

Review on image steganography using different LSB methods

Vijay Kumar Sharma *

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Bhanu Pratap Soni [†]

School of Electrical and Electronics Engineering

College of Engineering and Technical Vocational Education and Training

Fiji National University

Nasinu

Fiji

Neha Janu [§]

Department of Computer Science and Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

Sadaf Aziz [‡]

Department of Computer and Communication Engineering

Manipal University Jaipur

Jaipur

Rajasthan

India

* E-mail: Vijaymayankmudgal2008@gmail.com (Corresponding Author)

[†] E-mail: bhanu.soni@fnu.ac.fj

[§] E-mail: neha.janu@jaipur.manipal.edu

[‡] E-mail: sadafaziz78678600@gmail.com

Deepika Shekhawat^{*}

*Department of Computer Science and Engineering
Amity School of Engineering and Technology
Amity University Mumbai
Mumbai
Maharashtra
India*

Abstract

Steganography is originated from the words: 'stegos,' which in Greek means 'to cover or to hide,' and 'grayfia,' which means 'writing,' thus forming the concept of 'covered writing,' or 'writing which is hidden.' Steganography is the process or technique in which some confidential data or some information is concealed in reverse file or message which will be extracted from the recipient's side with the use of reverse algorithm used at the time of embedding. There are different types of steganography techniques involved, as the data can be of distinct varieties such as image, text, audio and video. Along with these steganography techniques there is also network steganography. But here, we are mainly going to discuss about LSB (i.e. Least significant bit substitution) based Image steganography methods.

Subject Classification: 94A60.

Keywords: Image steganography, LSB algorithm, Cryptography, AES cryptography, Bit flipping method.

1. Introduction

As steganography means hiding secret messages in undoubtedly ordinary files which are in plain sight [1][2][3][4][5]. In ancient times, some sort of secret inks which were mainly invisible were used to write some very crucial texts or documents to keep them safe from the hands of traitors or wrong people, now in modern days various techniques are being used like to embed hidden data in images or some scripts in Microsoft document files.

Now if we talk about who are the people who use these techniques then we will come to know that hackers, cybercriminals, and malicious attackers are the ones using steganography for the cyberattacks by embedding malicious codes or script files. But some people like spies use this technique to communicate with their high commands without coming in the light of any suspicion.

^{*} E-mail: deepikashekhawat08@gmail.com

Any medium can be used to hide messages in steganography [6]. But some people misunderstood it with cryptography, which involves the use of a 'key' to encrypt and decrypt data. It is mainly of two types –

1. Symmetric key cryptography – in this a private key which is single is used for decryption and encryption and the sender and the receiver both must know the key, but should not be sent through the channel as the hacker may obtain the access of the key and may execute some unauthorized tasks with it
2. Asymmetric key cryptography – here two different keys are used to encrypt and decrypt data, one is the private key, about which the receiver must be aware of and another one is the public key which is to be announced to the public.

The main differences between the steganography and cryptography are mentioned below in the Table 1–

Table 1
Basic difference between steganography and cryptography

Steganography	Cryptography
In this procedure, the information/ data is covertly mixed in some other file.	The information here is changed with the help of key and get converted to cipher text.
The structure of the data is not altered but concealed.	Here the structure of the data gets altered because of the secret keys.
The hidden data is not at all visible to anybody because of confidentiality issues.	The transformed data is visible to all but provided only due to integrity and non-repudiation.

As we know in Conventional, Steganography is categorized in four kinds (see in Figure 1), which are as follows [1]:

1. Image steganography: In this process secret hidden file is embedded in the image which is known as the cover image and after embedding, the image which is obtained is known as the stego image and it has the secret message or data concealed in it which can't be seen.[7] [8] [9]
2. Audio steganography: This process involves the alteration of the binary bits sequence of the audio file by hiding some message in it.[1][7]

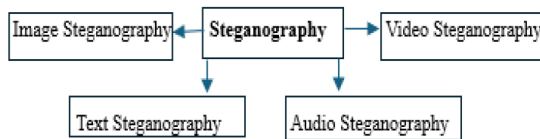


Figure 1
Steganography Types

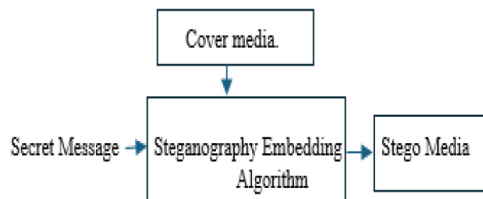


Figure 2
Steganography embedding process.

3. Video steganography: A video file is the combination of several collections of images and audio files, thus data can be hidden in these files, resulting in video steganography. [7]
4. Text steganography: When the information is hidden in text files then it is defined as text steganography.[1][7]

To get a better view about image steganography, first we need to understand “what an image is?” and “how it is formed?”. So the image is made from the building blocks called pixels, now these pixels are of three colors. The color scale is called the “RGB Encoding Scale”, as red, blue and green are the main colors and due to their combination several other colors are formed. When the bits are like 0,1,1 then it is meant that there are 0 parts of red and certainly 1 and 1 part of green and blue respectively.

2. Different Algorithms Used In Image Steganography

Figure 2 illustrate Steganography embedding process. For hiding the data several steganography techniques are used, such as –

Batch steganography – In this technique, the user hides confidential data within multiple covers or a batch of images for the security reason. [11]

Permutation steganography – As the name suggests, the data is hidden using several permutation combinations.[12]

Least significant bits (LSB) – The idea used here is changing the value of last bit of the pixel for the embedding of data in the image. [13]

Bit-plane complexity segmentation (BPCS) – Here the image is cleaved into two parts namely ‘informative region’ and ‘noise like region’ and the secret information or data is concealed in the cover image’s noise like region. Unlike the LSB algorithm, in this technique both the LSB and MSB planes are used to hide data.[14]

Chaos based spread spectrum image steganography (CSSIS) – Here the analog and binary data is transmitted through chaotic carriers. Computer simulations and performance analysis is used to examine this technique’s validity.[15]

Different techniques are involved in hiding information within each file type or medium and each technique has its own set of cons and pros and is appropriately deployed as per the requirement. In this paper after reviewing all the methodologies, we will discuss about the most popular method of hiding secret information within an image or data file using a technique called the LSB (Least Significant Bits).

In LSB Image steganography, the right most bit of the binary number is replaced in the cover image by the secret data bits of the hidden message. It is easy to compute because of its low capacity and more preferable due to the enhancement it makes in the stego image.

3. Evaluation

A. Literature Review

- 1) The first research discusses the LSB Image steganography using the bit flipping method which is used to increase the imperceptibility of the stego image. This method changes the message bit value by negating it and is done when the cover image bit changes by value greater than 50%. [16].

Table 2 shows the MSE, SSIM and PSNR of the embedded and extracted images. As the bit flipping method is done by two ways that are 1-bit pixel variant and 2-bit pixel variant, so here the results obtained are based on 1-bit pixel message image.

As there are colored images so some layers did the bit flipping and some doesn’t. Due to this phenomenon the differences in PSNRs is visible which is almost 9db.

Table 2
MSE, SSIM and PSNR of the resulting stego images [16]

Parametrics	Standard method			Discussed existing method[16]		
	Baboon	Cable car	Yacht	Baboon	Cable car	Yacht
MSE	0.1845	0.1848	0.4448	0.1692	0.1668	0.0183
PSNR	55.4718	55.4633	51.6487	55.8461	55.9082	65.4948
SSIM	0.9997	0.9982	0.9991	0.9998	0.9986	0.9996

- 2) In the second research, the classical 2-LSB and 3-LSB methods and the discussed existing methods are applied on 3 different cover images [11]. To view the effect of the messages on different sizes of images, different text files of distinct sizes are used. The values of the chaos generator logistic map used in this method are $x = 0.676$ and $u = 3.9761$. In this method, the employment of the logistic map random number generator and operation of XOR-ing for the encryption of data message in the algorithm has decreased the chances of any attack against the stego image. Table 3 shows the embedding results [17].

Table 3
Embedding results [17]

IMAGE	IQM	Text file – Text1.txt			
		2-bit LSB	Proposed 2-bit LSB [17]	3-bit LSB	Proposed 3-bit LSB [17]
Lena	PSNR	53.0082	55.2505	48.5549	51.397
	SSIM	0.9998	0.9999	0.9996	0.9998
Cat	PSNR	63.7063	65.9110	59.1702	62.0850
	SSIM	0.999998	0.999999	0.9997	0.9998
Bird	PSNR	65.0086	67.2403	60.5294	63.3893
	SSIM	0.999998	0.999999	0.9998	0.9999

The thing that came to notice is that, during the embedding method the reduction in the difference between the stego and cover images improves the LSB.

- 3) In the third research paper, the filtering method is done with the help of AES Algorithm in which XOR operations were also performed in the embedding and extracting algorithms. In AES Algorithm, substitutions and permutations are done as the operations are all linked in a series. And this method is done on bytes rather than the bits.[18]
- 4) In the fourth paper, the visual quality and level of security is well maintained, and the method proposed can also hide information of

bulky amount. Here the original message is encrypted first through the AES algorithm of cryptography [19] and then the message is embedded. In [20], stream builder approach for LSB steganography is explained with the use of AES for high security.

- 6) In the LSB Matching revisited, only one change is made :- two bits of secret image pixel with the two pixels of cover image. In the embedding algorithm of the steganography scheme, the secret data or message is first divided into 'v' bits, and then the '2v-1' pixels are chosen to hide in the cover input image. Moreover, in the method proposed, the capacity is $((2v-1) / 2v-1-1)*100\%$ higher as compared to the F5 approach. [21]
- 7) According to the paper, in the Pixel-value differencing method the secret bits are embedded in the block by the use of the difference value between its two consecutive pixels. Now here the authors have proposed the LSB replacement method where the secret message is hidden in the least significant bits of the cover image's pixels but after the embedding process the image quality does not remain the same and gets degraded. To get the improved quality back another algorithm is also used along with the LSB, which is the genetic algorithm. [22]
- 8) The research proposed here uses the achromatic component of the HSI (Hue Saturation Intensity) color model in spatial domain along with MLE (Multi-Level Encryption). The converted and transposed cover image of HSI color model is used, the secret key divides the image in four equal sizes and rotates each part with different angle. The encryption should be done with MLE algorithm as the secret information is to be divided in 4 equal blocks. Now the magic LSB method is used to embed message in one of the sub images which are rotated. This method provides good security along with enhanced high quality of visual of the stego images and the imperceptibility is also better as compared to other existing methods. [23]
- 9) To increase the security against unauthorized attacks adaptive methods of steganography are used and here in this paper it is used also for the same purpose. For embedding parts of the most adaptive algorithms LSB-F (LSB flipping) is considered best as it is more vulnerable against attacks and also allows adaptive algorithms to be extracted at the side of the receiver. Data extraction at the side of the receiver may become difficult when the LSB-M (LSB matching) is used but in it the security is also enhanced. In this research paper,

an adaptive algorithm is proposed which unlike other methods, uses LSB matching as its method of embedding. To determine the locations of the image as secured, a measure of complexity is used which is based on the analysis system of local neighborhood. Here the data is accurately retrieved when the complex pixel categorized at the side of the transmitter is embedded and at the receiver's side also it is considered to be complex. The PSNR values obtained are also high as compared to other adaptive algorithms and the security is also determined to be higher in comparison to the LSB-M.[28]

B. Parameters used

- a) MSE – it evaluates the average of the (difference)² between the actual value and the estimated values. Mean squared error between two images can be calculated by the formula given in [24]. X and N represent the dimension and C and L represent Cover and stego image respectively. Pixel locations of these images are denoted by i and k.

$$MSE = \frac{1}{XN} \sum_{i=1}^X \sum_{k=1}^N (C_{i,k} - L_{i,k})^2$$

- b) PSNR – it denotes “Peak Signal to Noise Ratio” expresses a ratio between the maximum feasible strength of a signal and the power of disturbing disturbance (Noise) that affects its quality. It is stated in [24] [25] [26] [27]-

$$PSNR = 10 \frac{\log_{10}(\text{Peak value})^2}{MSE} dB$$

- c) SSIM – It denotes “Structural Similarity Index Measure” shortly names as SSIM, it is used to tell the degradation in the image quality which is done because of the compression of data or by some losses during the transmission of data [26] [27].

Conclusion

This paper mainly focusses on steganography and its different types. Each algorithm is briefly discussed giving a clear insight into them. The technique which is deeply talked about is the Image steganography. The four types of methods involved in it are also defined, but the LSB Algorithm for Image steganography is backbone of this review paper.

Here the papers reviewed have used their own proposed methods of LSB technique for Image Steganography as the original LSB method is

simple to understand, implementation of it is also easy, thus the resulting stego images are of high quality. But in the Existing methods the quality of stego image is better, and the secret message is also hidden with full security.

The PSNRs, MSEs and SSIMs are calculated by the existing LSB methods and were compared with their given approaches which are also precisely matching the results. The observed values on different parameters are also higher in latest existing methods than the previous existing LSB Algorithm's because the research developed efficient algorithms then the previously existing algorithms.

References

- [1] Snehal Kurane, Hrutuja Harke, and Sheetal Kulkarni, "TEXT AND AUDIO DATA HIDING USING LSB AND DCT AREVIEW APPROACH", *Int. j. innov. eng. res. technol.*, pp. 1–4, Mar. (2021).
- [2] E. Nandhini, M. Nivetha, S. Nirmala, and R. Poornima, "MLSB Technique Based 3D Image Steganography Using AES Algorithm," *J. Recent Res. Eng. Technol.* ISSN, vol. 3, no. 1, p. 2936 (2016).
- [3] Singh and M. Singla, "A Novel Method of high-Capacity Steganography Technique in Double Precision Images," 2021 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, pp. 780-784 (2021).
- [4] S. Ilasariya, P. Patel, V. Patel and S. Gharat, "Image Steganography Using Blowfish Algorithm and Transmission via Apache Kafka," 2022 4th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India (2022).
- [5] R. Dumre and A. Dave, "Exploring LSB Steganography Possibilities in RGB Images," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1-7 (2021).
- [6] Sharma, V.K., Srivastava, D.K., Mathur, P.: "A study of steganography based data hiding techniques." *Int. J. Emerg. Res. Manag. Technol.* 145–150 (2017).
- [7] Mohammed A. Saleh, "Image steganography techniques- a review paper". Vol. 7, Issue 9, September (2018).
- [8] A. Sharma, A. Batta and V. K. Sharma, "A Review on Image Steganography and its Applications," 2021 Fifth International Conference

- on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, pp. 1466-1473 (2021).
- [9] V. k. Sharma, R. Jaya Krishna, A. Singh and V. S. Rathore, "Secure Data Hiding Technique using Secret Image Scrambling," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 831-836 (2020).
 - [10] Manish Munikar, "Image Steganography: Basic Concepts and Proposed Algorithm."
 - [11] N. Zhong, Z. Qian, Z. Wang, X. Zhang and X. Li, "Batch Steganography via Generative Network," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 1, pp. 88-97, Jan. (2021).
 - [12] H.Al-Bahadili, "A secure block permutation image steganography algorithm." *International Journal on Cryptography and Information Security* 3(3):11-122, September (2013).
 - [13] Avni Aggarwal, Arpit Sangal and Aditya Varshney, "Image steganography using LSB Algorithm." *International Journal of Information Sciences and Application (IJISA)*. ISSN 0974-2255, Vol.11, No.1 (2019).
 - [14] Shrikant S. Khare and Sanjay Laxmikant Nalbalkar, (2010)," Steganography – Bit Plane Complexity Segmentation.", *International Journal of Engineering Science and Technology*, Vol. 2(9), 4860-4868 (2010).
 - [15] K. Satish, T. Jayakar, C. Tobin, K. Madhavi and K. Murali, "Chaos based spread spectrum image steganography," in *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 587-590, May (2004).
 - [16] E Z Astuti, D R I M Setiadi, E H Rachmawanto, C A Sari1 and Md K Sarker (2019) "LSB-based Bit Flipping Methods for Color Image Steganography." *Journal of Physics-Conference Series* 1501 012019, (2020).
 - [17] ÖZCAN ÇATALTAŞ, 2KEMAL TÜTÜNCÜ , " Improvement of LSB based Image Steganography." *International Journal of Electrical Electronics and Data Communication* 5(9):1-5, January (2017).
 - [18] M.R. Islam, T.R. Tanni, S. Parvin, M.J. Sultana and A. Siddiqua, "A modified LSB Image steganography method using filtering algorithm and stream of password." Pages 359-370 | Published online: 29 Nov 2020, Information Security Journal.
 - [19] Sharma, V.K., Srivastava, D.K. "Comprehensive Data Hiding Technique for Discrete Wavelet Transform-Based Image Steganography Using Advance Encryption Standard." In: Vishwakarma, H., Akashe, S. (eds) *Computing and Network Sustainability. Lecture Notes in Networks and Systems*, vol 12. Springer, Singapore (2017).

- [20] Sharmin Sultana, Afrida Khanam, Md. Rashedul Islam, Adiba Mahjabin, Masud Ibn Afjal and Md. Fazle Rabbi, "A modified filtering approach of LSB Image steganography using stream builder along with AES Encryption." *Recent Trends in Information Technology and its Applications*, Pp 1-10, Volume 1 Issue 2 (2018).
- [21] Mansoor Fateh, Mohsen Rezvani, Yasser Irani, "A New Method of Coding for Steganography Based on LSB Matching Revisited", *Security and Communication Networks*, vol. 2021, Article ID 6610678, 15 pages (2021).
- [22] Hsein-Chu Wu, N. I. Wu and C. S. Tsai, "Image steganographic scheme based on pixel value differencing and LSB replacement methods." *IEE Proceedings - Vision Image and Signal Processing* 152(5) : 611 - 615 (2005).
- [23] Khan Muhammad, Muhammad Sajjad, Irfan Mehmood, Seungmin Rho, Sung Wook Baik, "A Novel Magic LSB Substitution Method (M-LSB-SM) using Multi-Level Encryption and Achromatic Component of an Image." 01 Nov 2016-Multimedia Tools and Applications (Springer US)-Vol. 75, Iss: 22, pp 14867-14893.
- [24] Tuieb, Munthir Bahir, Serteep, Hind Jumaa & Ali, Doaa Muhsin Abed. Image steganography using Fresnelet transformations, stated coefficients and a pre-processed message, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:6, 1683–1689 (2023).
- [25] Sharma, V. K., Srivastava, D. K., & Mathur, P. "Efficient image steganography using graph signal processing." *IET Image Processing*, 12(6), 1065–1071 (2018).
- [26] Sharma V.K., Sharma, P.C., Goud, H. et al. "Hilbert quantum image scrambling and graph signal processing-based image steganography." *Multimed Tools Appl* 81, 17817–17830 (2022).
- [27] Pilaian, Urmila, Kumar, Manoj & Mittal, Vivaan. Performance evaluation of LSB steganography based on multiple image formats, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:7, 1911–1924 (2023).
- [28] Vajiheh Sabeti, Shadrokh Samavi and Shahram Shirani, "An adaptive LSB matching steganography based on octonary complexity measure." *Multimedia Tools and Applications* Volume 64 Issue 3 June 2013 pp 777–793.