Al-Noor Journal for Information Technology and Cybersecurity

https://jncs.alnoor.edu.iq/

Hiding Encrypted Data In different image Types using spatial domain

M Idrees, M Ahmed, F T Mohammed

College of Computer Sciences and Mathematic, University of Mosul, Iraq

Article information

Article history:
Received: 15 October, 2024
Revised: 5 October, 2024
Accepted: 20 / 11/ 2024

Keywords:
Steganography
Least Significant Bit (LSB),
Normalization Correlation
Peak Signal
Noise Ratio (PSNR)

Correspondence:
Farah Tareq Mohammed
farahtarik@uomosul.edu.iq

Abstract

The development of Informatics fields and data transfer through the internet increases daily. This development has emerged in the need to protect this data by developing cryptographic algorithms and concealment techniques to reach a higher level of protection. This work is developed using the Least Significant Bit (LSB). Focusing on changing concealment sites in the less important cells between points, and also using a suggested algorithm to encrypt grayscale image data by adopting the positivist method of image point locations. The algorithm was applied to more than one grayscale image and the data was hidden in more than one color image. The algorithm was approved and achieved good results after using metrics. The Peak Signal Noise Ratio (PSNR), The Mean Squared Error (MSE), and the Normalization Correlation (NC) standard measure the accuracy of extracted data.

DOI: : https://doi.org/10.69513/jnfit.v1.i0.a6

1. Introduction

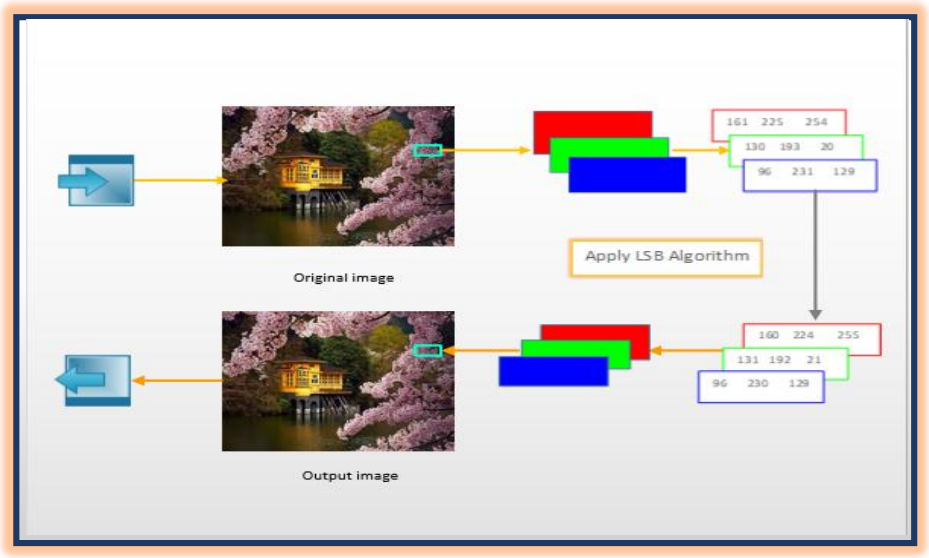
Internet and communication techniques developed and become popular for the user. Security of information become one of the most important things for the users. In the beginning, data encryption is used to encrypt a user's data based on something the user has, something the user is, or something the user knows. The major drawback of encryption is that the data is not hidden. So the attacker tries to find a way or algorithm to decrypt the data. On the other hand, Steganography is a technique of writing and transmitting invisible type hidden messages. In this way, no one can suspect of presence of the message. Researchers proposed many algorithms to provide high security for user information. Some of them use encryption or steganography techniques in their work. Others use mixed techniques of encryption and steganography in their work. De Rosal increases the payload information that the steganography technique hides in the image. Image edge is used for storing information because it is better tolerated to change [1]. M.I. Khalil Studies the deterioration of the medical image in the frequency domain while undertaking the steganography process [2]. M. Jain evaluate several LSB (least significant bit) and LSB array design digital image steganographic

techniques [3]. A. Soria proposed steganography algorithm increases the degree of imperceptibility evaluated by the PSNR measurement [4]. A.Sahu suggested steganographic method which hides 3 bits of secret message in a pixel [5].also, he discussed another technique based on three variants and hidden bits based on the variant [6]. Cao proposed a Novel coverless MSIM-based data hiding system that uses the average value of sub-image pixels to represent secret information by comparing pixel value intervals with secret information and also uses a random sequence to determine the sub-images [7]. Saleh proposed an algorithm based on mixing encryption and steganography, it used the Advanced Encryption Standard (AES) for encryption and steganography techniques for hidden data [8]. Aiswarya Baby made a review the technique of mixing encryption and steganography and showed the strength of this mix [9]. M. Alanzy proposed a multi-level algorithm for steganography by using LSB that enhanced security and saved image quality [10] and, Upadhyay used digital images and combined two techniques for hiding and encrypting a text using LSB [11], Kumar also, combined LSB with RC4 algorithm to achieve both security and hide images [12]. Khalil uses a chaotic map with optimized LSB for multiple data types which are audio, image, and text [13]. GUI used by Panigrahi for ease using a proposed LSB hide data technique when only a selected user can detect it [14]. This paper proposed a hybrid algorithm by mixing encryption and steganography. The paper is organized as follows: the first part is the Introduction including the related works overview, the second part is the Steganography methods in digital images, then the third part is the proposed algorithm, and the fourth is the Graphical interfaces, finally the last two parts are the Results and Conclusion.

2. Steganography methods in digital images:

The technique of hiding confidential information or data is called image steganography. Generally, pixel density is the method used to hide data in the masked images. Images are the most popular covers and are widely used in hiding information. Repetition rates in images made them the most popular types of covers, in hiding information. Two categories of classification were proposed: the spatial domain and the frequency domain for hiding information within images. The spatial domain merges the message directly into the intensity of the pixels while in the frequency domain (also known as the bandwidth) the image is transformed before the message is embedded within it. There are different file extensions for image files. Such as TIFF, JPEG, PNG, GIF, and BMP are used to hide information inside the image. However, all file extensions offer their unique advantages and disadvantages. Because pixel density is used to hide image information, there is sometimes a difference in the intensity of the original image and the resulting image or embedded image. The variation in density is so simple or subtle that it cannot be detected or understood by the human eye. One of the most common ways to hide messages is the LSB algorithm, DCT conversion, FFT conversion, etc. LSB algorithm is classified as a spatial field algorithm while FFT and DCT are located in the bandwidth class. The simplest way to hide the information is LSB which is efficient and cannot distinguish the change in the cover file. The data to be hidden is encoded by modifying the individual pixels of the less important bits of LSB in the cover file to be hidden. The difference is very small. For example, to hide the letter 'C' In color images, each color value is 24bit where the colors of each component red, green, and blue (RGB) are changed as shown in the following Figure(1) and example [15] :

In this paper, we suggest a new idea using the LSB algorithm depending on the serial input position of the most significant bit to indicate the hidden position of the least significant bit as shown in Figure (2). if we input serial position(MSB):(8,6,7,5) ,the resulting is:



Figure(1): Block diagram to explain

R	G	B	R	G	B
161	130	96	1 0 1 0 0 0 0 1	1 0 0 0 0 0 1 0	0 1 1 0 0 0 0 0
225	193	231	1 1 1 0 0 0 0 1	1 1 0 0 0 0 0 1	1 1 1 0 0 1 1 1
254	20	129	1 1 1 1 1 1 1 0	0 0 0 1 0 1 0 0	1 0 0 0 0 0 0 1

R	G	B		R	G	B
1 0 1 0 0 0 0 0	1 0 0 0 0 0 1 1	0 1 1 0 0 0 0 0	⇒	160	131	96
1 1 1 0 0 0 0 0	1 1 0 0 0 0 0 0	1 1 1 0 0 1 1 0	⇒	224	190	230
1 1 1 1 1 1 1 1	0 0 0 1 0 1 0 1	1 0 0 0 0 0 0 1	⇒	255	21	129

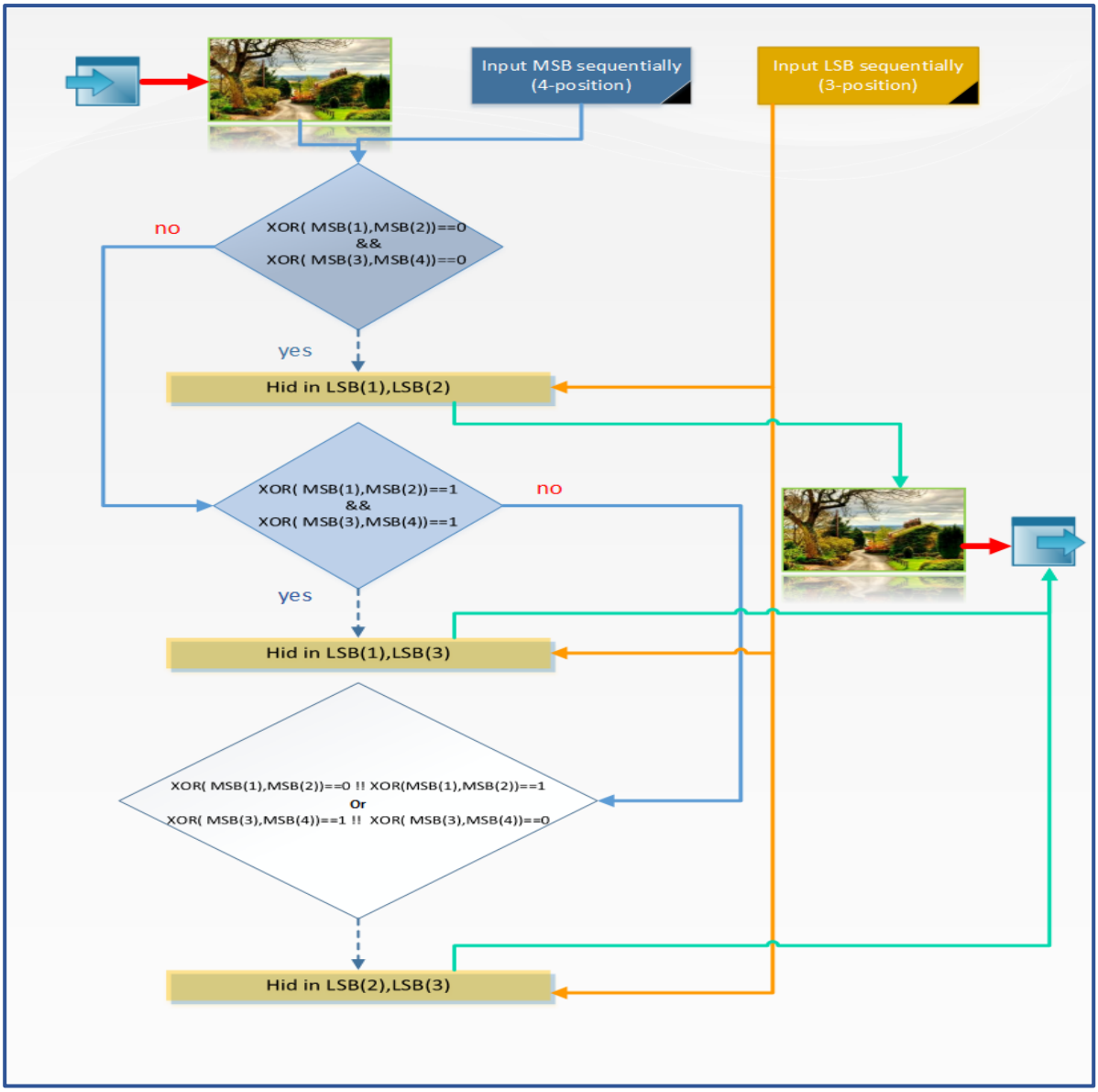
In this paper, we suggest a new idea using the LSB algorithm depending on the serial input position of the most significant bit to indicate the hidden position of the least significant bit as shown in Figure (2). if we input serial position(MSB):(8,6,7,5) ,the resulting is:

If MSB position = [8, 6, 7, 5],MSB(1)=8, MSB(2)=6,, MSB(3)=7,, MSB(4)=5.

LSB position = [3, 1, 2],LSB(1)=3, LSB(2)=1, LSB(3)=2.

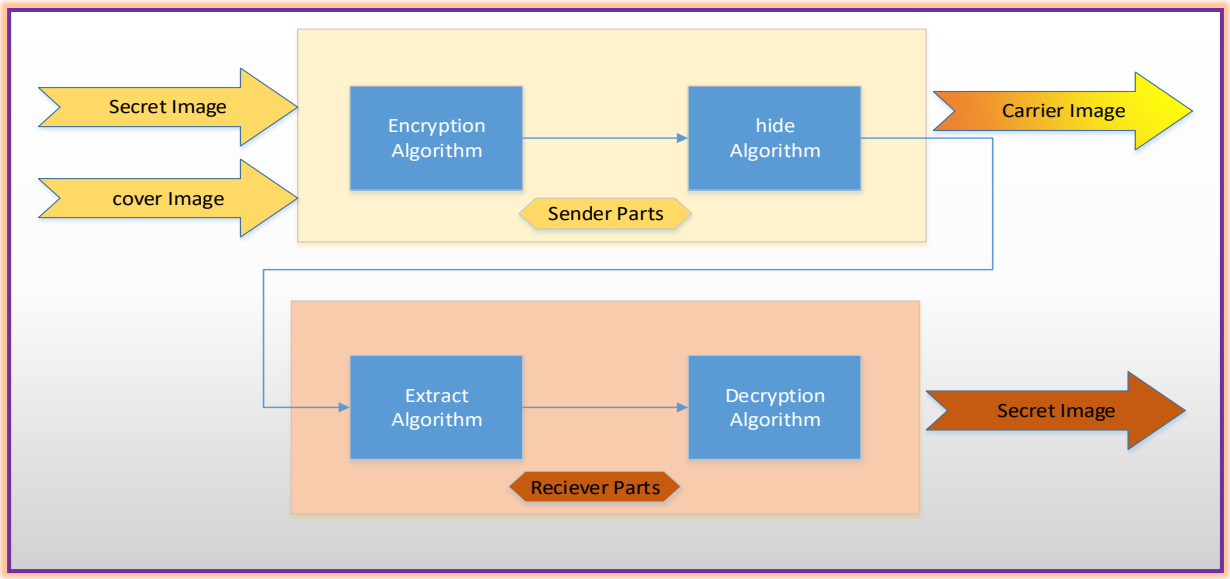
'D' =0 1 1 0 0 1 0 0

161	⇒ 1 0 1 0 0 0 0 1	⇒ 0 1 0 0 0 0 1	⇒
130	⇒ 1 0 0 0 0 0 1 0	⇒ 0 0 0 0 0 0 1	⇒
96	⇒ 0 1 1 0 0 0 0 0	⇒ 1 1 0 0 0 1 0	⇒
225	1 1 1 0 0 0 0 1	1 1 1 0 0 0 0 0	224



Figure(3): Block diagram to show algorithms

hide, and extract algorithm. Each part will be described briefly down as shown in the figure (3):



Figure(3): Block diagram to show algorithms

3.1 Encryption algorithm
This algorithm is used to encrypt the desirable image. The operation perform the following step as shown in the figure (4):
1. The beginning
2. Read the image to be encrypted (grayscale image).
3 - Convert the dimensions of the image to (N X N).
4 - Find the Deference Value for each point of the image according to the following equation: NEW-PIXEL (I, J) = 255 - PIXEL (I, J)..... (1)
5. Divide the image into a set of segments with the same size (as you want).
6. Rotate each section by 90 °.
7. Display the resulting image (after encryption).
8. The end

3.2 Decryption Algorithm:
This algorithm is used to decode the image from the encrypted image. The operation performs the following step as shown in the figure (6):
1. The beginning
2. Read the encrypted image (with a grayscale).
3 - Divide the image into a set of segments with the same size (The selected size).
4. Rotate each section by 90 °.
5 - Find the Deference Value for each point of the image according to the following equation:

NEW-PIXEL (I, J) = 255 - PIXEL (I, J)..... (2)

6- Displaying the resulting image (original).
7- The end

3.3 Hiding Algorithm:
This algorithm is used to hide the encrypted image to add a higher level of security for the proposed algorithm. The operation performs the following step as shown in the figure (5):
1. The beginning
2. Read the color image (cover).
3 - Convert the encrypted image to the binary format.
4. Enter bits values that will hidden within the input sequence (LSB).
5. Enter the bit values that will hidden based on the input sequence (MSB).
6 - The data is hidden in two bits of four bits in color value of each color level based on
a comparison between the values bits.
7. Repeat step 6 until reach the data matrix end of the image encoded.
8. Hide the LSB and MSB input sequence instead of the volume of segments
9. View the cover image, and calculate the PSNR value.
10. The
end

3.4 Extract Algorithm

This algorithm is used to extract the hidden encryption image so the result can be decrypted on another step. The operation performs the following step as shown in the figure (6):

1. The beginning
2. Read the color image (cover).
3. Retrieve the LSB and MSB values sequentially and the size of the section in its hidden form.
4- Retrieving the data from each color value of the sites that were hidden according to the condition, that was based on the values of the MSB to the end of the data matrix of the image based on size.
5. Convert BIT values from binary to decimal**.**
6- Arrange the values in a binary matrix according to the specified size.
7 - Enter the resulting matrix to the decoding algorithm.
8. Display the image after decoding.
9. Calculate NC and MSE values.
10. The end.

4. Graphical interfaces:

Any software requires a graphical user interface to simplify the operation that will be handled by regular users. Three graphical user interfaces were designed for this purpose. The first one as shown in the figure, includes the encryption process for the gray image after selecting the image to hide and specifying the size of the segment.

Figure (4) shows the interface of the encryption process

The second interface includes the process of selecting the cover image with the sequence of sites for the least and most important sites for concealment and calculation of the PSNR ratio.

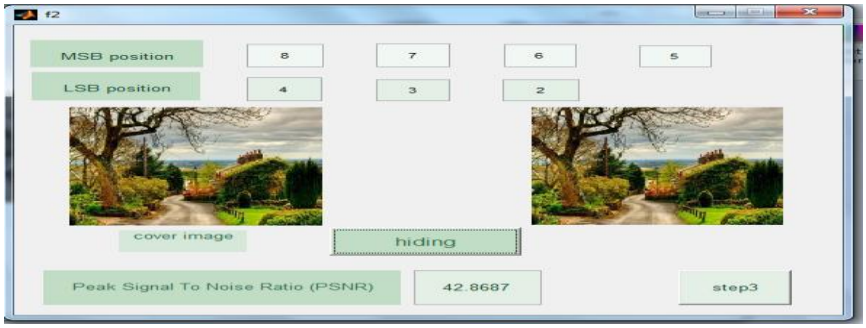


Figure (5) shows the interface of the concealment process.

The third interface includes the process of retrieving the encrypted image and decryption and calculating the ratio of NC to the secret image (retrieved).

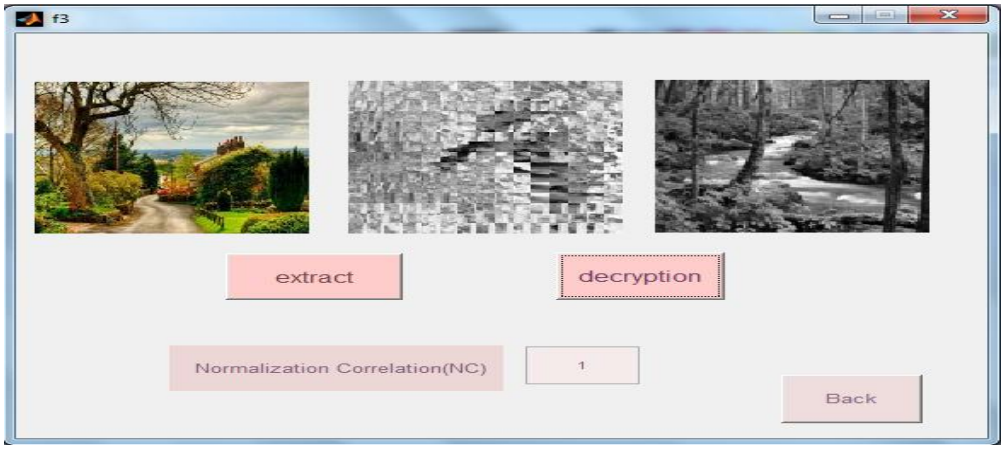


Figure (6) shows the special interface for retrieving the encrypted image and decryption.

5. Results

Several measurements were used to measure the quality of the images resulting from the proposed algorithms. Three types of measurements used for this purpose: Normalization Correlation (NC), Mean Squared Error (MSE), and Peak Signal to Noise Ratio (PSNR) The equation is mentioned as follows [15][16].

1. Normalization Correlation (NC)

$$NC=\sum_i\sum_j sw(i,j)*s(i,j) \,/\, \sqrt{\sum i\sum j\, sw(i,j)^2} * \sqrt{\sum i\sum j\, s\,(i,j)^2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

2. Mean Squared Error (MSE)

$$MSE=1/M*N \;\; \sum_{i,j}(sw(i,j)-s(i,j))^2 \quad \ldots\ldots\ldots\ldots\ldots\ldots (2)$$

3. Peak Signal To Noise Ratio (PSNR)

$$PSNR=20*\; Log10(255/\sqrt{\frac{1}{M*N}*\sum_i\sum_j(sw(i,j)-s(i,j))_2}) \quad \ldots\ldots\ldots\ldots (3)$$

which: sw: represents the values of the array containing the hidden data
s: such as the values of the original matrix
M: represents the number of rows
N: represents the number of columns

(1) and the rate of distortion was not realized. This indicates that the retrieved image is completely identical. It also, shows the efficiency of the algorithm's performance in coding and hiding the data at the 24-bit.in which 2-bit changed from the first 4-bits of each color value (6-bit per pixel). It is noted that the image size change is not related to the performance of the algorithm because it passes all points of the image sequentially (ie, Image without exception). Table (1) shows some values resulting from the implementation of the algorithm.

proposed algorithm performs on more than one image each of them has a different size. The results for the images have the same value for the correlation coefficient and rate of distortion. The values for the correlation coefficient were equal to

Table (1) Resulting values of the suggestion algorithm

Name of the cover image	size	The name of the hidden image	size	PSNR	NC	MSE	Bit sequence
Im1.jpg	320x320	En-im1.jpg	160x160	43.0783	1	0	LSB(4-3-2) MSB(8-7-6-5)
Im1.jpg	320x320	En-im1.jpg	160x160	48.4359	1	0	LSB(1-2-3) MSB(6-8-5-7)
Im2.Bmp	320x320	En-im2.bmp	160x160	47.1273	1	0	LSB(2-3-1) MSB(5-6-8-7)
Im3.Bmp	240x240	En-im3.bmp	120x120	47.1553	1	0	LSB(1-3-2) MSB(5-6-7-8)
Im4.png	240x240	En-im4.jpg	120x120	44.0843	1	0	LSB(4-1-2) MSB(5-6-7-8)
Im5.png	200x200	En-im5.png	100x100	49.3869	1	0	LSB(3-1-2) MSB(8-7-6-5)
Im6.png	280x280	En-im6.png	140x140	48.2460	1	0	LSB(2-1-3) MSB(7-8-5-6)
Im7.png	320x320	En-im7.jpg	160x160	47.8397	1	0	LSB(1-2-3) MSB(6-7-8-5)

6. Conclusion:

A hybrid combination of encryption and steganography is introduced in this paper. This combination provides more data security compared with each technique alone. Image information is encrypted and then hidden in another image. The measurement that is performed on the image samples shows the effectiveness of this combination. Also, it promises to get a better security level in the future after making more enhancements to it. The proposed algorithm can be used in different data communication applications to ensure data security. For example, Sending photocopies of a transcript throw the internet by e-mail and other applications

.

7. References

1] De Rosal Ignatius Moses Setiadi1Jumanto, Jumanto. "An enhanced LSB-image steganography using the hybrid Canny-Sobel edge detection." Cybernetics and Information Technologies 18, no. 2 (2018): 74-88.
[2] Khalil, M. I. "Medical image steganography: Study of medical image quality degradation when embedding data in the frequency domain." International Journal of Computer Network and Information Security 9, no. 2 (2017): 22.
[3] Jain, Mamta, and Saroj Kumar Lenka. "A review of digital image steganography using LSB and LSB array." Int. J. Appl. Eng. Res 11, no. 3 (2016): 1820-1824.
[4] Soria-Lorente, Anier, and Stefan Berres. "A secure steganographic algorithm based on frequency domain for the transmission of hidden information." Security and Communication Networks 2017 (2017).
[5] Sahu, Aditya Kumar, and Gandharba Swain. "Information hiding using group of bits substitution." International Journal on Communications Antenna and Propagation 7, no. 2 (2017): 162-167.
[6] Sahu, Aditya Kumar, and Gandharba Swain. "An improved data hiding technique using bit differencing and LSB matching." Internetworking Indonesia Journal 10, no. 1 (2018): 17-21.
[7] Cao, Yi, Zhili Zhou, Xingming Sun, and Chongzhi Gao. "Coverless information hiding based on the molecular structure images of material." Computers, Materials & Continua 54, no. 2 (2018): 197-207.
[8] Saleh, Marwa E., Abdelmgeid A. Aly, and Fatma A. Omara. "Data security using cryptography and steganography techniques." International Journal of Advanced Computer Science and Applications 7, no. 6 (2016): 390-397.
[

[9] Baby, Aiswarya, and Hema Krishnan. "Combined Strength of Steganography and Cryptography-A Literature Survey." International Journal of Advanced Research in Computer Science 8, no. 3 (2017).
[10] Alanzy, May, Razan Alomrani, Bashayer Alqarni, and Saad Almutairi. "Image steganography using LSB and hybrid encryption algorithms." Applied Sciences 13, no. 21 (2023).
[11] Upadhyay, Aditya, Rahul Misra, Santosh Kumar Henge, and Yogesh Bhardwaj. "Protection of Digital Image and Text Information Security Using LSB and Crossover Techniques." In Computational Vision and Bio-Inspired Computing: Proceedings of ICCVBIC 2022, pp. 601-608. Singapore: Springer Nature Singapore, 2023.
[12] Kumar, Nitish, Vasu Lakhani, Karanveer Singh, Mahim Bhardwaj, and Shubham Raj. "Development of LSB Based Steganography Method for Video and Image hiding." In 2024 11th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO), pp. 1-6. IEEE, 2024.
[13] Khalil, Noura, Amany Sarhan, and Mahmoud AM Alshewimy. "A secure image steganography based on LSB technique and 2D chaotic maps." Computers and Electrical Engineering 119 (2024).
[14] Panigrahi, Rasmita, and Neelamadhab Padhy. "An effective steganographic technique for hiding the image data using the LSB technique." Cyber Security and Applications 3 (2025).
[15] Farah Tareq," Dual Hiding in Digital Image Files", AL Rafidain Journal of Computer Sciences and Mathematics, no 8 (2011)
[16] Farah Tareq," Hybrid hiding in multimedia files", Al Rafidain Journal of Computer Sciences and Mathematics, no. 9 (2012).