



A Comprehensive Study on LSB based Steganography

Pankaj Nandan^{*1}, Dr. Raghav Mehra^{#2}, Dr. Amit Kumar Chaturvedi^{#3}

*^{*1}Ph.D. Scholar, Deptt. of Computer Science, Bhagwant Univ., Ajmer, Rajasthan*

^{#2}Associate Prof, CS Deptt., Bhagwant Univ., Ajmer, Rajasthan

^{#3}Assistant Prof, MCA Deptt., Engineering College, Ajmer, Rajasthan

Abstract: Steganography is not a new term for the people who are working in the field of computer or communication industry. At present the steganography technology widely used in the communication industry for sending and receiving secret messages and important documents. The application of LSB techniques in steganography improved its efficiency and effectiveness. The technology provides many solution for improving the payload capacity of the cover file. In this paper, we are going to present a comprehensive study on LSB based steganography and we have also going to compare the two image formats JPG and PNG in such a way which will be better cover image in case of Image based steganography.

Keywords: LSB, security, encryption, steganography, secret message, Information exchange.

1. Introduction: Communication in a confidential manner is the requirement from the past to till now in every society, administration, or business because all the information cannot be discussed or exchanged in a transparent manner. Variety of methods are used and proposed for making communication successful and fulfill the interest of the people. There are two popular techniques for confidential communication Cryptography and Steganography. There are many proposals for confidential communication which uses both Cryptography and Steganography in a strategically manner. The rapid growth and development in the field of communication had brought the world closer and number of subscriptions for 4G continues to growing by 41 million during the Q3 2022 to reach around 5 billion. 4G subscriptions are projected to peak at 5.2 billion by the end of 5.2 billion by the end of 2022. 5G subscriptions grew by 110 million during the third quarter to around 870 million and that number is expected to reach 1 billion by the end of 2022. By the end of 2028. 5 billion 5G subscriptions are forecast globally. This exponential growth of communication requirement clearly shows that need of communication and confidential communication is the utmost requirement of the world.

The purpose of steganography is to conceal and deceive the secret message. It is a form of covert communication and can involve the use of any medium to hide messages. It's not a form of cryptography, because it doesn't involve scrambling data or using a key. Instead, it is a form of data hiding and can be executed in clever ways. Steganography is an additional step that can be used in conjunction with encryption in order **to conceal or protect data**. Steganography is a means of concealing secret information within (or even on top of) an otherwise mundane, non-secret document or other media to avoid detection. All steganography detection programs today are essentially proof-of-concept, and their logic cannot be implemented in commercial security tools because they are slow, have fairly low detection rates, and sometimes even contain errors.

Steganography is the practice of hiding information inside something that appears normal and is not secret. **Cybercriminals use steganography to hide stolen data or malicious code in images, audio files and other media. Steganography has a critical advantage over cryptography:** In cryptography, you know the secret message is there, only its content is concealed; in steganography, the existence of the secret message is often difficult to notice. Stenography is **primarily used in legal proceedings, during court reporting.**

However, stenographers also work in other fields, including live television closed captioning, forums for deaf and hard-of-hearing audiences, as well as making the record for governmental agency proceedings. The major disadvantage of steganography is that, unlike cryptography, **it needed a lot of overhead to hide associatively few bits of information**. Because the steganographic system is found, it is rendered useless. However, it fares no worse than cryptography and is still the preferred medium.

Depending on the nature of the cover object (actual object in which secret data is embedded), steganography can be divided into five types:

- Text Steganography.
- Image Steganography.
- Video Steganography.
- Audio Steganography.
- Network Steganography.

2. **Related work:** communication industry is growing and evolving as a major industry in the world and almost all the other industries are relying on the communication industry. Major business stakeholders are leading in the world by efficiently using the communication technologies. Confidential communication is the utmost requirement of almost all the governance and industries in the world. Various researchers have given useful innovative proposals for using steganography and encryption for confidential communication. Some of them are discussed here.

Some LSB of the cover image are inverted depending on the secret data for embedding instead of replacing LSB with the secret data. First, the maximum and minimum values in the secret data are determined then subtract all values of the secret data from this maximum value. Finally, make a division for the results and embed the new results into the cover image to obtain the stego image. The results show that the proposed method gives high capacity and good imperceptibility in comparison with the previous methods. The cover image is partitioned into two equal parts and the difference between the maximum and minimum value of secret data determines if we use four LSBs or five LSBs of each pixel in the first part for embedding. Also, this difference determines which two cases will be applied to the inverted bits to invert again. Standard grayscale images are used to evaluate the performance of the proposed technique. Experimental results indicate that the present method increases the embedding capacity and enhances the quality of the stego image. In further research, besides the merits obtained in this paper, increasing the robustness property will be taken into consideration [1].

Least Significant Bit (LSB) is a common and popular technique for steganographic images, especially when the spatial domain of an image is considered. Because of its high quality of stego-image produced, this method is currently widely used and continues to be developed to date. The limitations of the LSB method are its simplicity and high predictability of inside secrets, so researchers try to improve the security of hidden messages in this way. This study proposes two layers of encryption and hiding stages. Here, first the message is encrypted by using a Secret key (extract from MSB) and double XOR operations using binary representation, and then an encrypted stream of bits is hidden into the cover image using the LSB technique. To ensure the quality of our proposed method, a well-known evaluation measure, such as MSE, PSNR, Entropy and histogram distribution, was calculated [2].

This proposal will conceal information into an image by using three methods that concentrate on the compression of the data before hiding it into the image and then compare the results using Peak Signal to Noise Ratio (PSNR). The three methods that will be used are Least Significant Bit (LSB), Huffman Code, and Arithmetic Coding and then the result will be compared [3]. Seven steganography methods were implemented. The methods were chosen for their different strengths in terms of resistance to different types of steganalysis or their ability to maximise the size of the message they could store. All of the methods used were based on the manipulation of the least significant bits of pixel values or the rearrangement of colours to create least significant bit or parity bit patterns, which correspond to the message being hidden [4].

Various Steganography algorithms have been proposed and implemented for hiding the existence of data in a cover object starting from the algorithms that work in transform domain to the ones that work in spatial domain, such as Least Significant Bit (LSB), which uses the three colours (RED, GREEN and BLUE) present in an

image. Three colours are present in the pixel of an image, therefore, this project proposed a new algorithm that chooses only the two colours (GREEN and BLUE) out of the three colours (RED, GREEN and BLUE) that made up of a pixel present in an image to hide data. This proposed algorithm successfully hides the data with the two colours (GREEN and BLUE) present in an image with no significant changes in the resulting colours of the image. The result of this experiment has shown the effectiveness of the proposed algorithm. This experimental result has shown that the algorithm strikes a balance between the security and the quality of the image. It should be noted that this research work only considers image as the cover object, other forms of cover object are not considered here. It should also be noted that the algorithm only hides data from 8 bytes to 1024 bytes using two different images of different size, which shows no effect on the effectiveness of the algorithm [5].

A new method is introduced here for applying the image steganography concept for image encryption. Using the PLIP (Parameterized Logarithmic Image Processing) addition to embed the scrambled original image into a selected cover image, the new algorithm generates an encrypted image. Computer simulation and security analysis are given to show that the algorithm has a very large key space and can withstand several common attacks. In this new idea, we have introduced an image encryption algorithm called the PLIPaddEncrypt algorithm. To embed the original image into the cover image, it fuses the scrambled original image with the cover image using the PLIP addition via specific parameters. This also shows a new application of the PLIP model for image encryption. Simulation results have demonstrated the encryption performance of the PLIPaddEncrypt algorithm. The security analysis has shown that the algorithm have sufficiently large key space and can withstand several common attacks. The algorithm has the potential for applications in privacy and copyright protection [6].

Network Security for data transmission is the most vital issue in modern communication system. In this paper, we have discussed a new steganographic technique. The effectiveness of the proposed method is described through which idea of enhanced security of data can be achieved. To hide data in a binary image, no key is needed here rather this algorithm is based on the number of occurrence of 0s and 1s in data that has to hide and number of occurrence of 0s and 1s in the last bit of each pixel of binary image file. The proposed algorithm assures the security and the data hiding effect is quite invisible [7, 8]. A new Least Significant Bit (LSB) steganography technique is presented in this work by treating the secret message based on its words content instead of its characters content. By using a specific small words dictionary by the sender and the receiver of the secret message, and representing each word in the secret message with an index in the words dictionary. Then embed these words indices, of the secret message, in the LSB of the pixels in the stego-image. The experimental results shown that the Word Based LSB technique will add more security to the secret message, reduces the distortion that will occur in the stego-image, increase the capability to hide very long secret message in a small stego-image, and minimize the time that is needed to hide and extract the secret message [9, 10, 11].

3. Important findings

The two essential properties of steganography are good visual imperceptibility of the payload, which is crucial for security of hidden communication and payload is essential for conveying huge quantity of secret information. Steganography has to satisfy two requirements, one is the capability and the other is transparency. Capacity means embedding large payload into media. Transparency means an ability to prevent distinction between stego and cover image by statistical analysis.

PNG format for a LSB Steganography is a great choice. As the LSB works on spatial domain thus, it becomes very important that there is no introduction of noise or error of any sort. Under this scenario PNG is the best format due to the fact that it uses a lossless compression so the substitutions made during the whole process of LSB steganography is not lost. PNG also provides huge storing capacity and high quality image after steganography thus, avoiding detection by just looking at the image.

Table 1: Images in PNG and JPEG format for comparison





	
<p>Figure 1(a): Ship_PNG.png</p>	<p>Figure1(b) : Ship_JPEG.jpg</p>
	
<p>Figure 2(a): Nature_house.png</p>	<p>Figure 2(b): Nature_house.jpg</p>



Table 2: LSB Images in PNG and JPEG format for comparison of the main images shown in table 1

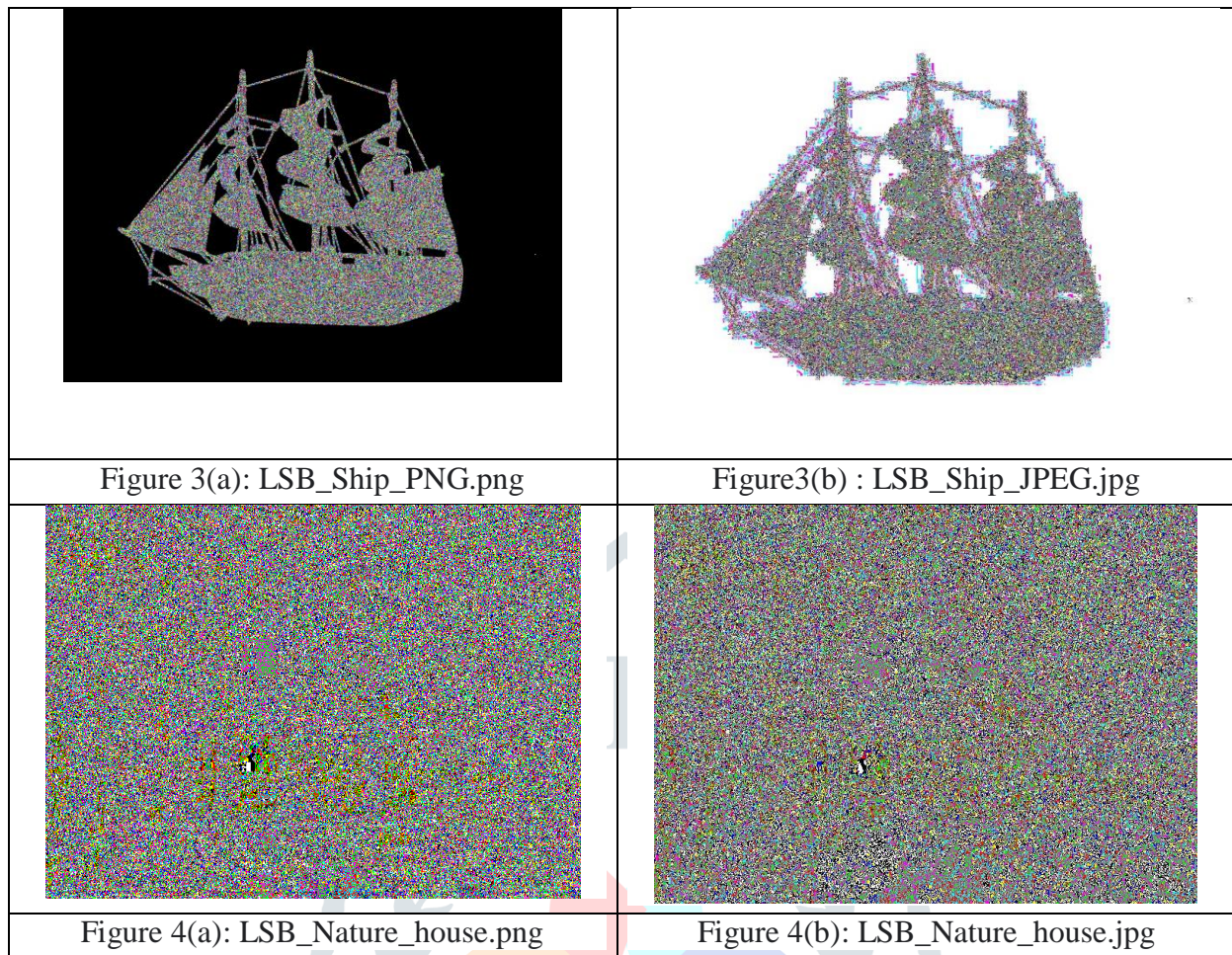


Table 3: Description of Image shown in Table 1

Name of the File	Main Image				Name of the File	LSB Bit plane of the main Image		
	Type of Image	Size KB	Dimension X*Y	Depth BPP		Type of Image	Size KB	LSB in %
Figure 1(a)	PNG	505	1024x768	24	Figure 3(a)	PNG	148	29.3%
Figure 1(b)	JPG	115	1024x728	24	Figure 3(b)	JPG	205	178.2%
Figure 2(a)	PNG	648	720x528	24	Figure 4(a)	PNG	238	36.72%
Figure 2(b)	JPG	138	720x528	24	Figure 4(b)	JPG	282	204%

4. Conclusion

It is found that Least Significant Bit (LSB) technique is the most suitable technique for secret messaging using steganography technique and it is illustrated well in the section 3 of this paper. In the section 3, four images are taken as figure 1(a), 1(b), 2(a), and 2(b) in which figure 1(a) and 2(a) are PNG images and figure 1(b) and 2(b) are JPG images. We have separated the LSB bit planes of these all four images and shown in the table 2 as Figure 3(a), 3(b), 4(a), and 4(b). Then we have analysed the sizes of these all the eight images i.e. figure 1 to 4 and shown in the table 3. It is observed that size of LSB image of PNG image is less and it is part of the png image i.e. these are drawn from the image itself, whereas in the case of JPG image the size of LSB is more than the size of the main JPG image i.e. it includes the surroundings of the image and hence increases the size of the LSB image.

Another point which is observed during this study is that after hiding the secret message in the JPG image, the size of the image increases more, which can be easily come in the notice of receivers or surveillance, whereas in case of PNG image, after hiding the secret message the size remains same, so it will not come in the notice of the unauthorized receiver or surveillance that there is any hidden message in the image cover.

In table 3, all these information are illustrated. So, it is concluded that PNG images are more safe and suitable than the PNG images for hiding secret message using LSB technique for Steganography than the JPG images. As well as the payload area in the PNG images is the part of image, whereas in case of JPG image it includes the surrounding area of image also.

References:

1. Dalia Nashat and Loay Mamdouh, "An efficient steganographic technique for hiding data", Journal of the Egyptian Mathematical Society, pp. 1-14, 2019
2. Ali Ahmed and Abdelmotalib Ahmed, "A Secure Image Steganography using LSB and Double XOR Operations", IJCSNS International Journal of Computer Science and Network Security, VOL.20 No.5, May 2020, pp. 139-144
3. Wa'el Ibrahim A. Almazaydeh, H. S. Sheshadri, "Image Steganography using LSB, LSB+Huffman Code, and LSB+Arithmetic Code", International Journal of Computer Applications (0975 – 8887), Volume 155 – No 11, December 2016, pp. 1-7
4. Kevin Curran, Karen Bailey, "An Evaluation of Image Based Steganography Methods", International Journal of Digital Evidence Fall 2003, Volume 2, Issue 2, pp. 1-40
5. O. Osunade, I. A. Ganiyu, "Enhancing the Least Significant Bit (LSB) Algorithm for Steganography", International Journal of Computer Applications (0975 – 8887), Volume 149 – No.3, September 2016, pp. 1-8
6. Yicong Zhou, Sos Aгаian, "Image Encryption Using the Image Steganography Concept and PLIP Model", Proceedings of 2011 International Conference on System Science and Engineering [ICSSE 2011], Macau, China - June 2011, ISBN : 978-1-61284-471-8, pp. 699-703
7. Debnath Bhattacharyya, Arpita Roy, Pranab Roy, and Tai-hoon Kim, "Receiver Compatible Data Hiding in Color Image", International Journal of Advanced Science and Technology, Volume 6, May, 2009, pp. 15-24.
8. Indu Nehra, Rakesh Sharma, "Review Paper On Image Based Steganography", International Journal of Scientific & Engineering Research, Volume 6, Issue 6, June-2015, pp. 1580-1583
9. Dr. Mohammed Abbas Fadhil Al-Husainy, "Word-Based LSB Image Steganography", International Journal of Advanced Research in Computer Science, Volume 2, No. 6, Nov-Dec 2011, ISSN No. 0976-5697, pp. 15-19
10. Sabyasachi Pramanik, Dr. R. P. Singh, Ramkrishna Ghosh, "new encrypted method in image steganography", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 14, No. 3, June 2019, pp. 1412~1419, ISSN: 2502-4752
11. N. Krishnaveni, Sudhakar Periyasamy, "A Novel and Innovative Approach for Image Steganography with Chaos", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 11, No. 1, July 2018, pp. 263~267, ISSN: 2502-4752
12. Iman I. Hamid, "Image Steganography Based on Discrete Wavelet Transform and Chaotic Map", International Journal of Science and Research (IJSR), ISSN (Online): 2319-7064, Volume 7 Issue 1, January 2018, pp. 588-591
13. Faten H. MohammedSediq Al-Kadei, "Two-level hiding an encrypted image", Indonesian Journal of Electrical Engineering and Computer Science, Vol. 18, No. 2, May 2020, pp. 961~969, ISSN: 2502-4752
14. Sabyasachi Pramanik, Samir Kumar Bandopadhyay, "APPLICATION OF STEGANOGRAPHY IN SYMMETRIC KEY CRYPTOGRAPHY WITH GENETIC ALGORITHM", INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY, Vol 10, No.7, ISSN 2277-3061
15. Mr.Jagadeesha.D.H, Mrs.Manjula.Y, Dr.M.Z.Kurian, "FPGA IMPLEMENTATION OF X-BOX MAPPING FOR AN IMAGE STEGANOGRAPHY TECHNIQUE", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, Vol. 2, Issue 6, June 2013, ISSN (Online): 2278 – 8875