Steganography Using Bit Plane Embedding and Cryptography

Bharti Rathor and Ravi Saharan

Abstract In the modern era of digital advancement of images, all information are exchanged through Internet, so for exchanging any secret message, either cryptography or steganography is used. Cryptography is a process of converting data in unreadable form. We can embed even the existence of data itself. In this paper, we proposed a new robust and secure method to embed secret message in an image. To increase robustness of message, intermediate significant bits (ISB) are used instead of using LSBs. To increase the security of message, encryption technique is used. The objective of the paper is to embed a message in bit plane such that it is robust against various attack and transformation (like scaling, cropping, filtering, etc.) and also maintaining the perceptual transparency of stego-image.

Keywords LSB · ISB · SIHS · Discrete logarithm · Random numbers

1 Introduction

Nowadays, information exchanging on Internet has rapidly increased. Large amount of information is being exchanged through Internet. As we know, Internet is open to all, information may leak out and can be used for illegal purpose knowingly or unknowingly. So information security plays an important role in Information Technology.

In the growing digital world, multimedia takes an important role in communication. Lots of information are being exchanged through images from one side to other. A user can send secret data/message by hiding in image. Two concepts such as steganography and cryptography are used to exchange information in concealed manner. In cryptography, we can convert our original message in a form that any

B. Rathor (✉) · R. Saharan
Central University of Rajasthan Kishangarh, Kishangarh 305817, Rajasthan, India
e-mail: 2015mtcse003@curaj.ac.in

R. Saharan
e-mail: ravisaharan@curaj.ac.in

A.K. Somani et al. (eds.), *Proceedings of First International Conference on Smart System, Innovations and Computing*, Smart Innovation, Systems and Technologies 79, https://doi.org/10.1007/978-981-10-5828-8_31

unauthorized user cannot read and understand. It is encrypted using a key which is shared between sender and receiver only and without this shared key, user cannot get message back from encrypted message. We encrypt the message in such a way that intruder cannot decrypt the message even know the existence of message. But in steganography, intruder does not have any clear idea even about the existence of message that is hidden in the image being shared. Image steganography helps to provide those methods that embed our secret message without degrading the perceptual quality of carrier image. The carrier image and secret message together produce stego-image by applying algorithm. Then, stego-image is transferred through Internet to the recipient. The recipient gets back the message using extracting algorithm and that key which is provided by the sender from stego-image separately [1, 2, 3].

Architecture of steganography model using the method of cryptography is illustrated in Fig. 1.

In the image processing, various type of steganographic techniques exist which are categorized based on the type of hiding carrier object. Various steganography methods can be used to provide more security and robustness by using good carrier object. Since the growth of digital images in multimedia on Internet, people use images mostly for exchanging information to one end to the other [4, 5]. It can be shown in Fig. 2.

There are several types of methods in image steganography.

(1) LSB (least significant bit) methods
(2) Transform domain methods

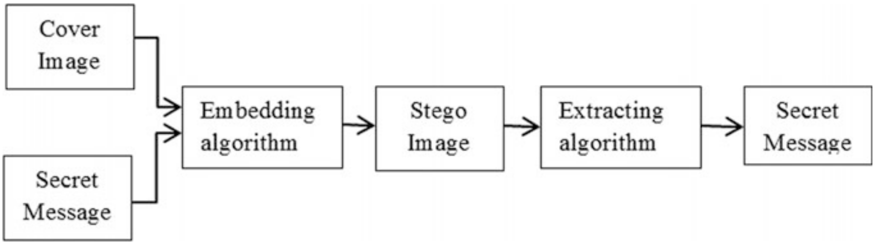
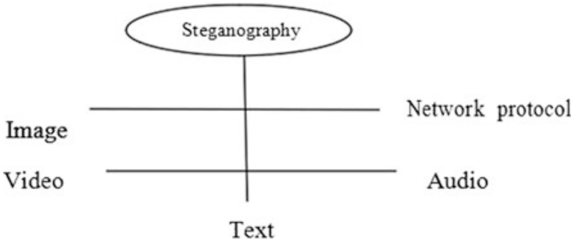


Fig. 1 Architecture of steganographic process using the concept of cryptography

Fig. 2 Types of steganography



(3) Statistical methods
(4) Distortion methods

LSB is a simple and easy method to implement but mostly used to hide the message bits directly into the least significant bits of the cover image. Revamping the least significant bits that does not mean change is perceptible to human because of the less amount of change in intensity value of pixels. But it is not so robust and secure that stego-image can survive against various attacks. In proposed technique, we use ISB method to hide our original message in the intermediate significant bits (2nd–7th LSB's) of cover image depending on its binary coding [6].

In the transform domain technique, we transform the spatial domain method to frequency domain with the help of discrete cosine transform (DCT), fast Fourier transform (FFT), discrete Fourier transform (DFT), and discrete wavelet transform (DWT), etc.

In masking and filtering methods, two signals are embedded together in such a way that only one of the signals is perceptible to the human eye using human visual system (HVS). This method is mostly used in watermarking techniques [7, 8].

2 Related Work

In the area of image processing, many steganography methods exist for hiding message in an image. These methods can be categorized into: (1) spatial domain technique (2) transform domain technique. The spatial domain based steganography directly changes some bits in the image pixel values in hiding data using LSB method.

In [2], Akram and Azizah used ISB method for hiding the message in cover image in such a way to improve the security and robustness of stego-image. The method is based on checking the value of the secret message to the range of 4th bit plane. Author suggests the result after applying technique for every bit plane (1–8) and all possible values of bias (x), best robustness can get with stego-image using the 4th bit plane at the bias value = 6.

The value of 8-bit plane can be represented by 2^{n-1}, where n is the order of the plane starting from 1 to 8. The maximum and minimum value of intensity value of pixel that can fit in 8-bit plane is 255 and 0. Here, n=5 because we are cosidering 4th bit plane for embedding purpose that is 5th LSB of that number. So L = 25–1 = 16 and number of ranges is 256/L = 256/16 = 16 are [1:15] [16–31]…. [248–255]. Each range is divided into two ranges that are left-hand group and right-hand group. Author embeds data bits in randomly chosen pixel based on the checking of pixel value lying in the left-hand group and right-hand group and replaced it by new pixel using the bias value.

In [7], Mohammad Ali Shamalizadeh Baei uses SIHS (secure information hiding system) method used to secure the secret message and decode the sequence mapping problem. Author uses discrete logarithm calculation to change the message in encrypted form. The main idea here is to generate a series of random numbers of length equal to the message length that ranging from 3 to 8. These series numbers will be used in random mapping. It will provide more randomness in encrypted form of secret message.

In [9], N.S. Raghav, Ashish Kumar, and Abhilasha Chachal suggest a novel technique to enhance the standard LSB technique by using pseudorandom generation using H'enon chaotic map. This encryption using pseudorandom generator provides more security to the system as the same subset of random numbers cannot be reproduced without knowing the random generator function and thus the secret data cannot be revealed easily. Further, they are used to encrypt to unhide the message in an image by selecting random pixels.

In [3], Anil Kumar and Rohini Sharma use hash-LSB method and encrypt data using RSA algorithm in order to achieve more randomness and hide data in carrier object. Author utilizes a hash function to create a pattern for concealing data bits into LSB of cover image. RSA algorithm gives very secure method of steganography because of using large prime numbers for key that is to be used for encrypting and decrypting message. This technique becomes more security cause of RSA algorithm.

In [4], Bhavana S. and K.L. Sudha explain about a way in which data can be embedded using LSb method along with chaos. Chaos-based techniques provide more security that can be revamped by utilizing multiple chaotic maps for encryption as well as decryption and hiding of message in cover image.

In [10], Y.K. Jain and R.R. Ahirwal have suggested an efficient LSB method which is used for generating a stego-key by dividing the image pixels ranges (0–255). Decide the fixed number of bits insertion into each range and adaptive number of bits insertion into different ranges based on pixel count of cover image in different ranges. K-bits of secret message are substituted into least significant part of pixel value.

The strength of proposed method is its perceptibility and more randomness and high hidden capacity of secret hidden information in stego-image. This method is used to provide high hidden capacity with robustness and more randomness of secret data. RGB image has more capacity to hide the message in cover image because it has 24 bits of each of three channels red, green, and blue [11]. So it provides more randomness and high hidden capacity. Generally, we use grayscale image for simple and efficient technique to hide information.

In this work, we are using SIHS method for providing more security and random selection of pixels, pseudorandom function generator for more randomness in bits of binary form of secret message, watermarking method for hiding message bits in such a manner that message should undamaged as same as possible; detailed procedure is explained in the next section of the paper.

3 Proposed Work

We proposed a new technique to hide secret message in cover image which consists of random cipher technique, embedding, and extracting algorithm.

In order to increase the security and robustness of the method, the secret message is encrypted with random cipher technique with the key which is to be known to sender and recipient only.

3.1 Cipher Technique

This is the process of generating a series of random numbers using key and encrypting a message (series of characters) using randomly generated numbers as, Caesar cipher technique. Random cipher encryption technique is explained in the following example.

Plaintext	A	T	T	A	C	K	A	T	D	A	N
Key	3	9	7	6	2	4	8	5	1	6	3
Cipher text	D	C	A	G	E	O	I	Y	E	G	Q

Security of this cipher technique is depends on the key.

3.2 Discrete Logarithm

It is used to generate a series of random numbers and then added into message characters. Produced series of characters known as encrypted message. These random number values are computed using the following Eq. 1:-

$$x(i) = a{*}x(i-1)(mod\, p). \tag{1}$$

where i = 1, 2, 3…, m

X (0) = is the sum of k digits.

a = 3 * x (0) and p = K.

These random numbers are also used for selecting pixel position where message is to be hidden [6].

3.3 Embedding Process

For improving the robustness of the method, hide the encrypted message in the cover image using concept of ranges and ISB method. We use the fact of 4th bit

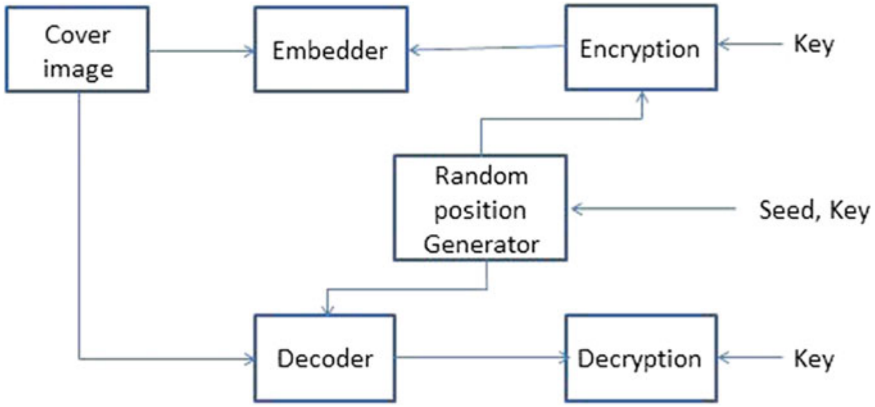


Fig. 3 Architecture of proposed model

plane and bias value is equal to 6 suggested by author in [2]. Proposed work model is given in Fig. 2 (Fig. 3).

4 Proposed Algorithm

In this section, we describe the proposed method to enhance security and robustness of stego-image. That contains embedding extracting algorithm and Vigenere cipher technique. The embedding and extracting algorithms are described below:

4.1 Embedding Algorithm

This algorithm is explained in the following steps.

- Input: An M × N carrier image and a secret message.
- Output: An M × N stego-image.

(1) Read cover image and secret message.
(2) Apply random cipher technique using key to encrypt the secret message for securing the message.
(3) Convert the decimal form of encrypted message to binary form.
(4) Now select random column of cover image matrix pixel using random numbers generated by discrete logarithm.
(5) Calculate range for selecting the 4th bit plane by $l = 2^{n-1}$(n = position of LSB, here n is 5for 4th bit plane) and number of ranges is 256/l.

(6) Every range is broken down into two equal groups L (left hand) and R (right hand); each group length is l/2.

(7) Now start comparing the 4th bit of selected pixel with each bit of binary form of encrypted message, this process is repeated for each row of selected random columns until the message length. If this equation is satisfied then go to Step 8 else go to Step 9.

(8) If

(a) pixel lies in the left group, calculate difference = original pixel value—minimum value of the range (where d is the distance between the original pixels and closer edge of the ranges).
Check whether (D >= b) is satisfies or not, if it satisfies then the pixel value will be the same else become (minimum pixel value of the range + b). Here, b = bias value.

(b) If pixel lies in the right group, d = maximum pixel value of the range—original pixel value. Check whether (D >= b) is satisfies or not, if it satisfies then the pixel value does not changed else become (maximum pixel value of the range –b).

(9) If

(a) Pixel value lies in the left group or in last group, the intensity value of pixel become (maximum pixel value of the previous range –b).

(b) Pixel value lies in the Right group or in the first range; the intensity value of pixel is (minimum pixel value of the next range +b).

(10) So hiding of encrypted message is completed and at last, we generate stego-image.

4.2 Extracting Algorithm

This algorithm is explained in the following steps.

- Input: An M × N stego-image
- Output: A secret message.

(1) Read the stego-image.

(2) Store the intensity value of original pixel and changed pixel of cover and stego-image.

(3) Calculate the range of both pixels for each row of selected same random columns as embedding algorithm using seed and random permutation until the length of message.

(4) If both pixel values lie in same range then embedded bit is 4th bit of original pixel else go to step 4.

(5) If 4th bit of pixel is 0 then embedded bit is 1 else 0.
(6) So, we get combination of 1-0 bits and then convert it into decimal form.
(7) Convert decimal form to character form of encrypted message.
(8) Decrypt the encrypted message using reverse of random cipher technique using same key as used before in encryption technique. At last, we get original message which was hidden in cover image.

5 Implementation and Results

5.1 Experimental Setup

The proposed algorithm is implemented on these configurations (Table 1).

5.2 High Capacity

For any steganographic technique, message size to be hidden in an image should be as large as possible. If secret message spread throughout the whole image then conceal the existence of message and revealing is hard to intruder. Proposed method provides high capacity of data which is to be embedded in an image.

5.3 Perceptual Transparency

After embedding, stego perceptual quality will be compromised into stego-image as compared to cover image. Quality of stego-image depends on the data hiding method for embedding message bit in an image. Perceptual transparency should be high. For that, we hide the message bit on the intermediate significant bit instead of least significant bit. Proposed method maintains perceptual transparency of stego-image, which can be shown as in Fig. 4 (Fig. 5).

Table 1 Configuration details

OS	Windows 7 ultimate 64 bit
Processor	Intel core i3 first generation
Memory	4 GB
Software used	MATLAB 2011a
Input image	Standard grayscale images of size 512 * 512 are used

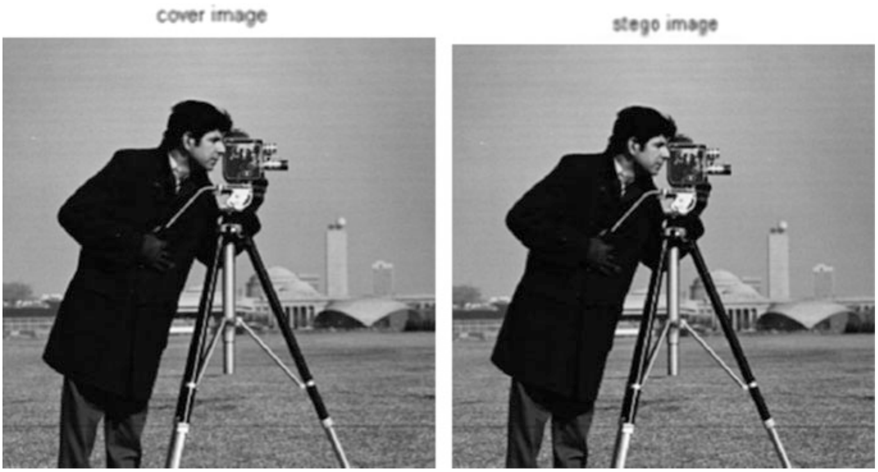


Fig. 4 Cover and stego-images

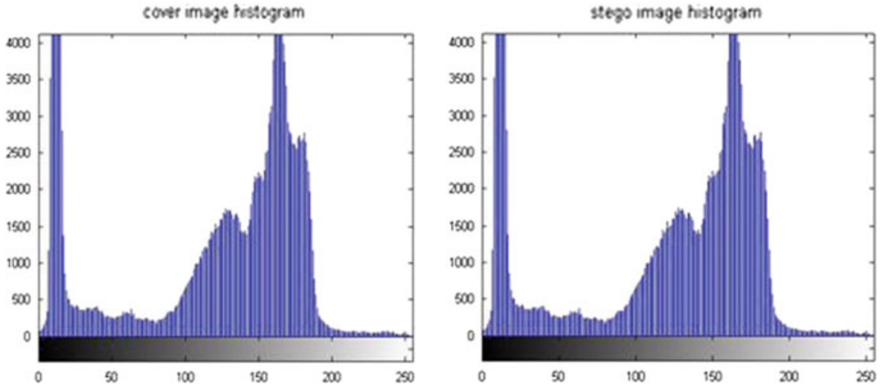


Fig. 5 Histograms of cover and stego-images

5.4 Temper Resistance

If once the message has been hidden into stego-image, it should be complex to modify the message. Any intermediate person cannot alter the secret message after embedding it into carrier object.

5.5 Computational Complexity

Computational cost for embedding and extracting an embedded message using applied algorithm is defined as computational complexity.

The computational complexity of infrequent operations is proportional to nnz, the frequency of nonzero elements in the matrix. Proposed method is less complex, efficient, and takes less time. So, it maintains computational complexity as much as less possible.

5.6 Robustness

After hiding message in the cover image, message should remain same if covered image handles with some operation such as cropping, scaling, filtering, JPEG compression, and addition of noise.

To check the robustness of suggested method, MSE and PSNR will be used. The MSE and PSNR are defined as given by Eq. 2 and 3.

$$MSE = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - I1(i,j)]^2. \tag{2}$$

MSE = mean square error rate between two objects.

Where I = Cover image, I1 = Stego-image and m. n = Number of pixels.

$$PSNR = 10 \log_{10}\left(\frac{R^2}{MSE}\right). \tag{3}$$

PSNR = Peak signal-to-noise ratio between two objects.

In the Eq. 3, R is defined as maximum oscillation in the input image data type. For example, if the input images have a double-precision floating-point data type, then R is 1. If input image has an 8-bit unsigned integer data type, R is 255.

The security comparison between images before and after applying attacks is given in Tables 2 and 3, respectively.

Table 2 PSNR and MSE between cover and stego-images

Images	PSNR (dB)	MSE
Cameraman	57.5122	0.1303
Vase	57.7232	0.1107
Woman_blonde	57.7385	0.1103

Table 3 PSNR and MSE of images after applying attacks

Images/PSNR and MSE between images		Gaussian noise attack	Salt and pepper attack	Poison noise attack	Filtering attack	JPEG compression attack
Cameraman	PSNR	56.9814	55.8912	54.8901	53.721	53.8231
	MSE	0.1621	0.1456	0.1483	0.1324	0.1782
Vase	PSNR	56.8761	55.8281	54.8741	53.7665	53.7671
	MSE	0.1456	0.1345	0.1567	0.1324	0.1564
Woman_ blonde	PSNR	56.7981	55.8720	54.8140	53.7634	53.7650
	MSE	0.1345	0.1567	0.1236	0.1546	0.1721

6 Conclusion

The technique is an enhancement over existing methods compared to several methods of steganography while maintaining the method simple enough and keeping it easy to implement according to practical aspects. We have used the random cipher technique using key and random selection of pixel from cover image, which gives extra security to the stego-image. The proposed algorithm gives better security that provides secrecy of the original message and more randomness with robustness. The performance analysis is being done. The values of PSNR and MSE are also being calculated.

References

1. Abbas, Cheddad, Joan Condell, Kevin Curran, PaulMcKevitt. Digital image steganography: Survey and analysis of current methods. In: ELSEVIER (2010).
2. Akram M.zeki and Azihah A. Manaf.: A Novel digital watermarking Technique based on ISB. In: World Academy of Science, Engineering and Technology Vol:3 (2009).
3. Anil Kumar and Rohini Sharma.: A Secure image steganography based on RSA algorithm and Hash—LSB technique. In: International Journal of advance research in Computer Science and software engineering volume 3 Issue, July(2013).
4. Bhavana. S and K.L. Sudha.: text steganography using LSB insertion method along with chaos theory. In: IEEE Explore (2011).
5. Mehdi Hussain and Mureed Hussain.: A Survey of Image steganography Techniques. In: (SZABIST), Islamabad, Pakistan. (2013).
6. R.O.EI Safy and H. H. Zayed.: An Adaptive Steganographic Technique Based on Integer Wavelet Transform. In: IEEE Explore (2009).
7. Mohammad Ali Shamalizadeh Baei and Reza karami.: A new algorithm for embedding message in image steganography.In:International Journal of Engineering Research & Technology (IJERT) Vol. 3 Issue 2, February (2014).
8. Raja Lakshmi C S, Sowjanaya T P and Hemant Kumar C S.: Image Steganography using H-LSb Technique for hiding Image and Text using Dual Encryption Technique. In: SSRG international journal of Electronics and communication Engineering (SSRG-IJECE)-volume 2 Issue 5, May 2015).

9. N S Raghav, Ashish Kumar, Abhilasha Chachal. Improved LSB method for Image Steganography using Henon chaotic Map. In: Open Journal of information Security and applications volume 1, July(2014).
10. Y. K. Jain and R. R. Ahirwal.: A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Key. In: International Journal of Computer Science and Security (IJCSS), vol. 4, (2010).
11. Prashant Manuja and Ravi Saharan.: Statistical Pixel blocks Selection. In: International conference on Advanced communication control and computing technologies(ICACCCT) ISBN No.978-4799-3914-5/14/$31.00@2014 @ (2014).