



Enhanced Security Through Integrated Morse Code Encryption and LSB Steganography in Digital Communications

Huda Ismail Olewi¹, Mohammed Majid Msallam^{2,3*}, Sarah Kareem Salim⁴, Hasanain A.H. Al-Behadili⁴

¹ Civil Engineering Department, University of Misan, Misan 62001, Iraq

² Computer Engineering Department, Ankara University, Ankara 06100, Turkey

³ Control and Systems Engineering Department, University of Technology, Baghdad 10066, Iraq

⁴ Electrical Engineering Department, University of Misan, Misan 62001, Iraq

Corresponding Author Email: mohammedarjeeli92@gmail.com

Copyright: ©2024 The authors. This article is published by IETA and is licensed under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

<https://doi.org/10.18280/ts.410147>

ABSTRACT

Received: 15 June 2023

Revised: 5 November 2023

Accepted: 26 December 2023

Available online: 29 February 2024

Keywords:

encryption data, steganography, Morse code, cryptography, least significant bit (LSB) technique, data hiding

In the digital era, the protection of sensitive data transmitted over the Internet, such as credit card information, is paramount. This study introduces an innovative system that enhances data security during internet transmission by synergizing steganography and cryptography. The proposed method employs a two-stage process: encryption followed by concealment. Initially, secret text data is encrypted using an evolved form of Morse code, converting it into ciphertext. Subsequently, this ciphertext is discreetly embedded within a cover image utilizing the least significant bit (LSB) technique, a method renowned for its subtlety and efficiency in data hiding. The effectiveness of this novel system was evaluated by comparing its performance with existing benchmarks. The chosen test case involved embedding encrypted data within a Baboon image. The results demonstrated a notable improvement of 2.596% over the baseline, affirming the system's efficacy. A critical aspect of this approach is the high quality of the resultant stego image. This quality is instrumental in ensuring the covert nature of the embedded data, thereby significantly reducing the likelihood of detection during internet transmission. Key elements of this study include the development of a more sophisticated Morse code encryption algorithm and the optimization of the LSB steganography technique. These advancements contribute to the system's robustness, rendering the encrypted and hidden data virtually undetectable and inaccessible to unauthorized entities. The integration of these two techniques represents a significant stride in the realm of digital data security, offering a dual-layered defense mechanism against potential cyber threats.

1. INTRODUCTION

Since secret information like passwords, information on credit cards, and so on is transferred over the Internet, the risk to data security and privacy has increased when it is transmitted over the Internet [1]. On the other side, despite the increasing security in transmission, hacker and intrusion group development continues daily. Consequently, there is a growing demand for data security [2]. To a certain extent, the cryptography method satisfies the requirements of information security as the cornerstones of security mechanisms, but recently, the traditional cryptography method has become ineffective because of issues relating to distortion in the data that indicate it contains sensitive data. This distortion of data increases the possibility of attack because the attacker is more suspicious of the presence of important data. As a result, information hiding emerges at a crucial juncture to address the issue of information security more effectively. Information hiding is now widely investigated and used in a few fields, including secure communications, the defense of intellectual property rights, and content verification [3, 4].

Cryptography is derived from the Greek word. It has two parts: crypto means hidden secret, and graphy means writing. It is a study of techniques for ensuring information security, including data integrity, confidentiality, authentication, and non-repudiation, during secure communication when third parties are present [5]. The fundamental principle of cryptography is to obscure the information content so that it appears to be random code to safeguard the information content. In general, there are two methods of cryptography, which are asymmetric-key cryptography and symmetric-key cryptography. In asymmetric key cryptography, there are two separate keys, which are the public key and the private key, to prevent any unethical access to the data. A public key is used for encryption in asymmetric-key cryptography, and a private key is used for decryption [6]. In many methods of cryptography, it codes secret data in a way that only the sender and recipient can understand. Morse code is one of these methods, which is a group of special characters used in telecommunication to encode secret data. In Morse code, dots, dashes, and spaces are used instead of alphabetic characters, numbers, and punctuation marks to protect the secret data [7].

The science and art of hiding a secret message under a cover medium is known as steganography. The term steganography comes from the Greek words stegano, which means enclosed, and graphy, which means writing, which literally translates to cover writing [8]. Steganography is the process of embedding a secret message into a suitable cover object, such as an image, video, sound file, or other file that will be transmitted over the internet. The embedding is parameterized by a key, making it difficult for a third party to find or delete the embedded material. Once embedded, a cover object is referred to as a stego object [9]. The LSB is a technique that is frequently used to hide secret data in images [10].

Recently, hackers have seized a lot of important data because of their knowledge of all encryption methods [11]. This motivated us to propose a new security system using the properties of cryptography and steganography. Steganography and cryptography complement one another and are orthogonal to one another, increasing security when used together [12]. Figure 1 demonstrates how steganography and cryptography are integrated.

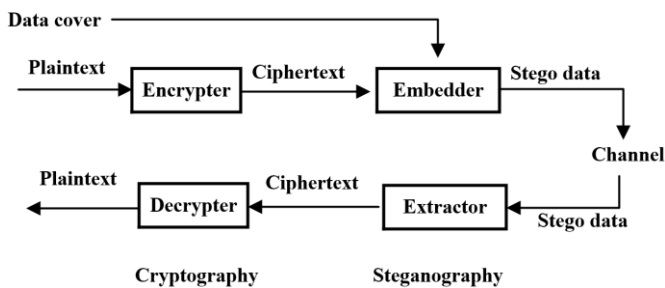


Figure 1. Combination of steganography and cryptography

The rest of this study is organized as follows: Section II introduces the literature survey on using cryptography and steganography to encrypt important data. The materials and methods that are used in this work are presented in Section III. In Section V, the results and their discussion are written, along with a comparison to the baseline study. Finally, the conclusion is written and suggests some future works.

Overall, the main goals of this article are as follows:

- The two stages, which are steganography and cryptography, are proposed to secure secret data when it transfers over the internet.
- The payload capacity of the cover image is increased when secret text is hidden inside it.
- Morse code was developed to enhance the encryption of data.
- The imperceptibility of the cover image is enhanced when hiding data inside it.

2. RELATED WORK

Researchers working in the field of secret digital data are constantly looking to combine existing techniques, such as steganography and cryptography. At the same time, other researchers are proposing new techniques to protect text, images, audio, and video to get high encryption for transferred data. Nofriansyah et al. [13] developed a model by combining cryptographic techniques using the Hill chipper algorithm and Morse code with steganography using the LSB algorithm to safeguard confidential communications from prying eyes during transmission of data via online media. They discovered

that protecting data with more than one algorithm was preferable. The message is encrypted using cryptography techniques and embedded into a cover image using steganography. The algorithms and techniques that were used have not contained novelty, and they are knowledge gained by hackers in their work. Nunna and Marapareddy [4] developed a web-based application to enable authorized users of the application to communicate and transmit data after embedding in cover images. They achieved two levels of security by using the crypto-steganography technique. They encrypt the data using the XOR operation and embed the encrypted data into the pixels of the cover image pseudo-randomly using a key chosen by the user. There would not be any distortion in the stego image, even though they are changing the bits of the components of the pixels. Nevertheless, a small amount of distortion will be produced that cannot be perceived by the human eye, and this makes it susceptible to attack. Kumar et al. [14] proposed a hybrid model that used first the LSB steganography technique to hide the secret text data into the cover image to obtain the stego image. Secondly, they applied the Advanced Encryption Standard (AES) to the stego image to get the encrypted image. Using their proposal, they achieved a value of Mean Squared Error (MSE) equal to 0.0019922 and a PSNR value of 75.1375, which means providing robust security because MSE is low and Peak Signal to Noise Ratio (PSNR) is high. They used AES and LSB, which are known to hackers. A method to hide information introduced by Neamah et al. [15] was to boost security and simultaneously increase imperceptibility in the cover image. Their method involved encrypting secret data using the encryption key and the Xnor operation, then utilizing the LSB technique to hide the encrypted data inside a cover color image. Although there is increased imperceptibility in their work, the payload capacity is still low. A method that increases the payload capacity was proposed by Tayyeh and Al-Jumaili [16]. Their work was a combination of the LSB technique and deflate compression algorithms for image steganography. The LZ77 and Huffman codes were applied in the proposed Deflate algorithm for compressing the important text. The compressed text was embedded in the cover image using the LSB technique. The hiding method used is conventional and not advanced, which is LSB and is already known by hackers and susceptible to breaches. In literature [17], an adaptive method was proposed to improve the imperceptibility of steganography by using an adaptive pattern depending on an inverted LSB technique. In increasing imperceptibility, Setiadi et al. [18] had a method that used graded fuzzy edge detection, which divides pixels into edge-related, non-edge-related, and primary categories.

The methods mentioned in the literature were aimed at increasing imperceptibility or payload capacity. The benefits of the LSB are payload capacity and imperceptibility, which are high, and the drawback of the LSB is poor robustness [19]. Despite the high payload capacity and imperceptibility of the LSB technique, our work using the developed Morse code and the LSB method of Neamah et al. [15] contributes further to increasing both. The novelty of this work is that Morse code is developed to reduce and encrypt secret data.

3. METHODS

3.1 Proposal system

A simplified schematic diagram of the proposed system is shown in Figure 2. The system is composed of two main parts,

namely the encryption layer and the decryption layer. At the encryption layer, the secret text is first encrypted using Morse code that we have developed. The bits stream then hide in a cover image using the LSB technique, which was used by Neamah et al. [15] to form the stego image. At the decryption layer, the secret text is extracted from the cover image, then decrypted to return the original text.

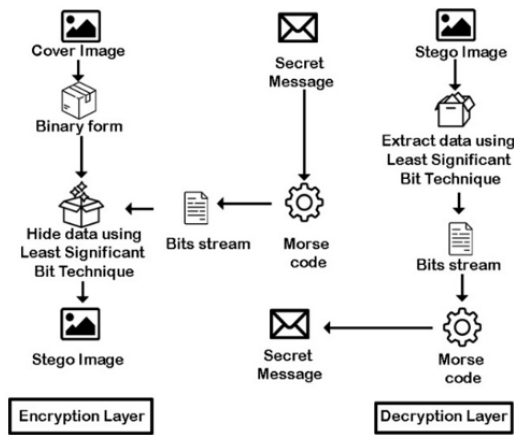


Figure 2. Block diagram of the proposed system

3.2 Morse code

Morse code was created by Samuel F. B. Morse, one of the inventors of the telegraph, in 1840. With the advent of radio in the 1890s, it was also widely utilized for radio communication [20]. Morse code is a method used in telecommunication to encode text characters as standardized sequences of two different signal durations. In Morse code, each letter of the alphabet is converted to dots and dashes, as shown in Morse code column Table 1.

Table 1. Our code for encryption of alphabets

Alphabet	Morse Code	Binary Morse Code	Header	The Developed Morse Code
E	.	0	00	000
T	-	1	00	001
A	.-	01	01	0101
I	..	00	01	0100
M	--	11	01	0111
N	-.	10	01	0110
D	-. .	100	10	10100
G	-. .	110	10	10110
K	-. .	101	10	10101
O	---	111	10	10111
R	.-.	010	10	10010
S	...	000	10	10000
U	..-	001	10	10001
W	-. .	011	10	10011
B	-. .	1000	11	111000
C	-. .	1010	11	111010
F	-. .	0010	11	110010
H	0000	11	110000
J	.-. .	0111	11	110111
L	.-. .	0100	11	110100
P	-. .	0110	11	110110
Q	-. .	1101	11	111101
V	0001	11	110001
X	-. .	1001	11	111001
Y	-. .	1011	11	111011
Z	-. .	1100	11	111100
Blank	----	1111	11	111111

In our work, Morse code is developed by converting the data in Morse code form into binary form by converting each dot to 0 and dash to 1, as shown in the binary Morse code column of Table 1. When encoding a secret message using our developed Morse code, a potential challenge arises. The intended recipient may have difficulty deciphering the character since the bit size of each character is not fixed. For example, some characters have one bit, such as E, and another has four bits, such as Z. So, the developed Morse code is divided into four groups. The first group contains one bit, the second group contains two bits, the third group contains three bits, and the fourth group contains four bits. Every group has a code, where the code of the first group is 00, the code of the second group is 01, the code of the third group is 01, and the code of the fourth group is 11. The code of the group is a header that is used to solve the difficulty that faced the intended recipient when deciphering the encoded message. To encrypt letters in developed Morse code, the header of the group is first put, then it is followed by Morse code in binary form. To clarify the process of encryption in our proposal, we assume that the secret text is HUDA. The letter H is DOT DOT DOT DOT according to Morse code, so we convert it to 0000 and add 11 as a header on the left to become 110000, such as in Table 1. While the letter U is DOT DOT DASH according to Morse code, we convert it to 001 and add 10 as a header on the left to become 10001, and so on. Then the secret text will become 11000010001101000101 in binary based on the developed Morse code, as shown in Figure 3. The encryption in the proposed method, which is developed using Morse code, is described in Algorithm 1.

H	U	D	A
110000	10001	10100	0101

Figure 3. Example of the developed Morse code

Algorithm 1

```

encryption(text)
stream = ∅
While text ≠ ∅
L = DEQUEUE (text)
G = GET_GROUP(L)
M = GET_MORSE_BINARY(L)
K = MERGE(G,M)
stream = ENQUEUE (K)

```

On the decryption side, the decryption step is addressed after the stream of bits is received. Firstly, it reads the first two bits from the encrypted secret text (1100001000110100010), which are 11, which means the fourth group. The fourth group has four bits, so the next four bits are read, which is 0000, and matched with Table 1 to get a letter, which is H. The decryption is described in algorithm 2.

Algorithm 2

```

decryption(stream)
text = ∅
While stream ≠ ∅
L = DEQUEUE (stream, 2) // read two bits
G = GET_GROUP(L)
B = DEQUEUE (stream, G) // read G bits
M = GET_MORSE_LETTER(B)
text = ENQUEUE (M)

```

The developed Morse code compresses the text in addition to encrypting it. The stream of bits for the developed Morse code is short when compared with the stream of bits for the ASCII code. Table 2 presents coding using developed Morse code and ASCII code for the HUDA word.

Table 2. Coding using developed Morse code and ASCII code

Coding Method	Stream of Bits	Number of Bits
Developed Morse code	1100001000110100010	19
ASCII code	1001000101010110001001000001	28

3.3 LSB technique

The most popular steganography technique is the LSB; it has a high embedding capacity and a low computing complexity [10]. This technique embeds a secret message in an image, audio, network, or text [21]. In the cover image, the LSB of each pixel is modified and replaced with a bit of secret data [14].

After encrypting the secret text using Morse code, the bits stream hides inside a cover image through the embedding process. First, the channel is selected using the algorithm of Neamah et al. [15]. Second, the LSB technique is implemented to hide a secret bit in a selected channel. At the end of this process, the stego image obtained was sent over the network. Figure 4 summarizes the LSB technique used by Neamah et al. [15].

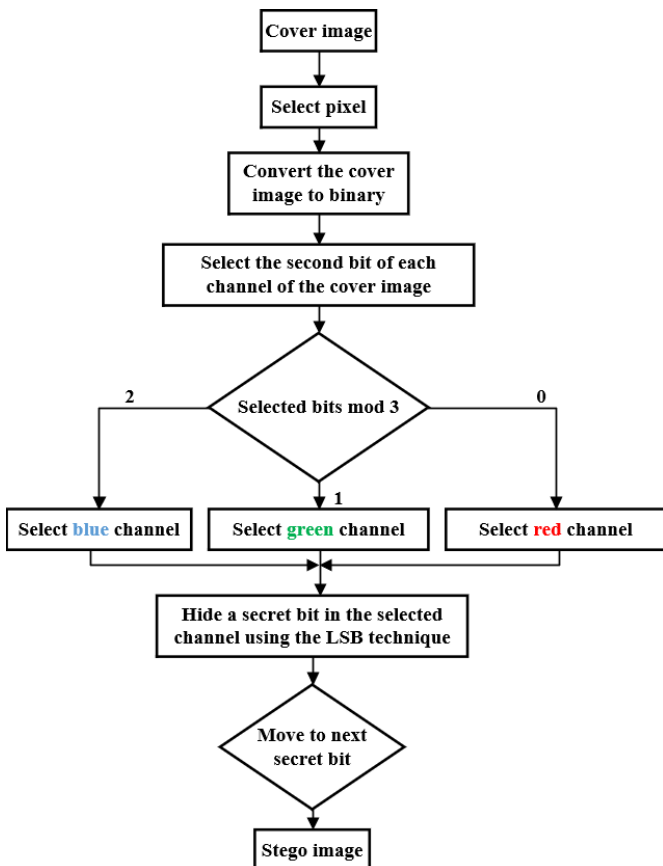


Figure 4. The structure of the LSB technique which used in the work [15]

4. RESULTS AND DISCUSSION

In our work, the cover images used to hide the secret text are Lenna, Airplane, Peppers, and Baboon, which are colored in size 512×512. The encryption and decryption used the environment MATLAB R2018b and were implemented on a personal computer (processor: AMD Ryzen 7 6800H with Radeon Graphics @ 3.20 GHz; operating system: Windows 10 64-bit; memory: 16 GB). In our proposal, the secret text contains 680 letters, which are equal to 5440 bits. After applying the developed Morse code, the data will be encrypted and compressed to 3190 bits. To know the number of bits hiding in the cover image by a receiver, 16 bits are added at the beginning of the bit stream before hiding in the cover image. The bit stream becomes 3206 bits, which hide in the cover image. Figure 5 presents the RGB histogram of the Lenna image and the Lenna image for the stego and the original image.

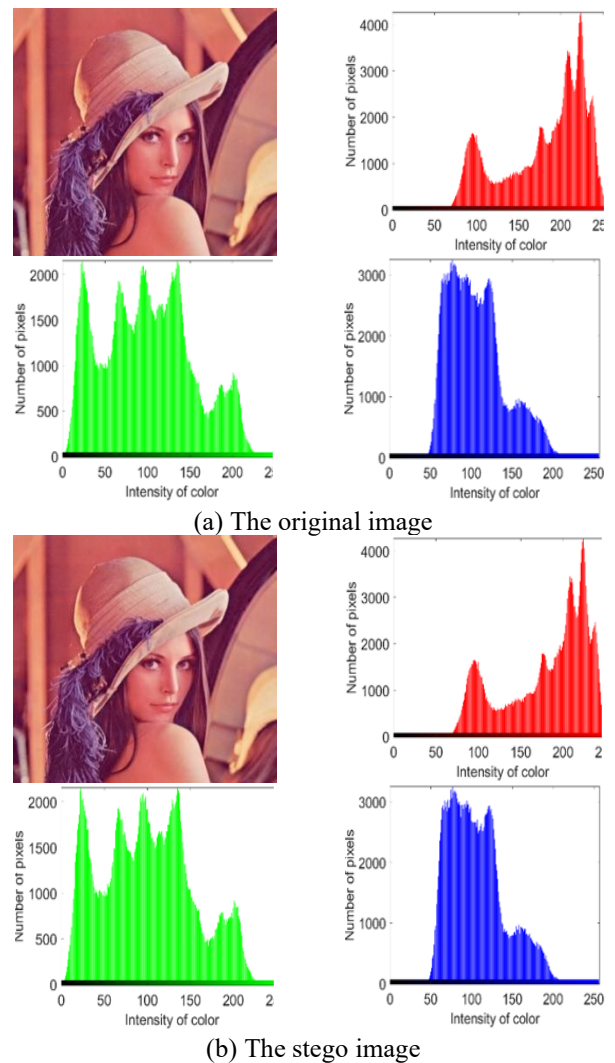


Figure 5. The RGB histogram of the Lenna image and Lenna image

The effectiveness of the proposed technique was measured using the Peak Signal-to-Noise Ratio (PSNR), which is an expression for the measure of the stego image that contained secret data relative to the original image. The PSNR is a statistical instrument that is utilized to evaluate digital image quality. While the MSE is the average of the squared differences between the stego image and the original image,

The similarity between two image or video frames is measured using the Structural Similarity Index (SSIM). The value of SSIM is between 0 and 1, where the 1 value indicates that two images are similar and the 0 value indicates that two images are not similar [22]. The values of MSE, PSNR, and SSIM for Airplane, Lenna, Peppers, and Baboon images when hidden with 5440 bits inside them are illustrated in Table 3. Eq. (1), Eq. (2), and Eq. (3) are the mathematical expressions for PSNR, MSE, and SSIM, respectively [22, 23].

$$\text{PSNR (db)} = 10 \log_{10} \frac{(2^n - 1)^2}{\text{MSE}} \quad (1)$$

$$\text{MSE} = \frac{1}{W \times H} \sum_{r=0}^{W-1} \sum_{c=0}^{H-1} (O(i, j) - S(i, j))^2 \quad (2)$$

$$\text{SSIM}(O_i, S_i) = I(O_i, S_i) \times C(O_i, S_i) \times S(O_i, S_i) \quad (3)$$

where, n is equal to 8 which is the number of bits per pixel of an image. While the pixel values of an original image and a stego image at the (i, j) positions are $O(i, j)$ and $S(i, j)$, respectively. The columns and rows in an image are denoted by the letters H and W , respectively.

$$I(O_i, S_i) = \frac{2\mu_{oi}\mu_{si} + \varepsilon}{\mu_{oi}^2 + \mu_{si}^2 + \varepsilon} \quad (4)$$

$$C(O_i, S_i) = \frac{2\sigma_{oi}\sigma_{si} + \varepsilon}{\sigma_{oi}^2 + \sigma_{si}^2 + \varepsilon} \quad (5)$$

$$S(O_i, S_i) = \frac{\sigma_{oi,si} + \varepsilon}{\sigma_{oi}\sigma_{si} + \varepsilon} \quad (6)$$

where, μ_{oi} and μ_{si} are the means of the original image and the stego image, respectively. σ_{oi} and σ_{si} are the standard deviations of the original image and the stego image, respectively. $\sigma_{oi,si}$ is the covariance between the original image and the stego image. The positive constant ε is used to avoid a null denominator.

Table 3. The result of our proposal

Colored Images	MSE	PSNR (dB)	SSIM
Airplane	0.0011787	77.4166	0.99999946285952
Lenna	0.001166	77.4637	0.99999970446795
Peppers	0.0012054	77.3193	0.99999976585324
Baboon	0.0010872	77.7678	0.99999968326329

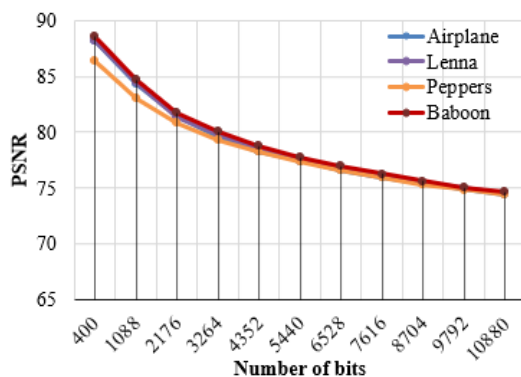


Figure 6. The value of PSNR for Airplane, Lenna, Peppers, and Baboon images

Figure 6 shows the values of PSNR for Airplane, Lenna, Peppers, and Baboon images. It is evident from this figure that the slope of the curve, which reflects the value of PSNR, is slowly decreasing as the amount of secret data hidden in the stego image increases. This indicates that even with more secret data bits, the PSNR value will stay high. It denotes a high level of stego image quality.

Table 4 presents a comparison between the PSNR of our proposal with the studies [15, 16], where the same cover image in size 512x512 pixels is adopted. Note that even though our proposal involves hiding more secret text (5440 bits) in the stego image, the PSNR is still high compared to baseline research.

Table 4. The PSNR of our proposal and other researchers

Colored Images with Size 512x512	Secret Text 4700 Bits PSNR (dB)		Secret Text 5440 Bits	Improvement %
	[15]	[16]	Proposal	
Airplane	60.44	76.03	77.4166	1.823
Lenna	61.74	75.81	77.4637	2.181
Peppers	57.65	75.77	77.3193	2.044
Baboon	58.39	75.80	77.7678	2.596

5. CONCLUSION

Transmitting credit card information over the Internet poses a risk to hackers. In this paper, cryptography and steganography are combined to enhance the security of secret text and the imperceptibility of stego images. The secret text was encrypted using Morse code and hidden in the cover image using the LSB technique. The advantages of our approach over existing methods are increased payload capacity and the imperceptibility of the stego image. The increased imperceptibility of the stego image increased the quality of the stego image, which reduced the doubt of attackers that there was confidential data inside the stego image. This article assumes that the secret data is limited to uppercase letters, so numbers and lowercase letters can be added as future work.

REFERENCES

- [1] Gladwin, S.J., Gowthami, P.L. (2020). Combined cryptography and steganography for enhanced security in suboptimal images. In 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), Amaravati, India, pp. 1-5. IEEE. <https://doi.org/10.1109/AISP48273.2020.9073306>
- [2] Talukder, M.S.H., Hasan, M.N., Sultan, R.I., Rahman, M., Sarkar, A.K., Akter, S. (2022). An enhanced method for encrypting image and text data simultaneously using AES algorithm and LSB-based steganography. In 2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE), Gazipur, Bangladesh, pp. 1-5. <https://doi.org/10.1109/ICAEEE54957.2022.9836589>
- [3] Zhou, X., Gong, W., Fu, W., Jin, L. (2016). An improved method for LSB based color image steganography combined with cryptography. In 2016 IEEE/ACIS 15th International Conference on Computer and Information Science (ICIS), Okayama, Japan, pp. 1-4.

- <https://doi.org/10.1109/ICIS.2016.7550955>
- [4] Nunna, K.C., Marapareddy, R. (2020). Secure data transfer through internet using cryptography and image steganography. In 2020 SoutheastCon, Raleigh, NC, USA, pp. 1-5. <https://doi.org/10.1109/SoutheastCon44009.2020.9368301>
- [5] Pradhan, D., Som, S., Rana, A. (2020). Cryptography encryption technique using circular bit rotation in binary field. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, India, pp. 815-818. <https://doi.org/10.1109/ICRITO48877.2020.9197845>
- [6] Gupta, A., Walia, N.K. (2014). Cryptography algorithms: A review. *International Journal of Engineering Development and Research*, 2(2): 1667-1672.
- [7] Bukhari, S., Arif, M.S., Anjum, M.R., Dilbar, S. (2016). Enhancing security of images by Steganography and Cryptography techniques. In 2016 Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, Ireland, pp. 531-534. <https://doi.org/10.1109/INTECH.2016.7845050>
- [8] Manohar, N., Kumar, P.V. (2020). Data encryption decryption using steganography. In 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, pp. 697-702. <https://doi.org/10.1109/ICICCS48265.2020.9120935>
- [9] Gutub, A., Al-Qahtani, A., Tabakh, A. (2009). Triple-A: Secure RGB image steganography based on randomization. In 2009 IEEE/ACS International Conference on Computer Systems and Applications, Rabat, Morocco, pp. 400-403 <https://doi.org/10.1109/AICCSA.2009.5069356>
- [10] Yahya, A., Yahya, A. (2019). Steganography techniques. *Steganography Techniques for Digital Images*, pp. 9-42. https://doi.org/10.1007/978-3-319-78597-4_2
- [11] Baklizi, M., Atoum, I., Hasan, M.A., Abdullah, N., Al-Wesabi, O.A., Otoo A.A. (2023). Prevention of website sql injection using a new query comparison and encryption algorithm. *International Journal of Intelligent Systems and Applications in Engineering*, 11(1): 228-238.
- [12] Tyagi, V. (2018). *Understanding Digital Image Processing*. Underst. CRC Press.
- [13] Nofriansyah, D., Defit, S., Nurcahyo, G.W., Ganefri, G., Ridwan, R., Ahmar, A.S., Rahim, R. (2018). A new image encryption technique combining hill cipher method, morse code and least significant bit algorithm. *Journal of Physics: Conference Series*, 954: 012003. <https://doi.org/10.1088/1742-6596/954/1/012003>
- [14] Kumar, M., Soni, A., Shekhawat, A.R.S., Rawat, A. (2022). Enhanced digital image and text data security using hybrid model of LSB steganography and AES cryptography technique. In 2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS), Coimbatore, India, pp. 1453-1457. <https://doi.org/10.1109/ICAIS53314.2022.9742942>
- [15] Neamah, R.M., Abed, J.A., Abbood, E.A. (2020). Hide text depending on the three channels of pixels in color images using the modified LSB algorithm. *International Journal of Electrical and Computer Engineering*, 10(1): 809-815. <https://doi.org/10.11591/ijece.v10i1.pp809-815>
- [16] Tayyeh, H.K., Al-Jumaili, A.S.A. (2022). A combination of least significant bit and deflate compression for image steganography. *International Journal of Electrical and Computer Engineering*, 12(1): 358-364. <https://doi.org/10.11591/ijece.v12i1.pp358-364>
- [17] Rustad, S., Syukur, A., Andono, P.N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University-Computer and Information Sciences*, 34(6): 3559-3568. <https://doi.org/10.1016/j.jksuci.2020.12.017>
- [18] Setiadi, D.R.I.M., Rustad, S., Andono, P.N., Shidik, G.F. (2023). Graded fuzzy edge detection for imperceptibility optimization of image steganography. *The Imaging Science Journal*. <https://doi.org/10.1080/13682199.2023.2219880>
- [19] Alatawi, H., Narmatha, C. (2020). The secret image hiding schemes using steganography- Survey. In 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, pp. 1-5. <https://doi.org/10.1109/ICCIT-144147971.2020.9213764>
- [20] Bakde, N.S., Thakare, A.P. (2012). Morse code reader. *International Journal of Recent Technology and Engineering (IJRTE)*, 1(4): 53-56.
- [21] Salim, S.K., Msallam, M.M., Olewi, H.I. (2023). Hide text in an image using Blowfish algorithm and development of least significant bit technique. *Indonesian Journal of Electrical Engineering and Computer Science*, 29(1): 339-347. <http://doi.org/10.11591/ijeecs.v29.i1.pp339-347>
- [22] Mudeng, V., Kim, M., Choe, S. (2022). Prospects of structural similarity index for medical image analysis. *Applied Sciences*, 12(8): 3754. <https://doi.org/10.3390/app12083754>
- [23] Atee, H.A., Hammood, D.A., Yasari, A.K.I. (2022). A steganography approach based on particle swarm optimization and least significant bit in color images. *AIP Conference Proceedings*, 2496: 020018. <https://doi.org/10.1063/5.0090872>