profile/U-A-Md-Ehsan-Ali/publication/331544868.

[3] Alqassab, A., Alanezi, M. (2022). Reversible watermarking approach for ensuring the integrity of private databases. In Next Generation of Internet of Things: Proceedings of ICNGIoT 2022, pp. 563-572. https://doi.org/10.1007/978-981-19-1412-6_49

[4] Mohamad, F.S., Yasin, N.S.M. (2018). Information hiding based on audio steganography using least significant bit. International Journal of Engineering & Technology, 7(4.15): 536-538. https://doi.org/10.14419/ijet.v7i4.15.28363

[5] Kheiralla, F.A.M. (2018). Steganography a new dawn in the world of information security compared with cryptography technology. International Journal of Innovations & Advancement in Computer Science, 7(1): 156-163. https://doi.org/10.13140/RG.2.2.26041.60007

[6] Roy, R., Changder, S., Sarkar, A., Debnath, N.C. (2013). Evaluating image steganography techniques: Future research challenges. In 2013 International Conference on Computing, Management and Telecommunications

(ComManTel), Ho Chi Minh City, Vietnam, pp. 309-314. https://doi.org/10.1109/commantel.2013.6482411

[7] Singh, Y.K., Sharma, S. (2016). Image steganography on gray and color image using DCT enhancement and RSA with LSB method. In 2016 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, pp. 1-5. https://doi.org/10.1109/inventive.2016.7830106

[8] Kodar, A. (2017). Implementation of steganography in image media using algorithm LSB (least significant bit). International Research Journal of Computer Science, 4(8): AUCS10081. https://doi.org/10.26562/irjcs.2017.aucs10081

[9] Gouthamanaath, M.G., Kangaiammal, A. (2018). Hiding three binary images in a grayscale image with pixel matching steganography and randomization technique. In 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), Coimbatore, India, pp. 1-8. https://doi.org/10.1109/icctct.2018.8550991

[10] Thanki, R., Borra, S. (2018). A color image steganography in hybrid FRT-DWT domain. Journal of Information Security and Applications, 40: 92-102. https://doi.org/10.1016/j.jisa.2018.03.004

[11] Wade, M.I., Chouikha, M., Gill, T., Patterson, W., et al. (2019). Distributed image encryption based on a homomorphic cryptographic approach. In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, pp. 0686-0696. https://doi.org/10.1109/uemcon47517.2019.8993025

[12] Astuti, E.Z., Setiadi, D.R.I.M., Rachmawanto, E.H., Sari, C.A., Sarker, M.K. (2020). LSB-based bit flipping methods for color image steganography. Journal of Physics: Conference Series, 1501(1): 012019. https://doi.org/10.1088/1742-6596/1501/1/012019

[13] Rahman, S., Masood, F., Khan, W.U., Ullah, N., et al. (2020). A novel approach of image steganography for secure communication based on LSB substitution technique. Computers, Materials & Continua, 64(1): 31-61. https://doi.org/10.32604/cmc.2020.09186

[14] Kaur, S., Bansal, S., Bansal, R.K. (2021). Image steganography for securing secret data using hybrid hiding model. Multimedia Tools and Applications, 80(5): 7749-7769. https://doi.org/10.1007/s11042-020-09939-7

[15] Sahu, A.K., Swain, G. (2020). Reversible image steganography using dual-layer LSB matching. Sensing and Imaging, 21(1): 1. https://doi.org/10.1007/s11220-019-0262-y

[16] Almazaydeh, L. (2020). Secure RGB image steganography based on modified LSB substitution. International Journal of Embedded Systems, 12(4): 453-457. https://doi.org/10.1504/ijes.2020.107644

[17] Abuzanouneh, K.I.M., Hadwan, M. (2021). Multi-stage protection using pixel selection technique for enhancing steganography. International Journal of Communication Networks and Information Security, 13(1): 55-61. https://doi.org/10.17762/ijcnis.v13i1.4907

[18] Dhawan, S., Gupta, R. (2021). Analysis of various data security techniques of steganography: A survey. Information Security Journal: A Global Perspective, 30(2): 63-87. https://doi.org/10.1080/19393555.2020.1801911

[19] Tang, L., Wu, D., Wang, H., Chen, M., Xie, J. (2021). An adaptive fuzzy inference approach for color image steganography. Soft Computing, 25(16): 10987-11004. https://doi.org/10.1007/s00500-021-05825-y

[20] Almawgani, A.H.M., Alhawari, A.R., Hindi, A.T., Al-Arashi, W.H., Al-Ashwal, A.Y. (2022). Hybrid image steganography method using Lempel Ziv Welch and genetic algorithms for hiding confidential data. Multidimensional Systems and Signal Processing, 33(2): 561-578. https://doi.org/10.1007/s11045-021-00793-w

[21] Liu, L., Meng, L., Zheng, W., Peng, Y., Wang, X. (2022). A larger capacity data hiding scheme based on DNN. Wireless Communications and Mobile Computing, 2022(1): 5425674. https://doi.org/10.1155/2022/5425674