Science Journal of Circuits, Systems and Signal Processing
2023; 11(1): 12-18
http://www.sciencepublishinggroup.com/j/cssp
doi: 10.11648/j.cssp.20231101.12
ISSN: 2326-9065 (Print); ISSN: 2326-9073 (Online)

A Web-based Least Significant Bit (LSB) Image Steganographic Technique

Nimishkumar Baldha

Department of Computer Science, University of Regina, Regina, SK, Canada

Email address:
nbt599@uregina.ca

To cite this article:
Nimishkumar Baldha. A Web-based Least Significant Bit (LSB) Image Steganographic Technique. *Science Journal of Circuits, Systems and Signal Processing*. Vol. 11, No. 1, 2023, pp. 12-18. doi: 10.11648/j.cssp.20231101.12

Received: July 5, 2022; **Accepted**: October 11, 2022; **Published**: July 6, 2023

Abstract: Steganography is the art of hiding secret messages into cover during communication. Steganography is a technique for sending secret messages across ordinary cover carriers in such a way that the presence of the messages is unnoticed. There are various steganographic techniques based on the cover being used in the steganographic process. The covers can be an image, audio, video, and text. The most widely used steganographic technique nowadays is Image Steganography. Image steganography is hiding the existence of the data using the image as the cover object. Most of the image steganographic technique hides the secret messages as plaintext and intruders may try to extract the secret message if he/she knows that the image being communicated is a stego image. In this paper, a web-based Least Significant Bit (LSB) image steganographic technique with two layers of AES encryption that does not require a key exchange mechanism between sender and receiver is explained. The proposed method follows six step mechanism on the sender's side which includes user authentication to initiate communication, two 128-bit key generation and storing it to the central server database, message encryption using one of the generated keys in previous step and image encryption using another key followed by the image steganography. The image generated after sixth step is ready to send via any medium to the receiver. The receiver of the image also follows six steps process to convert the stego image to the decrypted message. After completing the authentication, receiver inputs the received image from the sebder and the system checks for the integrity of the inputted image. Once the integrity is verified, the system pulls the decryption keys from the database. Using this decryption keys, the image decryption and message takes place. The goal of the proposed method is to avoid key exchange mechanism using client/server architecture. The proposed method encrypts the secret message and stego image to add another layer of security.

Keywords: Image Steganography, Cryptography, Advanced Encryption Standard, Image Encryption, Least Significant Bit (LSB) Steganography

1. Introduction

Steganography is the art and science of concealing one piece of information within another piece of information, such as text, video, audio, or a picture, such that it is not visible to unwanted users. It's the art of enclosing a message with a cover while leaving no trace on the original message. Steganos (covered or secret) and Graphie (writing) are Greek terms that literally mean "covered writing" [14]. Its beginnings may be dated back to the year 440 BC. The fundamental purpose of steganography is to conceal important information among other seemingly harmless carriers in such a manner that no one other than the authorized user can discover that it contains a hidden message [1].

Here is it important to note that, both steganography and cryptography are used to safeguard sensitive information from unwanted users in a different way. The primary difference between cryptography and steganography can be understood using the definitions of each: steganography is a technique to hide the existence of the communication, on the other hand, cryptography is the technique to convert data into the incomprehensible form [2]. The purpose of steganography is to make communication secure while cryptography provides data protection. As we are hiding the existence of the message so the data is not visible after performing steganography, on the contrary, the data is visible in the case of cryptography.

In cryptographic techniques, we are hiding the data into cover without altering the format of the data while cryptography alters the structure of the data [2].

Numerous steganographic techniques have been invented and worked on in the last decade but the most common steganographic technique is the Least Significant Bit (LSB) steganography which replaces the LSB of the image pixel. A decent steganography approach focuses on three factors: capacity (the highest amount of information that can be buried inside the cover picture), visual quality, and resilience [3]. In recent years, CNN based image steganographic techniques also introduced which is inspired from encoder-decoder architecture. These techniques uses CNN model thus needs more computation than the traditional techniques [15].

The proposed steganographic technique takes advantage of three concepts: Cryptography (to secure data), Steganography (to hide data) and client-server architecture (to remove the requirement of the key sharing mechanism). There are two reasons behind choosing client-server architecture: Eliminate key sharing process and check the integrity of the message.

The paper is organized into the following sections: section 2 explains related works, section 3 explains the proposed method, section 4 demonstrate example and results, section 5 shows advantages and limitations and section 6 is the conclusion and future works.

2. Related Works

Many methods for image steganography have been proposed. The least significant bit (LSB) approach is the most used method for concealing any information in an image [5]. The method authors have proposed in "LSB Based Text and Image Steganography Using AES Algorithm" performs the steganography and encryption using Advanced Encryption Standard (AES). In the author's method, the steganography process takes place first then the stego image is given to AES encryption in order to provide security for the hidden data [6]. This method required an AES key exchange mechanism between sender and receiver and does not check for the integrity of the data. Another study on "Data Hiding Through Multi-Level Steganography and SSCE" demonstrate a secret key steganographic model is developed that employs plain text as the cover data and the secret message is embedded in the cover data to make the stego text, which is then inserted into the cover picture to form the stego image [7]. Another paper describes a system for transmitting huge amounts of secret data while maintaining a secure connection between two communication partners. To make detection more difficult, steganography and cryptography can be integrated into this approach. As a secret message, any type of text data can be used. The hidden message is conveyed across the network using the steganography principle. Furthermore, the proposed approach is straightforward to apply. The created system also offers a wide range of practical, personal, and military uses for both point-to-point and point-to-multipoint communications [8].

In [9], a method is provided in which two major algorithms, Advanced Encryption Standard (AES) and RC5, are employed. As is well known, AES may generate a 128-bit cypher text, and in our technique, the RC5 algorithm employs a 128-bit block size. Each image will also include a watermark to ensure that the images are delivered securely. A cover image can be created in a variety of ways, including LSB, DCT, and DWT.

In [10], a technique for enhancing the security of cloud data employing information hiding, hashing, and encryption is described. The AES symmetric encryption method and the RSA asymmetric encryption algorithm were used by the author to construct hybrid encryption during the data encryption stage. After that, the LSB method will be used to conceal the encrypted data within a picture. The system employs the SHA hashing technique during the data validation stage.

The authors followed four procedures on both the sender and receiver end to improve data security in order to develop a strong and successful model. On the sender's end, the targeted picture is first encrypted using AES, and then, using the LSB method, the targeted text data is cloaked inside the AES encrypted image. By employing LSB-based picture steganography to disguise this combined text image with a cover image, the data security is further strengthened. For safe data transmission from the sender end, the Stego picture is separated and indexed in the last step [11].

The author in [12] suggested using the Shannon-Fano compression technique to boost the steganography image's PSNR (Peak Signal-to-Noise Ratio) value. The LSB (Least Significant Bit) steganography technique and the AES (Advanced Encryption Standard), the current standard for symmetric key encryption, are employed in the StegoCrypto algorithm. In order to improve the value of the PSNR steganography image, the employment of the compression approach in conjunction with the Shannon-Fano method attempts to decrease the quantity of embedded data.

The healthcare institutions have seen multiple data breach incidents in recent years. These cyberattacks broke the Health Information System's (HIS) confidentiality rules, exposing a huge volume of patient information. By employing digital mammograms as the cover picture during the steganography process, the author in [13] describes a method for protecting and maintaining the privacy of the patient data for breast cancer.

3. Proposed Method

The proposed method is divided into two parts: Sender and Receiver. The system performs encryption and steganography on the sender side and decryption, integrity checks and reverse steganography on the receiver side. The proposed technique for the sender is shown in Figure 1. The sender side process is a six-step process and the six steps are as follows:

Step 1: User Authentication

Step 2: User Input (Secret Message, Image)

Step 3: Keys Generation (K1, K2)
Step 4: Message Encryption
Step 5: LSB Image Steganography
Step 6: Image Encryption

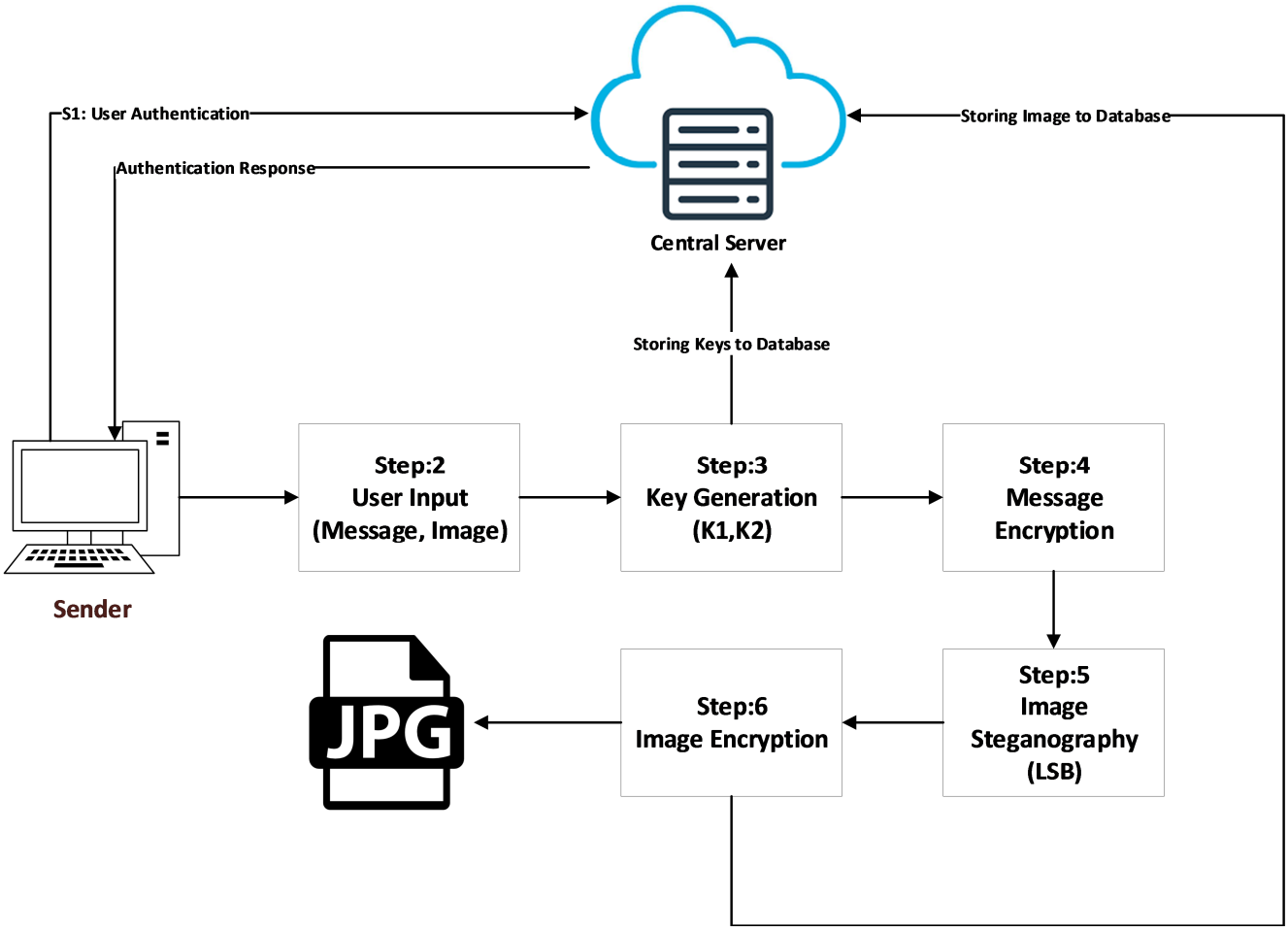

Figure 1. *Proposed Method Sender's Architecture.*

Let's understand these six steps in detail:

Step 1: User Authentication:

In this first step of the process, the user needs to authenticate himself/herself through username and password. The user will enter the username and password and the system will let the user enter into the system. Here it is important to note that two-factor authentication mechanisms such as OTP, security questions or biometric can be used to provide more security. So when a user enters into the system he/she can use GUI to perform encoding or decoding.

Step 2: User Input:

The user needs to enter the secret message and the colour cover image. Here the binary length of the secret message must be according to the number of pixels in the image because each character will be encoded in one pixel of the image and the colour cover image is important. After all, the proposed method will be encoding the bits on the "Blue" colour of each pixel.

Step 3: Key Generation:

The system will generate two random 128-bit keys for AES encryption. The important property of these keys are it's unique for each image steganography transaction you perform, For example, you go into the system and complete the sender's six steps for one image and one message and you want to use the system for a second message then the secret keys for both the transaction will be different. The process of generating these keys is in two steps: In the first step, the system takes a random number and micro time and append both numbers to get the final number. Here, the micro time is the current Unix timestamp in microseconds. In the second step, Message-Digest Algorithm (MD5) is used to calculate the 128-bit hash value (i.e key) of the final number. This key generation process runs two times to generate two different keys. One for the message encryption and one for the image encryption. Here it is important to note that, the generated keys are stored in the server database which later will be retrieved on the receiver side. The purpose of storing these keys into the server database is to eliminate the requirement of a key exchange mechanism between sender and receiver as these stored keys will be retrieved automatically by the system for the decryption on the receiver side.

Step 4: Message Encryption:

In this step, the input message will be encrypted using the AES 128-bit algorithm and CBC encryption mode.

One of the 128-bit keys from step-3 will be used to encrypt the message. The encrypted message will be stored in the server database for integrity check on the receiver side. This step also converts the encrypted message into binary to embed the message into the image.

Step 5: LSB Image Steganography:

The rationale behind LSB embedding is that changing the final bit value of a pixel will not result in a noticeable change in colour. 0 is black, for example. Changing the value to 1 won't make much of a change because the colour is still black but in a lighter tint.

LSB Steganography Process:

A) Convert message to Binary:

B) Validate the size of the image according to the message size (i.e the number of pixels in the image must be greater than or equal to the size of the binary message as each pixel in the image can embed one bit of the binary message).

C) Loop through each bit of the message

(i) Get the RGB value of the pixel

(ii) Convert 'Blue' to binary

(iii) Inject the message bit to LSB of the 'Blue' colour

After completing the LSB steganography process the new image is produced with minimal colour/shade change of the cover image.

Step 6: Image Encryption:

The stego image generated by step-5 contains an encrypted message embedded into the pixels of the image. In this step, the stego image will be encrypted using the AES 128-bit algorithm and CBC encryption mode. The second 128-bit key that we have generated in step-3 will be used to encrypt the stego image. The encrypted image will be stored in the server database for integrity check on the receiver side. The encrypted image is ready for transmission to the receiver through any medium suitable for the sender as well as the receiver. The secret message has four-layer protection during transmission and it is impossible to decrypt the message during transmission.

Now let's look at the proposed technique for the sender. The proposed technique for the receiver is shown in Figure 2. The receiver side process is an eight-step process and the eight steps are as follows:

Step 1: User Authentication
Step 2: User Input (Stego Image)
Step 3: Integrity Checks
Step 4: Keys Retrieval (K1, K2)
Step 5: Image Decryption
Step 6: Recovering Encrypted Message from the Image
Step 7: Message Decryption
Step 8: Data Destruction

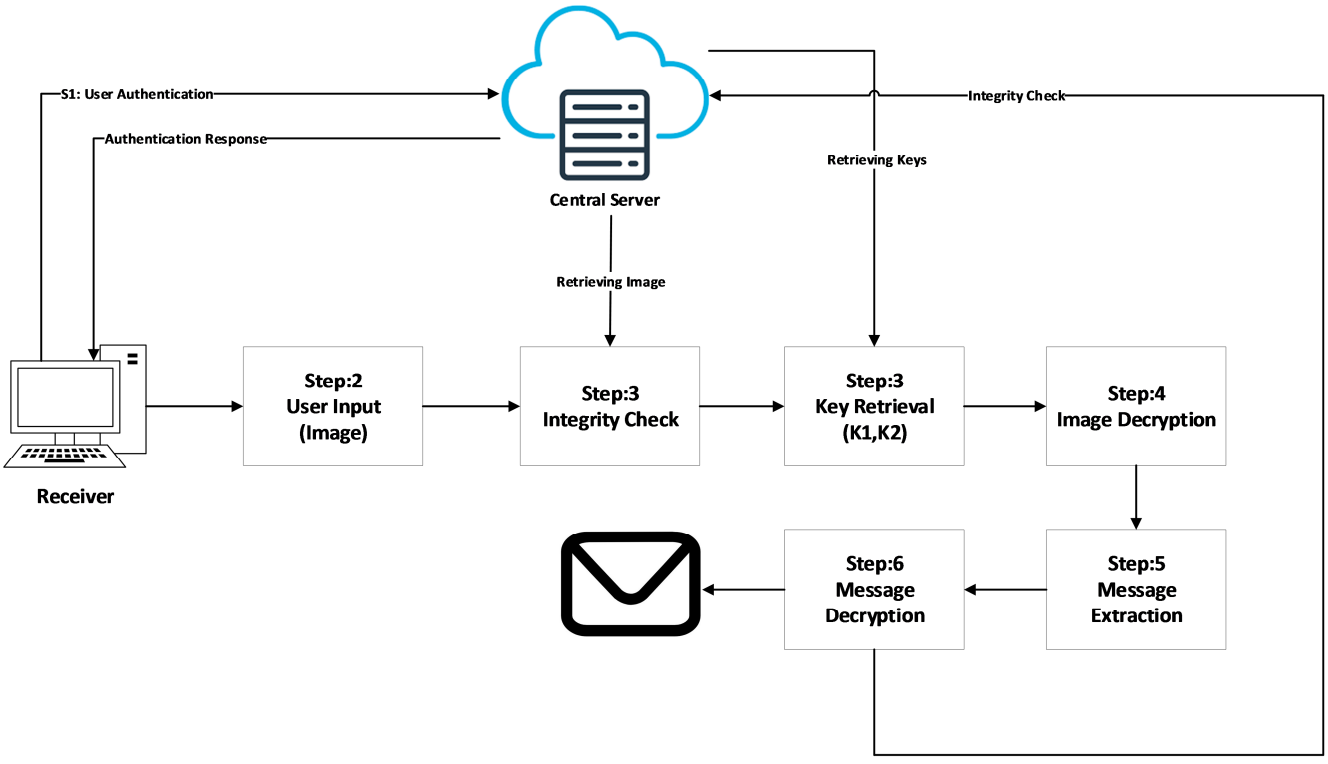

Figure 2. *Proposed Method Receiver's Architecture.*

Here it is seen that the receiver side is almost reversed to the sender's side with two additional steps: Integrity Check and Data Destruction.

Step 1: User Authentication

The user authentication step-1 is the same as sender step-1 rest of the steps are explained in subsequent paragraphs.

Step 2: User Input

In this step, the receiver user inputs the stego image received from the sender. The steps process the image and extract the important metadata of the image. The most

important metadata is the actual name of the image without the extension (e.g. jpg, png) and the name is used as the database key to retrieve the keys and to check the integrity of the received stego image.

Step 3: Integrity Check

In this step, the encrypted image stored in the database while performing the steganographic process on the sender side is compared with the image entered by the user. To compare the image we first need to retrieve the image stored in the database and to do this the metadata extracted in the previous step will be used. If both the images are the same then the image is not altered during communication and can safely be decrypted but if the images are not the same then the process will be stopped and the user will receive an error message.

Step 4: Key Retrieval

After completing the integrity check the system will retrieve the keys for the AES decryption from the server database. Again, the metadata extracted in step-2 will be used to retrieve the keys from the database.

Step 5: Image Decryption:

In this step, the image decryption will take place using the appropriate 128-bit decryption key that is retrieved in the previous step. The output of this step is the stego image with the embedded encrypted secret message in it.

Step 6: Recovering Encrypted Message from the Image:

We must go through the image one pixel at a time. In an array of extracted bits, we save the Least Significant Bit (LSB) of each pixel. After extracting the LSBs of the relevant pixels, we must convert each 8 bit from extracted bits to the appropriate character. The text encoded in the stego picture may thus be retrieved in this manner [4].

Step 7: Message Decryption:

In this step, the system will decrypt the message retrieved from the stego image using another key that we have retrieved in the key retrieval step. The outcome of this step is the secret message in a readable form.

Step 8: Data Destruction

This step destroys the data as the name suggests. As we know the confidentiality of the data is the most important thing in steganography and cryptography. This step destroys the secret data stored in the database. The data destruction takes place in two cases: when the user logs off from the system or after the defined time interval by the system. This process ensures that the data is not retrievable after destruction even if the user has an image received from the receiver. For example, the receiver received the stego image from the sender and retrieved the secret message from the image. Now, the receiver logged off from the system or defined time interval passed that means system has destroyed the data. The same receiver is logging into the system and trying to use the same image to retrieve the message then the system will show the error message to the receiver even though the user is legit. The purpose of this process is, in case the hacker got the used stego image and tries to retrieve the same message that has already been retrieved by the legit user then the hacker will not be able to retrieve the message as the data is destroyed by the system when the message was retrieved by the actual legit user for the first time.

4. Example and Results

Authentication: The sender authenticated himself/herself using a username and password.

User Input: The sender wants to send “Hello World” to the receiver as a secret message.

Message: Hello World

Cover Image:

Figure 3. *Cover Image.*

Key Generation:

1st Key:

Random Number: 707136259

Microtime: 0.21220200 1635696012

Final Number: 20107178360.212202001635696012

MessageDigest (20107178360.212202001635696012)

Key 1: c3c7a6511099e03b6994b0d541881120

Similarly, we can generate 2nd key:

Key 2: 11286bb6df85f24ad46cc5b415c2960c

Message Encryption (AES 128-bit, CBC, Key 1):

Encrypted Message: v6uatN0+yWzcGVs8z2dqew==

This encrypted message is converted to binary to embed into the image.

Image Steganography (LSB):

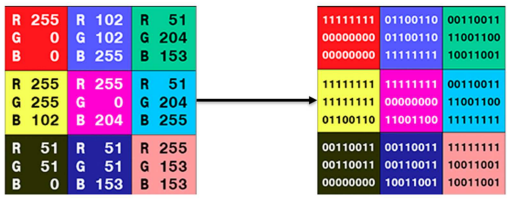

Figure 4. *LSB Operation.*

Encrypted Message Bit: 1

Cover Image Blue Pixel: 00000000 00000001

Output Stego Image:

Figure 5. *Stego Image (Embedded Message).*

Image Encryption (AES 128-bit, CBC, Key 2):

The stego image (Figure 5) is encrypted using AES 128-bit encryption and CBC encryption mode. The output will be a jpg image but cannot be opened using an image viewer as the image is encrypted.

Output:

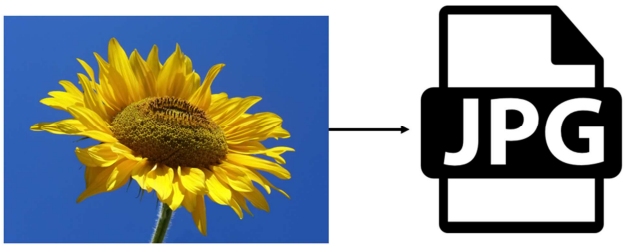

Figure 6. *Stego Image Encryption.*

Now, the output of this step is ready for transmission through any medium.

5. Advantages and Limitations

There are several advantages of using the proposed technique and the most important advantage is that the proposed technique does not require a key exchange channel/mechanism to perform AES encryption/decryption. Apart from that, this is a web-based steganographic technique so the sender and receiver can send/receive a message from anywhere in the world where the internet connection is available. Additionally, this method provides both confidentially and integrity checks of the secret data. On the other hand, the major limitation of the system is that the highly secure infrastructure is required to store data and access to the web application for sender and receiver must be enforced to modern authentication mechanisms such as Biometric, Two-factor mechanisms etc. The minor limitation is that the limited size of the message can be transmitted using this method.

6. Conclusion, Discussion & Future Work

The proposed steganography method hides and secures the existence of the message during communication by performing LSB image steganography and by encrypting stego image. The method enforces the confidentiality of the data using two layers of encryption: Encryption of Message & Stego Image. As described, the presented technique conceals the presence of the message and misguide the hackers. Apart from that, the system uses double encryption mechanism to make it impossible for the unauthorized users to retrieve the plain text. Additionally, the mechanism provides integrity of the data by comparing encrypted and received images on the receiver side. The system will help to circumvent the key exchange pipeline and to make it impractical to comprehend the message. In future, work can be done to increase the size of the message to be transmitted.

References

[1] A. Singh and H. Singh, "An improved LSB based image steganography technique for RGB images," 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2015, pp. 1-4, DOI: 10.1109/ICECCT.2015.7226122.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp. 68–73.

[3] Nadeem Akhtar, Pragati Johri and Shahbaaz Khan, "Enhancing the Security and Quality of LSB based Image Steganography", IEEE 5th International Conference on Computational Intelligence and Computer Networks, pp. 385-390, September 2013.

[4] Text extraction from image using LSB based steganography. (2019, -03-15T18:42:30+00:00). Retrieved from https://www.geeksforgeeks.org/text-extraction-from-image-using-lsb-based-steganography/

[5] J. Fridrich and M. Long, "Steganalysis of LSB encoding in color images", 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No. 00TH8532), vol. 3, pp. 1279-1282, July 2000.

[6] P. P. Bandekar and G. C. Suguna, "LSB Based Text and Image Steganography Using AES Algorithm," 2018 3rd International Conference on Communication and Electronics Systems (ICCES), 2018, pp. 782-788, doi: 10.1109/CESYS.2018.8724069.

[7] Bhattacharyya, Dr. Souvik & Banerjee, Dr- Indradip & Sanyal, Prof (Dr.) Goutam. (2011). Data Hiding Through Multi Level Steganography and SSCE. Journal of Global Research in Computer Science.

[8] Shashikala, Channalli & Ajay, Jadhav. (2009). Steganography An Art of Hiding Data. International Journal on Computer Science and Engineering. 1.

[9] M. S. Hossen, M. A. Islam, T. Khatun, S. Hossain and M. M. Rahman, "A New Approach to Hiding Data in the Images Using Steganography Techniques Based on AES and RC5 Algorithm Cryptosystem," 2020 International Conference on Smart Electronics and Communication (ICOSEC), 2020, pp. 676-681, doi: 10.1109/ICOSEC49089.2020.9215442.

[10] M. S. Abbas, S. S. Mahdi and S. A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography," 2020 International Conference on Computer Science and Software Engineering (CSASE), 2020, pp. 123-127, doi: 10.1109/CSASE48920.2020.9142072.

[11] M. S. Hasan Talukder, M. N. Hasan, R. I. Sultan, M. Rahman, A. K. Sarkar and S. Akter, "An Enhanced Method for Encrypting Image and Text Data Simultaneously using AES Algorithm and LSB-Based Steganography," 2022 International Conference on Advancement in Electrical and Electronic Engineering (ICAEEE), 2022, pp. 1-5, doi: 10.1109/ICAEEE54957.2022.9836589.

[12] W. Dharma Walidaniy, M. Yuliana and H. Briantoro, "Improvement of PSNR by Using Shannon-Fano Compression Technique in AES-LSB StegoCrypto," 2022 International Electronics Symposium (IES), 2022, pp. 285-290, doi: 10.1109/IES55876.2022.9888656.

[13] S. Khalifeh, J. Georgi and S. Shakhatreh, "Design and Implementation of a Steganography-based System that Provides Protection for Breast Cancer Patient's Data," 2022 56th Annual Conference on Information Sciences and Systems (CISS), 2022, pp. 19-24, doi: 10.1109/CISS53076.2022.9751183.

[14] A. N, A. V. K and N. R, "Sharing Confidential Images with Abbreviated Shares using Steganography and AES Algorithm," 2022 2nd International Conference on Intelligent Technologies (CONIT), 2022, pp. 1-5, doi: 10.1109/CONIT55038.2022.9847932.

[15] N. Subramanian, O. Elharrouss, S. Al-Maadeed and A. Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409-23423, 2021, doi: 10.1109/ACCESS.2021.3053998.