Spatial Domain Image Steganography based on Security and Randomization

NamitaTiwari
Department of CSE & IT
MANIT
Bhopal, India

Dr. Madhu Sandilya
Department of ECE
MANIT
Bhoapl, India

Dr. Meenu Chawla
Department of CSE & IT
MANIT
Bhopal, India

***Abstract*—In the present digital scenario secure communication is the prime requirement. Commonly, cryptography used for the said purpose. Another method related to cryptography is used for the above objective is Steganography. Steganography is the art of hiding information in some medium. Here we are using image as a means for covering information. Spatial domain image Steganography has been used for the work because of its compatibility to images. Objective of the paper is to increase the capacity of hidden data in a way that security could be maintained. In the current work MSB of the randomly selected pixel have been used as indicator. Result analysis has been performed on the basis of different parameters like PSNR, MSE and capacity.**

Keywords-- Spatial domain; PSNR; MSE

I. INTRODUCTION

Steganography can be used to hide or cover the existence of communication of encrypted data. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. A solution to this problem is Steganography [1]. The purpose of both Steganography and Cryptography is to provide secret communication. Cryptography hides the contents of a secret message from an attacker, whereas Steganography even conceals the existence of the message. In cryptography, the system is broken when the attacker can read the secret message [2]. Breaking a steganographic system has two stages: first the attacker can detect that Steganography has been used second he is able to read the embedded message.

In section II requirement and importance of steganography has been described. Section III explains about different techniques of image steganography. Section IV shows LSB technique. Section V describes about different LSB based methods. Section VI defines the objective of proposed work. Section VII explains different parameters for result analysis. Section VIII shows the comparative result analysis. Section IX describes conclusion and future work of the paper.

II. REQURIMENTS FOR STEGANOGRAPHIC SYSTEM

- Imperceptibility: The stego image and original image should be perceptually identical.
- Undetectable embedded data.
- Security
- Maximizing Capacity of embedded data.
- Robustness: The embedded data should survive against various attacks.

Applications and Importance of a Steganographic system that it is used as Security reinforcement layer to cryptography [1]. It is used in digital watermarks, fingerprinting, defense, business, and education field. Image Steganography is about exploiting the limited powers of the human visual system (HVS)[2]. Within reason, any plain text, cipher text, other images, or anything that can be embedded in a bit stream can be hidden in an image. Image Steganography has come quite far in recent years with the development of fast, powerful graphical computers.

III. TECHNIQUES FOR IMAGE STEGANOGRAPHY

A. Spatial Domain based Steganography

It includes LSB (Least Significant Bit) Steganography. The spatial methods are most frequently employed because of fine concealment, great capability of hidden information and easy realization. LSB Steganography includes two schemes: Sequential Embedding and Scattered Embedding. [4]

B. Transform Domain based Steganography

The method of transform domain Steganography is to embed secret data in the transform coefficients.

C. Document based Steganography

This method embeds data in documents files by adding tabs or spaces to .txt or .doc files.

D. File Structure based Steganography

This method inserts secrets data in the redundant bits of cover files, such as the reserved bits in the file header or the marker segments in the file format.

IV. SPATIAL DOMAIN EMBEDDING

In the LSB technique, the LSB of the pixels is replaced by the message to be sent, this has the effect of distributing bits evenly, thus on average only half of the LSB's will be modified [4, 5].

Least Significant Bit Method
Consider a 24-bit picture
Data to be inserted: character 'A': (10000011)
3 pixels will be used to store one character of 8-bits

Example:

00100111	11101001	11001000
00100111	11001000	11101001
11001000	00100111	11101001
Embedding 'A'		
00100111	11101000	11001000
00100110	11001000	11101000
11001001	00100111	11101001

V. LSB BASED STEGANOGRAPHY METHODS

A. Stego One Bit

This method changes only single LSB of the pixel. Changing the LSB will only change the integer value of the byte by one. This small change is not noticeable. This is the first method to be tested and will involve encoding some of the basic processes required for later Steganographic methods to be tested also. This should have very less effect on the appearance of the image [2].

B. Stego Two Bit

Using this method two LSBs of one of the colours in the RGB value of the pixels will be used to store message bits in the image.[2] The advantage of this method is that twice as much information can be stored here than in the previous method.

C. Stego Three Bit

Using this method three LSBs of one of the colours in the RGB value of the pixels will be used to store message bits.The data hiding capacity is three times the storage capacity of Stego One Bit but the image will be even more distorted.

D. Stego Four Bit

Using this method four LSBs of one of the colours in the RGB value of the pixels will be used to store message bits.The data hiding capacity is 4 times the storage capacity of stego 1 bit, but the image will be more distorted.

A. Stego Colours Cycle

In order to make the detection of the hidden data more difficult it was decided to cycle through the colours values in each of the pixels in which to store the data [2, 7]. This also means that the same colours were not constantly being changed. For example the first data bit could be stored in the LSB of the blue value of the pixel, the second data bit in the red value and the third data bit in the green value.SCC technique is an enhancement. This technique is more secure than the LSB. But still it is suffers detecting the cycling pattern that will reveal the secret data. Also it has less capacity than LSB.

TABLE I. MEANING OF INDICATOR VALUES FOR PIXEL INDICATOR TECHNIQUE

Indicator Channel	Channel-1	Channel-2
00	No Hidden data	No Hidden data
01	No Hidden data	2 Bits of Hidden Data
10	2 Bits of Hidden Data	No Hidden data
11	2 Bits of Hidden Data	2 Bits of Hidden Data

E. Pixel Indicator High Capacity Technique

It uses the least two significant bits of one of the channels to indicate existence of data in the other two channels [5]. Table 1 shows meaning of indicator values for pixel indicator technique.

F. Triple-A: Based on Randomization

This algorithm can be divided into two major parts: Encryption and Hiding [7].

1) Encryption: Part one is related to encrypting the message (M) using AES algorithm, which will produce Enc (M, K). In implementation the key K can be generated from a set of user password.

2) Hiding: The RGB Image is used as a cover media. Enc (M, K) is hidden according to triple-A algorithm, which needs to have a pseudorandom number generator (PRNG). The assumption for PRNG is to give two new random numbers in every iteration. The seeds of these PRNGs namely Seed1 (S1) and Seed2 (S2) are formed as a function of the Key (K). S1 is restricted to generate numbers in [0, 6]. S1 random number is used to determine the component of the RGB image, which is going to be used in hiding the encrypted data Enc (M, K). Table 2 shows how (S1) random number selects the RGB components. S2 is restricted to the interval [1, 3]. S2 random number determines the number of the component(s) least significant bits that is used to hide the secret data. Table 3 shows how (S2) random number determines the number of component bits. By combining data from the previous tables, we can see that the minimum number of bits used in each pixel is 1. If we use only one bit of one chosen components of the RGB image.

TABLE II. SEED 1 RANDOM NUMBER USAGE

	Random Number	Meaning to the algorithm
1st PRNG	0	Use R
	1	Use G
	2	Use B
	3	*Use RG*
	4	*Use RB*
	5	*Use GB*
	6	*Use RGB*

TABLE III. SEED 2 RANDOM NUMBER USAGES

	Random Number	Meaning to the algorithm
2st PRNG	1	Use 1 bit of the component(s)
	2	Use 2 bit of the component(s)
	3	Use 3 bit of the component(s)

TABLE IV. PROPSED ALGORITHM

3 MSB of channel (R/G/B)			Channel (R/G/B)
0	0	0	1 bit Hidden Data
1	0	0	2 bit Hidden Data
1	1	0	3 bit Hidden Data
1	1	1	4 bit Hidden Data

The maximum is 9 bits if we used all the three components with three bits.

Capacity factor = number bits used inside a pixel to hide part of the secret message/ the number of bits in the pixels itself

Capacity factor can be in the range from 1/24 to 9/24.

VI. Objective Of The Study

Objective of the work is to increase the capacity of hidden data in the way that image should be less distorted and unauthorized person cannot detect that Steganography is going on. Randomization has been used to select the pixel to overcome the sequential pattern. It is proposed to use MSB (Most Significant Bit) of the pixel as indicator for data hiding. Message is hiding in all three channels according to the indicator bits in MSB.

In Proposed Method there are two phases.

A. First Phase

The indicator channel has been decided by the user, suppose red is an indicator channel and three MSB of red channel are 101, and then MSB of indicator channel will decide that which channel is used for data hiding. (101 used for RGB respectively).

For example:

R	G	B
1	0	1

Here 1 indicates to hide the data and 0 indicate for not hiding the data. In above case, channel R and B will use for hiding data and channel G will not use for hiding data.

B. Second Phase

In first phase we have decided the channels for data hiding, now in second phase we will decide the no. of bits to be hidden. Three MSB of selected channel (R/G/B) will decide that how many bits of message will be hidden in that particular channel. Table 4 shows the method of second phase.

To optimize the proposed algorithm it has been checked on different parameters.

VII. Parameters For Result Analysis

A. Capacity

This is the term refers to the amount of data that can be hidden in the medium. It is defined as the maximum size that can be hidden in the medium. It is defined as the maximum size that can be embedded subject to certain constraints [10].

Capacity factor = number bits used inside a pixel to hide part of the secret message/ the number of bits in the pixels itself

B. MSE

Mean squared error is the average squared difference between a reference image and a distorted image [10].

$$MSE = \sum_{i=1}^{M} \sum_{j=1}^{N} (X_{i,j} - Y_{i,j})^2 \quad (1)$$

C. PSNR

Peak signal to noise ratio is the ratio between the reference signal and the distorted signal in an image [9, 10].

$$PSNR = 10 \log_{10} \left[\frac{{I_{max}}^2}{MSE} \right] dB \quad (2)$$

D. Histogram Analysis

Histogram analysis has been performed on original image and stego image to differentiate between both images. For more accurate analysis it is proposed to perform Histogram analysis on each channel separately.

VIII. Result Analysis

Table 5 shows the comparison of proposed algorithm with existing 7 algorithms. 1 bit and 2 bits are better in MSE and PSNR then proposed algorithm but capacity of proposed algorithm is better than all existing algorithms.

5KB of data has been taken for hiding in 512*512 size image. All Steganographic algorithms have been performed on same data and on same image size. It is observed that proposed algorithm is using less amount of image for hiding the same data. For hiding 5 KB data the algorithm takes only 2.50 % pixels of whole image and 1bit method takes 15.04 % pixels of the image. If requirement for Steganographic algorithm is high capacity and good MSE and PSNR then proposed algorithm could be used for this purpose.

IX. Conclusion And Future Work

Steganography has its own place in the field of security. Steganography used in an open-systems environment such as the Internet and Far-fetched applications, privacy protection, authentication, data integrity, intellectual property rights protection.

Proposed method is achieving highest capacity among all existing methods without any distortion in image. When proposed method has been performed on different images, it has given constant result but other existing methods gave different results on different images. Proposed method is secure and undetectable because of randomness.

In future, techniques to improve security for data hiding by using randomization will be used to extend this work.

TABLE V. RESULT ANALYSIS

	1 bit	2 bit	3 bit	4 bit	SCC	PIT	AAA	Proposed Algorithm
MSE	.0261	.062	.1646	.6216	.0259	.0611	.1060	.1606
PSNR	63.96	60.20	55.96	50.19	63.99	60.27	57.87	56.07
Capacity in percentage	15.04	7.52	5.01	3.76	5.01	7.52	3.00	2.50

REFERENCES

[1] S. Venkatraman, A. Abraham, M. Paprzycki,"Significance of steganography on Data Security", *International conference on Information Technology: Coding and Computing(ITCC'04)*, Las Vegas, 5-7 April 2004.

[2] K. Baily, K. Curran, "An Evaluation of Image Based Steganography Methods using visual inspection and automated detection techniques", Multimedia Tools & Applications, Vol. 30, No.1, pp. 55-88, July 2006, Springer.

[3] V. Lokeswara Reddy, A. Subramanyam, P. Chenna Reddy, "Implementation of LSB Steganography and Its Evaluation for Various File Formats" ,International Journal of Advanced Networking and Applications, Vol.02, Issue:05, pp.868-872, 2011

[4] Chen Ming, Zhang Ru, Niu Xinxin, Yang Yixian,"Analysis of Current Steganography Tools: Classification & Features", *IEEE International conference on Intelligent Information Hiding and Multimedia signal Processing (IIH-MSP'* 06) ,Pasadena, CA, USA, 2006.

[5] Adnan Abdul Aziz Gutub, "Pixel Indicator Technique For RGB Image Steganography", *Journal of Emerging Technologies in Web Intelligence, Vol.2 No.1, February 2010, Academy Publisher.*

[6] Mohammad Tanvir Parvez and Adnan Gutub, "RGB Intensity Based Variable-Bits Image Steganography", *APSCC 2008 – 3rd IEEE Asia Pacific Services Computing Conference, Yilan, Taiwan, 9-12* December 2008.

[7] Adnan Gutub, Ayed Al-Qahtani, AbdulazizTabakh," Triple-A: Secure RGB Image Steganography Based on Randomization*" IEEE International Conference on Computer System and Application, Rabat, May-June 2009*, pp.400-403

[8] Mamta Juneja and Parvinder Singh Sandhu, " Designing a Robust Image Steganography Technique Based on LSB Insertion and Encryption" , *IEEE International Conference on Advances in recent technologies in Communication and Computing , Kottayam, Kerela, 2009, pp.302-305*

[9] Amirtharajan, R., RambhatlaSubrahmanyam, Pakalapati J S Prabhakar, Kavitha, R, and Balaguru, "MSB over hides LSB - A dark communication with integrity", IEEE International Conference on Internet Multimedia Services Architecture and Applications, IMSAA 2011.

[10] Rengarajan Amirtharajan, K. Ramkrishnan, M. Vivek Krishna, Nandhini. J, John Bosco and Balaguru Rayappan, "Who decides hiding capacity? I, the Pixel Intensity, *IEEE International Conference on Recent Advances in Computing and Software System"(RACSS'12), Chennai 2012, pp-71-76.*

[11] Mehdi Kharrazi, Husrev T. Sencar, and NasirMemon" Image Steganography: Concepts and Practice*" WSPC/Lecture Notes Series: 9in x 6in, Institute of mathematical sciences, Singapore* April 22,2004

[12] M Amin, M. Salleh, *S. Ibrahim, M.R.K atmin, and M.Z.I. Shamsuddin,"* Information Hiding using Steganography", *4th National Conference on Telecommunication Technology Proceedings, Shah Alam, Malaysia*, 2003, pp.21-25.

[13] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Performance Study Of Common Image Steganography And Steganalysis Techniques", *Journal of Electronic Imaging Vol.15 No.4, Oct–Dec 2006, pp. 041104-1-15.*

[14] Saeed Sarreshtedari, Mohsen Ghotbi and Shahrokh Ghaemmmaghami, "On The Effect Of Spatial To Compressed Domain Transformation In LSB-based Image Steganography", *IEEE International Conference on Computer Systems and Applications* , 2009, pp.260-264.

[15] Hassan Mathkour, Batool Al-Sadoon, Ameur Touir, "A New Image Steganography Technique", *IEEE 4th International Conference on Wireless Communications, Networking and Mobile Computing*, 2008, pp. 1-4.

[16] Farhan Khan and Adnan Abdul-Aziz Gutub, "Message Concealment Techniques using Image based Steganography*", Department of Computer Engineering, King Fahd University of Petroleum & Minerals, Dhahran*,31261, Kingdom of Saudi Arabia

[17] HediehSajedi, Mansour Jamzad,"Cover Selection Steganography Method Based on Similarity of Image *Blocks", 8th International Conference on Computer and Information Technology Workshops, IEEE*, 2008, pp. 379-384.

[18] Yanming Di, Huan Liu, Avinash Ramineni, and Arunabha Sen," Detecting Hidden Information in Images : A Comparative Study", *Department of Computer Science and Engineering Arizona State University*, Tempe, AZ 85287,2005

[19] Li Zhi, Sui Ai Fen, "Detection of Random LSB Image Steganography", *IEEE 60th Vehicular technology Conference*, 2004, pp.2113-2117.

[20] Wien Hong and Tung-Shou Chen, "A Novel Data Embedding Method Using Adaptive Pixel Pair Matching", *IEEE Transactions on Information Forensics and Security, Vol.7,No.1,February 2012.*

[21] WeiqiLuo,Fangjun Huang and Jiwu Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited" , *IEEE Transactions on Information Forensics and Security, Vol.5, No.2, June 2010.*

[22] M. Khodaei and K. Faez, "New adaptive Steganographic method using least significant bit substitution and pixel value differencing" , IET Image processing , Vol.6, iss.6, pp 677-686, 2012