IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DEVELOPING AN ALGORITHM FOR DATA SECURITY USING STEGANOGRAPHY

[1]Deepika H, [1]G C Chandana, [1]Rakshitha A,[1]Varshitha J,[2]Prof. (Dr.) Ravi J

[1] Student, Department of Electronics and Communication Engineering, Global Academy of Technology,
[2] Professor, Department of Electronics and Communication Engineering, Global Academy of Technology,
Bangalore, India

Abstract: In the field of digital communication, the security of information is crucial that must be taken into consideration. Image steganography is defined as hiding any data inside an image. The proposed technique provides a comprehensive review of LSB-Based image steganography. There are many techniques in steganography used to conceal the information, Least Significant method (LSB) is one such technique which is used to hide data. The LSB technique involves embedding information within the least significant bit of the pixels of an image, making it difficult for the human eyes to detect the hidden information. The proposed method improves the embedding efficiency and reduces the visual distortion of the stego image and the proposed algorithm is applied in various applications that require secure communication of confidential information.

Index Terms **- Steganography, Cover Image, Secret Image, LSB method, Stego-Key, PSNR and MSE.**

I.INTRODUCTION

In the modern world, the internet has made transmission of data quick and easy but secured transmission of data is still important to protect it from hackers, theft, corruption or unauthorized access. There are various methods employed to conceal information within any medium, and one notable technique is steganography. Steganography is the art and science of hiding information within other data or media, such as text, images, audio or video, in a way that is undetectable to human senses. The word "steganography" it is derived from the Greek word "steganos" meaning "covered or concealed" and "graphein" meaning "writing". The main objective of the steganography is that the secret information or data must not be visible to human eyes unless a stego key is given to the receiver to extract the secret message [1]. Steganography encompasses different forms, including Text Steganography, Image Steganography, Video Steganography and Network Steganography.

Image steganography is defined as image embedded in an image. This method is divided based on context into two groups: those in spatial domain and Transform domain. LSB method comes under spatial domain. This approach replaces some LSB's of the cover image with the data bits of the hidden image. The altered image is called as stego image, altered image does not change the quality of image thus it is difficult for human eye to notice that there is an image inside the real image. A stego image is sent to the receiver by some media, this media will not be able to view a hidden image, only an initial image can be viewed. In order to decipher a hidden or concealed image, the receiver will be provided with an encryption key. [2].

The application of the proposed technique are, it can be used by intelligent agencies for communication, bank note printing, to prevent color copiers from reproducing images of currency as fake notes [3].

But this method has its limitations, like the amount of information that may be contained in an image is restricted because it's large; and if you replace a lot of bits they can distort the quality of the image. As steganography is simply a way to hide messages and does not provide any encryption or security against interception, it should be stressed that this method of safety communication is not completely reliable [4].

II.LITERATURE SURVEY

Nandhini Subramanian, Somaya Al-Maadeed, et al., [1] The main goal is to examine and analyse various deep learning algorithms that are accessible for image steganography. The three main types of deep learning techniques used in image scanning are traditional approaches, Convolutional Neural Network based methods and General Adversarial Networks Based Methods. In addition to the technique, a detailed explanation is given of the data used, the experimental setup investigated, and generally used evaluation measures.

Mohammed A. Saleh [2] Since the growing use of the internet and multimedia has increased the interest in image steganography in order to secure and protect them, there is a significant interest in security approaches that aim to protect information and digital data. In order to assess and investigate picture steganography methods, algorithms, and schemes, a comprehensive literature review is done.

Pratap Chandra Mandal and Imon Mukherjee [3] The main challenge in proposing a steganographic technique is to strike a suitable balance between higher embedding capacity, imperceptibility, and security that distinguishes it from correlated systems such as cryptography and watermarking also provides a comprehensive state-of-theart review and analysis of some recent steganographic techniques.

Kavitha A. B and P. Anbalagan [4] The authors of this paper evaluate the proposed algorithm and examine various LSB steganography methods used for secure data transmission. They examine the applicability and limitations of this technique, comparing it to comparable techniques according to a variety of parameters.

Inas Jawad Kadhim, Prashan Premaratne, et al., [5] This is a detailed description of the different LSB Based steganographic techniques applied for secure data transmission. The author will examine the different methods in terms of their ability, robustness and security. Different performance evaluation indicators and future research directions are also discussed.

Kurnia Anggriani and Nan-I Wu [6] The purpose of the study is to summarise and analyse the benefits and challenges of existing techniques, in order to examine how coverless image scanning has developed over the past five years. Furthermore, the results of experiments shall be presented in charts and graphs so that they provide an accurate performance comparison. This is done to outline future research requirements and opportunities in the Coverless Image Steganography research topic.

Nasro Min-Allah and Naya Nagy, et al., [7] The quantum steganography is essential to the inclusion of classified data in carrier messages based on quantum computing techniques. An overview of recent progress in the field of quantum steganography and image tracking systems, a discussion of algorithm improvement which has been carried out in these areas, an explanation ofmethodologies applied with respect to each presented system as well as a Comparative Study of current schemes is provided.

Liao Z and Wang J [8] A survey has been presented of image steganography based on LSB, comprising the fundamental concepts, benefits and disadvantages linked to LSB techniques as well as some more common methods.

Wang H and Zhang Z [9] It examines in detail the numerous methods of LSB based image steganography, including its advantages and shortcomings, as well as discusses problems and future research objectives for this area.

Mohammed Mahdi Hashim [10] The different indications of the evaluation factors, which have been derived from image scanning algorithms, are explained by the proposal method. Three main parameters are considered to be the effectiveness of the steganographic process, namely the capacity of the cargo, the quality of the image and the security measures, which are mainly focused on imitative steganographic processes, which are most popular in steganographic branches. In general, the most efficient way to insert a secret message is to use the least important bit. Moreover, the information on a least important bit of LSB as part of different image formats is more detailed in this paper.

Youmin Xu and Chong Mou [11] The model designs a conditional flow-based frame-work, dubbed as Robust Invertible Image Steganography (RIIS), to alleviate the distortion influence and improve robustness. This is consistent with a module on enhancement and optimization strategy to handle irreversible processes such as channel reductions and quantization because flow models are bijective.

Ritu Sindhu and Pragati Singh [12] It is primarily designed to provide an overview of the steganography process, its necessity, advantages and techniques; identify which steganographic processes are more useful and what needs they fulfil in order to determine which applications will have a greater degree of compatibility with steganographs.

Gupta A and Kumar A [13] Present a survey of LSBbased image steganography techniques, including a detailed description of the LSB algorithm and its applications in steganography, along with a comparison of several state-of-the-art LSB-based methods.

S. Sravani and R. Raniith [14] The primary purpose is to employ an LSB algorithm for steganography. It involves placing a cryptic image on the cover and uploading it to the Internet. This approach may be used with any type of multimedia, including text, photos, audio files, and videos. Steganography is used in cover images to disguise the location of a region (for example, in the form of a map) and transfer the image over the internet. The efficacy of this method in security-related applications has been tested using MSE and PSNR values.

P. T. Sivagurunathan and M. Archana, et al., [15] To disguise electronic messages, the purpose of this is to apply modern steganography techniques. The text is stored and inserted into the cover image by means of a proposed assignment algorithm. This method will give a better level of security and robustness compared with the old systems, which have good embeddedness. This proposed system will improve PSNR values and MSEs, as well as analyse load capacity.

III.METHODOLOGY

The proposed block diagram for secured communication is shown in Figure 1:

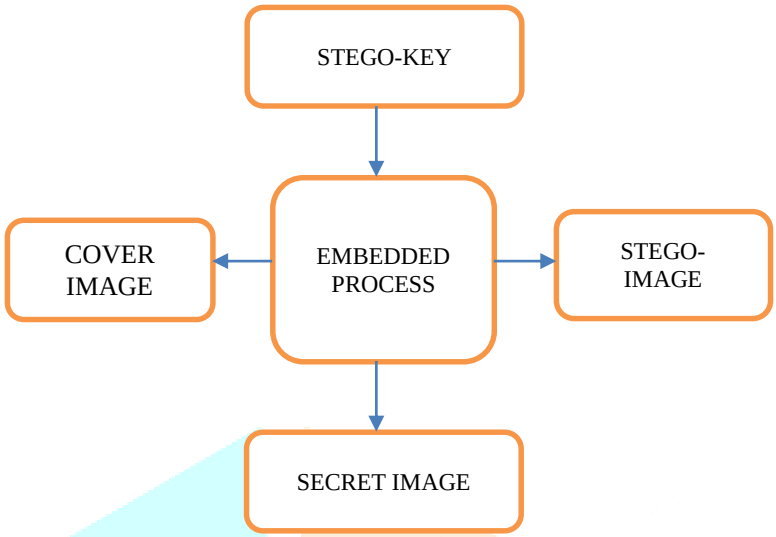

FIGURE 1: BLOCK DIAGRAM OF STEGANOGRAPHY

LSB ALGORITHM TO EMBED THE IMAGE:

1.Read the carrier image and display it.
2.Read the secret image and display it.
3.Resize the secret image to match the dimensions of the carrier image.
4.Perform LSB substitution to embed the secret image into the carrier image:

- Extract the RGB channels of the carrier and secret images.
- For each pixel in the images, preserve the MSB of the carrier image and replace the LSB with the MSB of the secret image.
- Combine the modified channels to create the steganographic image.

5. Display the steganographic image.
6. Calculate the Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) between the original and steganographic images.
7. Display the MSE and PSNR values.

Cover image: To stow away a hidden image or information, image steganography's cover image must be the first image. In order to be able to insert a message which cannot be seen, it has been chosen for its redundancy and complexity. To insert a hidden message, the image of your cover is modified to create a steganographic image and you can share it with an intent recipient.

Secret image: The image or message contained beneath the cover image, often known as a secret image. The hidden image is often smaller in size and lower in quality than the cover image since it must be compressed and concealed within the cover image without changing the overall appearance of the cover image.

Stego key: In steganography, it refers to a secret key or password used to embed a message into a cover medium. The stego key is often used to manage the embedding process and specify where the message will be concealed within the cover medium. It is also utilised to retrieve the concealed message from the cover medium.

Embedding process: In steganography involves hiding a message within a cover medium such as an image, audio file, or video. The process involves selecting a portion of the cover medium and modifying it to embed the secret message. The goal of the embedding process is to make the modifications to the cover medium imperceptible to the human eye or ear while preserving the quality of the cover medium.

PSNR and MSE: PSNR (Peak Signal-to-Noise Ratio) and MSE (Mean Squared Error) are two often used measures for assessing image or video compression quality. The average squared difference of a picture from the initial to the compress image shall be measured by MSE. The difference between each pixel in the original and the compressed image shall be calculated to square it and sum up all the differences:

MSE = mean ((Cover_image(:) – Stego_image(:)).^2)

PSNR is a measurement employed in image steganography to assess the image quality by comparing the maximum signal strength with the noise introduced during embedding, with higher values indicating minimal distortion. It is logarithmic measure of the ratio of the maximum possible pixel value to the MSE:

PSNR = 10log10(R2 / MSE)

In general, higher PSNR and lower MSE values indicate better quality of the compressed image.

IV.RESULTS AND DISCUSSION

Figure A: Cover Image

Figure B: Secret Image

Figure C: Steganographic Image

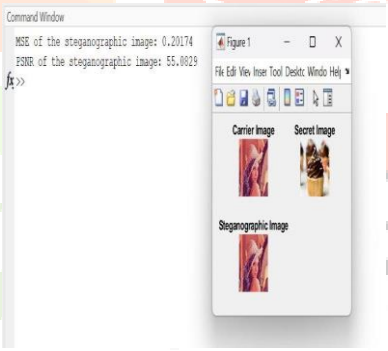

Figure D: PSNR and MSE

Figure A illustrates the cover image of size 255x255, Figure B gives the secret image of size 255x255 and Figure C shows the stego image in which secret image is embedded inside it. Figure D provides the calculation of PSNR and MSE for stego Image.

This technique is found to be very effective as no data loss occurs in encryption. Hence, the proposed method provides the security to greatest level.

Cover Image	Dimension	Secret Image	Dimension	MSE	PSNR
Cat.jpg	590x1280	Tree.jpg	590x1280	0.45927	51.5102
Monalisa.jpg	255x255	Chimpazee.jpg	255x255	0.37321	52.4113
Girl.jpg	255x255	Girl2.jpg	255x255	0.31748	53.1136
Forest.jpg	436x266	Swing.jpg	436x266	0.24248	54.2841
Tiger.jpg	255x255	Lion.jpg	255x255	0.21489	54.8086
Lenna.jpg	255x255	Cake.jpg	255x255	0.20174	55.0829

TABLE 1: THESIS

Table 1 displays the calculation of PNSR and MSE for different stego images. Both PSNR and MSE can be used to assess the stego picture's quality in LSB steganography. The PSNR and MSE will reflect the fact that the stego image differs from the original image because LSB steganography modifies the least significant bit of each pixel. The stego image is closer to theoriginal image in quality and has a higher level of security in terms of the message being undetected to unauthorised users, as indicated by a higher PSNR and a lower MSE.

V. CONCLUSION

The Image Steganography is a technique used in sending secret information by hiding inside a cover image. Least Significant Bit technique are widely used in every field of security. In the proposed method, demonstrates Least Significant Bit technique to measure the two parameters such as Peak Signal Noise Ratio [PSNR] and Mean Square Error [MSE]. The PSNR is 55.0829 dB and MSE is 0.20174 for Lenna.jpg image, as cover image has good quality and high resolution. Therefore, the PSNR of the stego image is high and MSE is low.

VI. ACKNOWLEDGMENT

We express our sincere gratitude to Global Academy of Technology, Bangalore, and as well as our guide Dr. Ravi J, for granting us the opportunity to conduct this project.

REFERENCES

[1] Nandhini Subramanian, Somaya Al-Maadeed, Omar Elharrouss, Ahmed Bouridane, "Image Steganography: A Review of the Recent Advances," in IEEE Access, vol. 9, pp. 23409- 23423, 2021.

[2] Mohammed A. Saleh, "Image Steganography Techniques - A Review Paper", in International Journal of Advanced Research in Computer and Communication Engineering, vol. 7, 2019.

[3] Pratap Chandra Mandal and Imon Mukherjee, "Digital image steganography: A literature survey,in Information Sciences, vol. 609, pp. 1451-1488, 2022.

[4] Kavitha A B and Anbalagan P, "A Survey of LSB-based Image Steganography Techniques for Secure Data Transmission" in IEEE International Conference on Computational Intelligence and Computing Research, pp. 1-6, 2021.

[5] Inas Jawad Kadhim, Prashan Premaratne,Peter James Vial, and Brendan Halloran, "A Comprehensive Survey of Least Significant Bit (LSB) Based Steganography Techniques" in 4th International Conference on Computational Systems and Information Technology for Sustainable Solutions, pp. 148-153, 2021.

[6] Kurnia Anggriani and Nan-I Wu "Research on Coverless Image Steganography", in International Journal of Network Security, vol. 25, pp. 25-31, 2023.

[7] Nasro Min-Allah, Naya Nagy, Malak Aljabri, Mariam Alqahtani and Razan Sabri, "Quantum Image Steganography Schemes for Data Hiding: A Survey", in Applied Science, vol. 12, pp. 10294,2022.

[8] Liao Z, & Wang J, "A Survey on Least Significant Bit (LSB) Steganography in Images" IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference, pp. 296-301, 2021.

[9] Wang H, & Zhang Z, "A review of least significant bit-based image steganography techniques" in Journal of Ambient Intelligence and Humanized Computing, vol. 12(8), pp. 8999-9016,2021.

[10] Mohammed Mahdi Hashim "Performance evaluation measurement of image steganography techniques with analysis of LSB based on variation image formats", vol. 7, 2018.

[11] Youmin Xu, Chong Mou, "Robust Invertible Image Steganography", in IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp. 7865-7874, 2022.

[12] Ritu Sindhu and Pragati Singh, "Information Hiding using Steganography" in International Journal of Engineering and Advanced Technology, vol. 9, 2020.

[13] Gupta A & Kumar A, "Survey of Least Significant Bit (LSB) Based Image Steganography Techniques" in 3rd International Conference on Electronics and Sustainable Communication Systems, pp. 19-22, 2021.

[14] S. Sravani and R. Raniith, "Image Steganography for Confidential Data Communication," in 12th International Conference on Computing Communication and Networking Technologies, pp. 01-05, 2021.

[15] P. T. Sivagurunathan, M. Archana, N Durga Shree and G Yuvashrie, "Image Steganography for Confidential Communication and Secured Data Storing", in Advances in Intelligent Systems and Computing, vol. 1428, pp. 315–324,2022.