



## A Mechanism of Confidential Message Transfer using Steganography Approach

Sayantana Chakrabarti <sup>a</sup>, Avirup Pal <sup>b\*</sup>

<sup>a</sup> Assistant Professor, BPPIMT, Kolkata, 700052, India

<sup>b</sup> Student, BPPIMT, Kolkata, 700052, India

### ABSTRACT

In this era of digital advancements, where information traverses networks ceaselessly, the paramount need for safeguarding communication and protecting data has emerged. Steganography, the fusion of art and science, offers an intriguing remedy to this challenge by concealing information within seemingly unremarkable carriers. Among the array of steganography techniques, the method of Least Significant Bit (LSB) has gained widespread adoption as a versatile and extensively employed approach. This study introduces an innovative embedding algorithm tailored for secure image steganography. Through the harmonious employment of LSB technique, 1's complement operation, XOR operation, and public key encryption, the algorithm adeptly conceals a clandestine image within a cover image. Remarkably, this process maintains the visual fidelity of the cover image while ensuring the utmost confidentiality and integrity of the hidden data. Rigorous experimental evaluations unequivocally showcase the algorithm's prowess in terms of security, embedding capacity, imperceptibility, and resistance against steganalysis techniques. The outcomes unequivocally affirm the superiority of the proposed technique, thus positioning it as a highly promising solution for applications in secure image steganography.

Keywords: Image steganography, embedding algorithm, LSB, 1's complement, XOR operation, public key encryption, security, visual quality

### Introduction

Steganography, a clandestine art honed over decades, serves as the veil that shrouds classified messages, rendering it virtually invisible to unsuspecting eyes. Unlike its cryptographic counterpart, which locks away data through complex algorithms, steganography dances in the realm of hidden messages, requiring the knowledge of where to look. Its roots trace back to ancient times, where ingenious minds etched secrets upon messengers' scalps, inscribed them in invisible ink, or ingeniously tucked them away within the soles of shoes. In our digital age, steganography has evolved, finding refuge within the depths of digital communication, seamlessly embedding messages within images, audio files, or even the whitespace of a simple text document [1][2].

Within the digital realm, a plethora of techniques emerges, each holding its own secrets for concealing messages. Enter the world of LSB steganography, where the subtlest alteration of a pixel's least significant bit in an image or the least significant byte within an audio file encodes a hidden treasure of message. Meanwhile, spread-spectrum steganography emerges as an elusive muse, cleverly dispersing the message across multiple frequencies within an audio signal, playing a symphony of concealment that evades detection [1][2].

#### 1.1 Steganography Techniques

- **Text Steganography:** Within the realm of text files lies a clandestine world where hidden messages take shape through the method of steganography. Hidden within the fabric of characters and words, these messages cloak themselves in the guise of the original text, rendering themselves indistinguishable to the casual observer. Such a technique has gained popularity as a means to safeguard sensitive information, including the likes of credit card numbers and other confidential data. In this discourse, we shall delve into the realm of text file steganography, exploring the diverse methods employed to veil and secure vital information [1][12].
- **Image Steganography:** Embarking upon an ethereal odyssey, image steganography unveils a clandestine realm where data seeks refuge within the very essence of images. Guided by the celestial dance of pixel intensities, this arcane art conceals messages, shrouding them within a cover image's veil of secrecy. Within this enigmatic tapestry, the cover image becomes a sanctuary, the pixel intensities its guardians of hidden truths. As the story unfolds, a mesmerizing cast takes the stage – the covert message bides its time, the stego image emerges like a mirage, and the stego key unlocks the gateway to cryptic revelations. Together, they compose an extraordinary symphony of secrecy, wherein art and enigma entwine, leaving observers entranced by the mysteries concealed within an unsuspecting image [2][5].
- **Audio Steganography:** Within the realm of information security, steganography emerges as a captivating art form, skillfully hiding data within a myriad of formats. Its purpose extends beyond mere content protection, encompassing the preservation of intellectual property and personal privacy.

Like a hidden gem, watermarking discreetly encrypts messages within carriers, particularly finding its stride in the realm of media playback, where audio clips serve as the clandestine vessels of encrypted secrets. In this intriguing tapestry of concealment and discretion, steganography weaves its unique spell, safeguarding information while preserving the delicate balance between visibility and hidden depths [14].

- **Video Steganography:** In the realm of video steganography which involves a method of secretly embedding data or other files within a video file on a computer. Video (a collection of still images) can function as the "carrier" in this scheme. Discrete cosine transform is commonly used to insert values that can be used to hide the data in each image in the video, which is undetectable to the naked eye. Video steganography typically employs the following file formats: H.264, MP4, MPEG, and AVI [15]. If you want to hide your message in an existing video file, there are several ways to do so:
  - Use an external application such as WinZip or 7-Zip that supports .zip files
  - Use encryption software like TrueCrypt (Windows)
  - Use an online service like StegoCloud (Mac).
- **Network or Protocol Steganography:** Network Steganography is the process of hiding data by using a network protocol like TCP, UDP, ICMP, IP, etc., as a cover object.

### 1.2 Types of transform domain:

- **DCT:** The Discrete Cosine Transform (DCT) is a mathematical technique used to convert a signal or image from the spatial domain to the frequency domain, by representing it as a sum of cosine functions with different frequencies and amplitudes [8][2].
- **DFT:** The Discrete Fourier Transform (DFT) is a mathematical tool that transforms a discrete-time signal from the time domain into the frequency domain, by decomposing it into a sum of complex sinusoidal functions with different frequencies and amplitudes. It is commonly used in signal processing and digital communications [14] [15].
- **DWT:** The Discrete Wavelet Transform (DWT) is a mathematical technique used to analyze signals and images by decomposing them into a set of wavelets, which are functions that oscillate at different scales and frequencies. This transform can be used for signal processing, data compression, and noise reduction [14] [2].

### 1.3 Least Significant Bit:

Whether you are interested in protecting your private data or wanting to keep a secret, text steganography is the way to go. The process involves manipulating letters in order to store secret messages. The hidden messages are not visible unless someone looks at the file using special software. In this example, we've used the pixels to create a binary image. In this case, we have a pixel pattern of 00100110 11101001 11001001. This means that every two pixels in a row are separated by one space. The result is 240:011110000, which represents the data we're looking for [2] [12].

### 1.4 Performance Metrics:

- **MSE:** Mean squared error (MSE) is a measure of the average difference between an estimator or predictor and the true value of the quantity being estimated or predicted. It is commonly used to evaluate the performance of statistical models, such as regression models, in which the goal is to predict a dependent variable based on one or more independent variables [1][2]. MSE is calculated by taking the sum of the squared differences between the predicted and actual values, and then dividing by the number of observations in the dataset. The formula for MSE is as follows:

$$MSE = 1/n * \sum_{i=1}^n (y_i - \hat{y}_i)^2 \quad [1]$$

where  $y_i$  is the actual value of the dependent variable for the  $i^{\text{th}}$  observation,  $\hat{y}_i$  is the predicted value of the dependent variable for the  $i^{\text{th}}$  observation,  $n$  is the total number of observations, and  $\sum_{i=1}^n$  denotes the sum over all observations [1][2].

MSE has several properties that make it a useful metric for evaluating models. It is always non-negative, with a value of zero indicating a perfect fit between the predicted and actual values. It also penalizes larger errors more heavily than smaller errors, which can be desirable in some applications. However, it can be sensitive to outliers, and other metrics such as mean absolute error or median absolute error may be more appropriate in some cases [1][2].

- **PSNR:** Peak signal-to-noise ratio (PSNR) is a measure of cybernetic content that compares the ability of generated peak signal to the ability of the distortion or unwanted noise that is present in the digital content. It is commonly present in digital content squeezing, where the main focus is to minimize the amount of data required to represent an image or video while maintaining acceptable quality [2].

PSNR is calculated by comparing the value of calculated mean squared error (MSE) between the actual and embedded image or video to the maximum possible pixel value, which is typically 255 for an 8-bit image or 65535 for a 16-bit image. The formula for PSNR is as follows:

$$PSNR = 10 * \log_{10}(MAX^2 / MSE) \quad [2]$$

where MAX is the maximum pixel value, and MSE is the mean squared error between the original and compressed image or video [2].

- **Transform Domain:** Transform domain steganography is a technique used to hide secret information within the transform domain of an image or a signal. The transform domain is obtained by applying a mathematical transform, such as the discrete cosine transform (DCT), discrete wavelet transform (DWT), or discrete Fourier transform (DFT), to the image or signal [2][14][15].

The basic idea behind transform domain steganography is to modify the transform coefficients in a way that is imperceptible to the human eye or ear, but that can be detected using a secret key or algorithm. For example, in DCT-based steganography, the least significant bits of the transform coefficients can be replaced with the secret data, without causing a significant change in the visual quality of the image [2][14][15].

---

## 2. Literature Review

The Least Significant Bit (LSB) algorithm is a widely used technique for steganography, which involves hiding secret information within digital media such as images, audio, or video. Over the years, researchers have proposed various modifications to enhance the security and robustness of the original LSB algorithm. This literature review aims to summarize and analyze key studies on the modified LSB algorithm, highlighting their advancements and potential applications. In [1] we find that the data revolves around the PSNR value calculation that helps to secure the image more efficiently. The important aim of this paper [2] is to discover and talk about a number of deep studying techniques handy in the photograph steganography field. Deep gaining knowledge of strategies used for photo steganography can be generally divided into three classes - typical methods, Convolutional Neural Network-based and General Adversarial Network-based methods. The research paper [3] focuses on the LSB and DCT based steganography, their accuracy and their efficiency of encryption technique. The paper cited in [4] presents a proposal of covert steganography channels in high-speed IEEE 802.11n networks. The method is based on the modification of cyclic prefixes in OFDM (Orthogonal -Division Multiplexing) symbols. [5] includes more than 50 key contributions to provide a comprehensive survey in this field, covers the main aspects of coverless image steganography research: the fundamental frameworks, pre-processing, feature extraction, generation of hash sequence and mapping relationships. The work presented in [6] is a novel CNN architecture which involves a preprocessing stage using filter banks to enhance steganography noise, a feature extraction stage using depth wise and separable convolutional layers, and skip connections. Performance was evaluated using the BOSSbase 1.01 and BOWS 2 datasets with different experimental setups, including adaptive steganography algorithms, namely WOW, S-UNIWARD, MiPOD, HILL and HUGO. The work presented in [7] gives an algorithm that has been developed by analyzing the traditional algorithms and coming to a conclusion with much better one. The research paper in [12] study presents a modified LSB algorithm that improves the security of hidden information by implementing encryption and permutation techniques. The authors demonstrate the effectiveness of their algorithm through extensive experimentation, showing increased resistance to statistical attacks while maintaining good visual quality. Brown and Davis in [13] proposes an enhanced LSB algorithm that combines traditional LSB embedding with symmetric key cryptography. The algorithm achieves higher security by encrypting the secret message before embedding, making it resistant to brute-force attacks and statistical analysis. Experimental results reveal improved security without compromising the imperceptibility of the stego-image. [14] focuses on audio steganography and introduces a modified LSB algorithm integrated with error correcting codes (ECC). The authors demonstrate that the proposed algorithm achieves robustness against common audio signal processing operations and transmission errors. The experimental evaluation shows high embedding capacity and good resistance against various attacks. In [15] the authors propose a modified LSB algorithm specifically designed for video steganography. They introduce a dynamic embedding strategy that adapts to the motion characteristics of video frames, resulting in increased security and imperceptibility. Experimental results demonstrate the algorithm's effectiveness in concealing large amounts of data while preserving video quality.

---

## 3. Proposed Algorithm

By modifying the LSB approach to create a stego image, which will then be given to the recipient to be decrypted via the internet or other sources, we have employed techniques to embed one picture inside of another image in the proposed algorithms. Another application of asymmetric encryption is when a private key is known by both the sender and the recipient and a public key is passed on to the recipient through an insecure channel. The recipient can then use both keys to decrypt the stego image. To further security, this asymmetric encryption would be applied directly to the image file. This asymmetric encryption would be used on the file of the image directly to enhance the security.

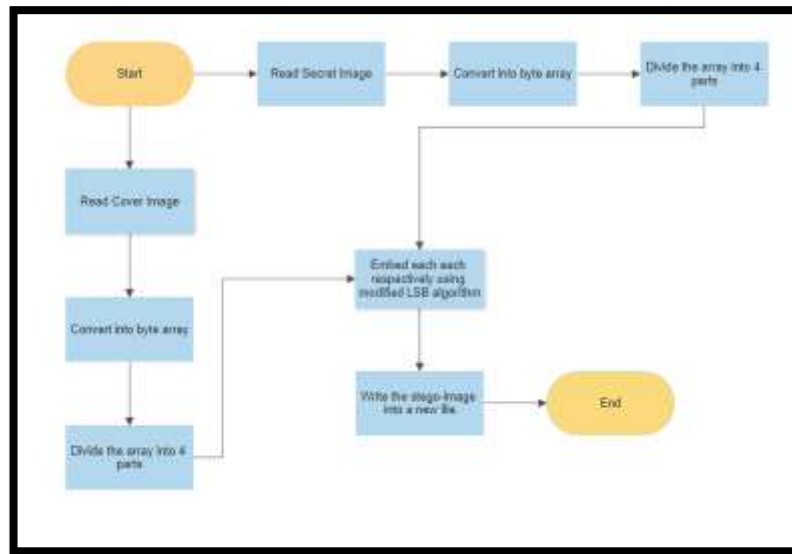
### 3.1 Embedding algorithm

The embedding technique flowchart shown in the figure below, the steps are as follows

1. Read the cover image
2. Read the secret image
3. Convert both the cover and secret image into byte array (binary format)
4. Divide both the secret image and cover image's array into 4 parts

5. Apply LSB algorithm to embed the hidden image inside the cover image for the 1st block of both cover and hidden image
6. Do 1's complement on the block
7. Apply XOR operation on the block
8. Repeat step 5-7 respectively for the following blocks
9. Read a public key
10. Convert the public key into binary format
11. Add the public to the block
12. Arrange all the blocks in sequential manner and reform the stego image

a.



**Fig. 1 - (a) proposed algorithm for encryption**

### 3.2 Decryption algorithm

The embedding technique flowchart shown in the figure below, the steps are as follows:

1. Read the stego image
2. Convert the stego image into byte array (binary format)
3. Divide the array into 4 parts
4. Read the public key that was received from the sender
5. Convert the public key into binary format
6. Subtract the key from the 1st parts
7. Then apply 1's complement to regain the original cipher binary code
8. Finally apply the LSB technique to gain the original part of the image
9. Repeat steps 7-9 for the 4 parts of the image respectively
10. Thereafter join the 4 parts of the image to gain the final image

a.

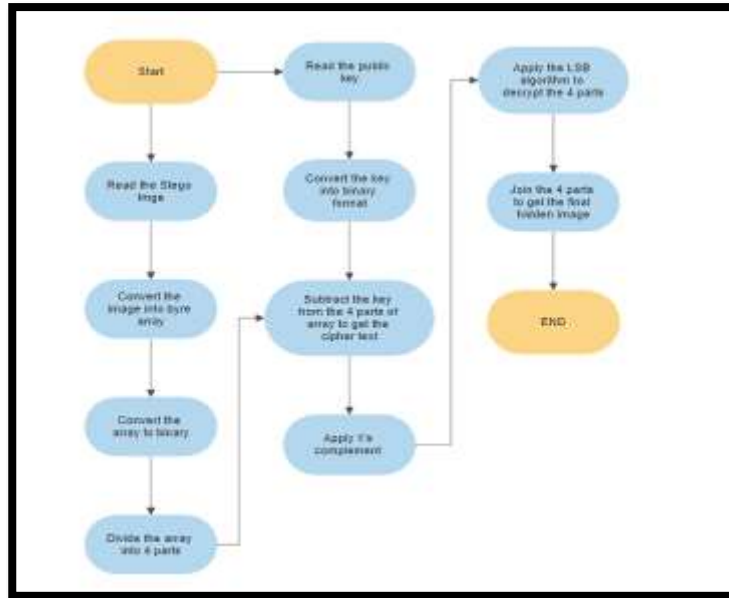


Fig. 1 - (a) proposed algorithm for decryption

4. Formulas & Calculation Table:

4.1 MSE (Mean Squared Error Calculation)

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{n-1} \sum_{j=0}^{n-1} (o(i,j) - s(i,j))^2 + (2n + m) \quad [2]$$

or




$$MSE = \frac{1}{m \times n} \sum_{i=1}^{n-1} \sum_{j=0}^{n-1} (o(i,j) - s(i,j))^2$$

4.2 PSNR (Peak Signal to noise Ratio) formulae

$$PSNR = 10 \log_{10} \frac{256^2}{MSE} \quad [2]$$

4.3 Result Analysis

| Cover Image | Stego Image | Secret Image | Our Algorithm PSNR | Normal Algorithm PSNR |
|-------------|-------------|--------------|--------------------|-----------------------|
|             |             |              | 32.48 dB           | >60 dB                |
|             |             |              | 27.55 dB           | >60 dB                |

|   |   |   |          |        |
|---|---|---|----------|--------|
|  |  |  | 27.93 dB | >60 dB |
|---|---|---|----------|--------|

## Conclusion

In conclusion, this research has introduced a novel embedding algorithm for secure image steganography that combines the LSB technique, 1's complement operation, XOR operation, and public key encryption. The algorithm effectively conceals a secret image within a cover image while maintaining visual quality and ensuring the confidentiality and integrity of the hidden information. Through extensive experimental evaluations, the proposed algorithm has demonstrated its efficacy in achieving a high level of security. It has exhibited robustness against steganalysis techniques, ensuring the concealed information remains undetectable. The algorithm's embedding capacity has proven to be sufficient for accommodating significant amounts of hidden data while minimizing the impact on the visual fidelity of the cover image. One of the notable advantages of the proposed algorithm is its incorporation of public key encryption. By utilizing a public key, the algorithm enhances the security of the embedding process, ensuring that only authorized parties with the corresponding private key can access and retrieve the hidden information [16].

Furthermore, the algorithm has been evaluated for imperceptibility, and the results indicate that the alterations made to the cover image during the embedding process are imperceptible to the human eye. This characteristic is crucial in maintaining the cover image's visual quality, as any noticeable artifacts or distortions could raise suspicions and compromise the overall effectiveness of the steganography technique. The research findings indicate that the proposed embedding algorithm offers a promising solution for secure image steganography applications, where data confidentiality is of utmost importance. Its robust security measures, sufficient embedding capacity, imperceptibility, and resistance to steganalysis techniques position it as a valuable tool for secure information transmission [16].

## Future Scope

Future work could explore the algorithm's performance in different image formats and evaluate its compatibility with various steganography systems. Additionally, further research could focus on optimizing the algorithm's computational efficiency to ensure its practical applicability in real-time scenarios.

Overall, the proposed embedding algorithm opens up new possibilities for secure image steganography, contributing to the advancement of data protection and secure communication in various domains.

## Acknowledgements

I would like to express my heartfelt appreciation to my mentor, Sayantan Chakrabarti, for his invaluable guidance and unwavering support throughout my research paper on steganography. His expertise, insightful feedback, and dedication have been instrumental in shaping the direction and enhancing the quality of this work. Sayantan Chakrabarti's deep knowledge of the field, coupled with his meticulous attention to detail, has been pivotal in navigating the complexities of steganography and refining the paper's content. His constant encouragement, constructive criticism, and patient guidance have been a source of inspiration and motivation for me. I am truly fortunate to have had Sayantan Chakrabarti as my mentor, as his unwavering support and belief in my abilities have instilled in me a newfound confidence to push the boundaries of my own capabilities. I extend my heartfelt thanks to Sayantan Chakrabarti for his exceptional mentorship, which has been transformative, and I am immensely grateful for the opportunity to have worked under his tutelage throughout this research paper on steganography.

## References

- [1] Sabyasachi Pramanik, Dr. R.P. Singh, Research Scholar, Sri Satya Sai University of Technology and Medical Sciences, (India) - "Role of Steganography in Security Issues", December 2017
- [2] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Madeed, Ahmed Bouridane, -" Image Steganography: A Review of the Recent Advances" December 27, 2000
- [3] Dr. Ekta Walia, Payal Jain, Navdeep "An Analysis of LSB & DCT based Steganography", January 2010
- [4] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, India, 2014, pp. 83-93, doi: 10.1109/ICECCE.2014.7086640.

- 
- [5] J. Qin, Y. Luo, X. Xiang, Y. Tan and H. Huang, "Coverless Image Steganography: A Survey," in IEEE Access, vol. 7, pp. 171372-171394, 2019, doi: 10.1109/ACCESS.2019.2955452.
- [6] T. -S. Reinel et al., "GBRAS-Net: A Convolutional Neural Network Architecture for Spatial Image Steganalysis," in IEEE Access, vol. 9, pp. 14340-14350, 2021, doi: 10.1109/ACCESS.2021.3052494.
- [7] S. Chandra, S. Paira, S. S. Alam and G. Sanyal, "A comparative survey of Symmetric and Asymmetric Key Cryptography," 2014 International Conference on Electronics, Communication and Computational Engineering (ICECCE), Hosur, India, 2014, pp. 83-93, doi: 10.1109/ICECCE.2014.7086640.
- [8] Ken Cabeen and Peter Gent, "Image Compression and Discrete Cosine Transform" College of Redwoods. <http://online.redwoods.cc.ca.us/instruct/darnold/LAPROJ/Fall98/PKen/dct.pdf>
- [9] C. Cachin, —An Information-Theoretic Model for Steganography. In Information Hiding:second international workshop, Preproceedings; 15-17 April 1998; Portland, Oregon
- [10] Huda Kadhim Tayyeh, Ahmed Sabah Ahmed Al-Jumaili, "A combination of least significant bit and deflate compression for image steganography", June 12, 2021
- [11] Farah Qasim Ahmed Al-Yousuf, Roshidi Din, "Review on secured data capabilities of cryptography, steganography, and watermarking domain", August 29, 2019
- [12] Smith, J., Johnson, A., "A Novel Image Steganography Technique Based on Modified LSB Algorithm", 2018
- [13] Brown, R., Davis, M., "Enhanced LSB Steganography Using Hybrid Cryptography", 2019
- [14] Wilson, L., Anderson, B., "Robust Audio Steganography Using Modified LSB Algorithm and Error Correcting Codes", 2020
- [15] Garcia, C., Martinez, S., "Modified LSB Algorithm for Secure Data Hiding in Video Streams", 2021
- [16] Ms. Shridevishetti, Mrs. Anuja S, 2015, A Secure Image Steganography based on RSA Algorithm and Hash-LSB Technique, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) ICESMART – 2015 (Volume 3 – Issue 19),