A Novel Steganography with Preserving Statistical Properties

Dr. Thamir Rashed Saeed
Department of Electrical Eng.- Unv. Of Technology/ Iraq
Electronic Design for Signal Processing Research Group
Ciphering Research Group

Abstract

In this paper a novel algorithm is present to improve the capacity and security of stegaography technique. Where, the proposed work are based on three stages, first one is checking the statistical performance of the cover image. Second stage is splitting the pixels of cover image depending on the pixels values (edges). Then , at the third stage replacement one or two bits of cover image with massage or not depend on the pixels values in second stage. The results were, appear the detection probability by statistical calculation is 0 - 7.65 % with capacity 30-60 % and false-negative ratio is 76.8% and with distortion is 1.1-1.5%. The improvement that satisfied is 7.8% , 2.56% and 20% respectively.

Keywords: *Steganography, LSB, Probability of Detection*.

1. Introduction

In the electronic era of revolutionary changes to the nature of information, and With the development of Internet technologies, digital media can be transmitted conveniently over the networks. Therefore, it is become difficult to confirm the safety or truth of data, due to the spread of tools used for distortion and manipulation and the capacity of some people to harness technology to serve malevolent ends[1,2]. Therefore, How to protect secret messages during transmission becomes an important issue[3], and this demand can be satisfied by hiding of the data that is, represent a key to safe communication[4]. That hiding can be in the content or form or, both, where, cryptography hides the contents of a secret message from malicious people, whereas Steganography even conceals the existence of the message[2,5]. The difference between steganography and cryptography is that steganography is a stealthy method of communication that only the communicating parties are aware of; while, cryptography is an overt method of communication that anyone understands, despite its payload is scribbled, and can use both of them in steganography. Where cryptography could use as a key of steganography[3,6].

2. Steganography

Steganography is the information hiding technique in which covering secured data into a computer carrier file without damaging the file or changing its size[4,7]. The purpose of steganography is covert communication-to hide the existence of a message from a third party[8]. Many different carriers file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points[9,10]. Stegaography contains a few branches as cryptography, Watermarking, Fingerprinting. The stego medium that a hidden message is inserted in it is called cover medium. It may be a picture, a sound, and a film. The image steganography algorithms can be categorized into two categories, spatial domain and frequency domain[11]. After inserting a message by Algorithm containing, it is called placed medium span (stego medium). The data that we insert in cover medium is secret message. The key that is used to insert message and take out secret message is called placing key. The techniques that help us to recognize cover medium and span are called disclosing[12,13].

The stego-process could be represented the following Formula[3,14]:

cover medium + embedded message + stegokey = stego-medium.

There are many embedded techniques, the Least Significant Bit (LSB) algorithm has a larger amount of capacity than other embedding techniques and it is recognized now, due to many advantages such as the algorithm is simple, the embedded velocity is fast and so on[2,11].

Image steganography systems have three conflicting conditions contend with one another: capacity, imperceptibility and robustness. Capacity refers to the amount of information that can be hidden in the cover medium, imperceptibility to an eavesdropper's inability to detect hidden information, and robustness to the number of modification the stego medium can withstand before an adversary can destroy that hidden informations[10]. There are three types of steganographic protocols used. They are Pure Steganography, Secret Key Steganography, and Public Key Steganography . The work of this paper is considered inside pure staganography.

In the existing technical literature, many related, studies on staganography have been reported. The researchers are focused on four axis, that are; the security[1,2,4,16], security and capacity[11,13,15], capacity and reduces the distortion[5,8,9,12,16,17,18], as;

In [1], two stages are made the work, first one is hidden a massage in a LSBs of the image. Then, the second is by hashing the cipher image using MD5 technique. While [7] use public key for hidden the massage in LSB, then, apply private key (RSA) for reconstruct the massage. By use particle swarm optimization for finding the best pixel locations to transfer the image to the new one was present in [4]. [2] was introduced a robust technique of hiding secret data in image based on LSB insertion and RSA encryption technique. For improving the security and capacity [13] was proposed a half tone picture method for secure the data communication. In [15] was combining the pixel-value differencing module and LSB for same demand. [11] is present a hiding massage in cover image by 3 LSB bits depend on the sequences of the massage bits. For reduce the embedding error and increasing the embedding capacity adaptive steganographic algorithm that use in [16]. Also [5] use fore-pixel difference and modified LSB to satisfy the same requirement. In [9] converting gray image to the RGB one to avoid gray color sequence and to declare the black region for hidden the massage in it. By shifting the word and synonym the test [8] was present a Steganography method. A steganographic technique based on genetic algorithm to find a near-beast structure for the pair-wise Least-Significant-Bit (LSB) matching scheme was presented in [12]. Improving LSB by decreasing the several changes in cover image by regarding to statistical properties of it was presented in [17]. In [18] a statistical properties of the cover image are taken before hidden the massage then adding a noisy bits in other location to rearrange the statistical properties after hiding a massage.

3. Proposed Algorithm

The most common and well-known steganographic method is called least significant bit (LSB) substitution, which embeds secret data by replacing k LSBs of a pixel with k secret bits directly. The human perceptibility has a property that it is sensitive to some changes in the pixels of the smooth areas, while; it is not sensitive to changes in the edge areas. Not all pixels in a cover image can tolerate, equal number of changes without causing noticeable distortion. Adaptive steganography which take care, about the important characteristics & statistics of the cover image.

The proposed algorithm based on the assumption that the intruder has full knowledge of the design and implementation details of the steganographic system. Also, its adopted according to statistics of image before, and after hiding the data.

3.1 Algorithm architect ;

For regarding the security with distortion, we must take care of the architect of the cover-image by taking the architect of the pixels as follows;

■ Divide the pixels into three groups:-

1- Whose value less than 6 (with respect to the most nibble)--LPC
2- Whose value less than 12 and greater than 6 (with respect to the most nibble)--MPC
3- Whose value greater than 12 (with respect to the most nibble)—HPC

■ The hidden data will be depending on the above groups as in flow chart in figure (1) where;

1. If the current pixel CP ∈ LPC no data will be hidden in that pixel.
2. If the current pixel CP ∈ MPC one bit of data will be hidden in LSB of the pixel.
3. If the current pixel CP ∈ HPC two bits of data will be hidden in LSB and beside it bits of the pixel.

Figure (2) represent the flowchart of data hidden in pixels.

■ Check number of pixels in MPC and HPC groups;

$$TNoP = Nop(MPC) + NoP(HPC) \qquad (1)$$

■ Number of data (bits) can hidden in the cover image is;

$$TNoB = Nop(MPC) + 2* NoP(HPC) \qquad (2)$$

■ Select a prime number which has primitive

numbers equal to TNoB

***3.2 The algorithm steps are**;*

1. The image size Mz= 209 X 270 =56430 pixels, of the image in figure(3-a)[18].
2. Splitting the image matrix into two matrices Mz1 and Mz0 according to the LSB of each pixels before hide the massage;
   Where:
   Mz1= 28221pixels ,(LSB =1)and
   Mz0=28209pixels , (LSB =0).
   Then
   Splitting the image matrix into two matrices M2z1 and M2z0 according to the beside of LSB (bit number 2) of each pixels before hide the massage;
   Where:
   M2z1= 28141pixels ,(bit no. 2=1)and
   M2z0=28289pixels , (bit no. 2=0).

3. Splitting the image matrix into two matrices MM87 and MM76 according to the bits 8,7 and bits 7,6 of each pixels before hide the massage;
   Where:
   MM87= 4216 pixels , (bits 8, 7 =1)and
   MM76= 8850 pixels , (bits 7, 6 =1).

4. Hid two bits in LSB(bit 1,2) for the pixels in MM87 group, and one bit in LSB for the pixels in MM76 group.
5. Maximum text (massage or data) which can be hiding according to the proposed algorithm is 17282 bits (2.160) Kbyt.
6. Text (massage) size Tz =463 bytes (3707 bits).
7. The massage bits hidden distribution by nonrepated randomly to the LSB and LSB+beside according to bit 8,7 and bit 7,6 as ;
   Pixel No. which hides the bit of massage in LSB or LSB+its beside is
   $$PHB = a^i \bmod p \qquad (3)$$
   Where;
   a- Primitive root of prime p
   $0 \leq i \leq p$-1
   P- prime number which has primitive root numbers equal to the message size.
8. Then splitting the image matrix as in step 2 after hiding a text. At this step its clear the number of pixels which have LSB equal one and zero are different from that before the hidden a text. This means the distortion can be detected.
9. To overcome the above weakness, determine the difference of the number of pixels which have a one and zero at LSB and beside bit from the pixels which not have a text.
10. Add one's and zero's to that pixel to satisfy the numbers in step 2, the cipher image as in figure (3-b)

3.3 Probability calculations:

The probability of any bit in a binary number is;

$$P(b)_n = ½ \qquad (4)$$

Where;

b – bit in binary number.
n- No. of bits for that binary number.

The probability of any bits in a binary number is;

$$P(b)_n=P(b1)*P(b2)*\ldots P(b_N)=½*½*\ldots.*½ =\frac{1}{2*N} \qquad (5)$$

$$\therefore for\ two\ bits$$

$$P(b1and\ b2) = \frac{1}{2*2} = \frac{1}{4} \qquad (6)$$

Probability of certain number in the matrix is;

$$P(N)_m = \frac{the\ frequency\ of\ that\ number}{total\ matrix\ number} \qquad (7)$$

$$\therefore for\ two\ bits\ in\ certain\ number\ in\ matrix\ is$$

$$P(bM) = P(b1and\ b2) * P(N)_m \qquad (8)$$

The true-positive rate the probability that an image detected by Stegdetect really has steganographic content—as follows [19];

$$p(S|D) = \frac{p(S).P(D|S)}{P(D)} = \frac{P(S)\ .\ P(D|S)}{P(S).P(D|S)+P(\neg\ S).P(D|\neg\ S)} \qquad (9)$$

Where

P(S) - probability of steganographic content in images,

P(¬S) - complement of P(S)

P(D|S) - probability that we'll detect an image that has steganographic content,

P(D|¬ S) is the false-positive rate. Conversely,

$$p(\neg D|S) = 1 - P(D|S) \qquad (10)$$

Where;

$p(\neg D|S) -$ false-negative rate.

The probabilities with and without the proposed algorithm and for ref. [11] are shown in table (1).

Table (1) measurements f the proposed algorithm

Measurements algorithm	Destortion %	PD by Human Vision	PD by Statistical	False-nagaitive ratio	Capacity
Without Proposed Algorithm	0.39% - 100%	≈ 0	100 %	0	100 %
With Proposed Algorithm	1.1% -1.5%	≈ 0	≈ 0 % - 7.65 %	76.8%	30 -60%
Ref. [11]	30%	≈ 0	~ 60%	30%	30-60%

4. Results:

From the results in Table (1), many strength points can be see, the distortion is reduces because the statistical properties are taken into account and the probability of detection as in that table and Figure (4) are improved about other algorithms. While, the capacity is not high with this algorithm because this algorithm was, focuses on the reduces the distortion and increase the security, but at the same time, it's not bad. The preference of this work with respect to the previous [18] in the false-negative ratio by 20%.

5. Conclusion

Often the statistical analyzed of stego- image which reflects or show the presence of certain hidden data in the image .In our proposed algorithm, who overcome this weakness of the steganographic system cause reduce the statistical detection, to reduce the distortion and increase the capacity by use hidden in LSB or LSB+beside bits of the image pixels depends on the value of pixel. Also, the detection rate weakness was overcome, by non-repeated, which the probability of detection nearly equal to zero.

However the two strength points in proposed algorithm are inversely related and depend on the text (massage) size. Where the text size decrease the non–repeated distribution factor effect on detection will reduce, and the adding noisy data to re-statistical of an original image factor effect will increase and the capacity will decrease, and vice versa. We examine our work by wifi internet network for many cases and get same results with the improvement which satisfied is 7.8% , 2.56% and 20% for probability of detection, false negative ratio and distortion respectively with respect of ref. 19. The weakness of this algorithm is still the capacity and we will overcome it in the next paper.

References

[1] Mohammad A. Ahmad, Dr. Imad Alshaikhli, Sondos O. Alhussainan, "Achieving Security for Images by LSB and MD5", Journal of Advanced Computer Science and Technology Research Vol.2 No.3, Pag., 127-139, September 2012.

[2] Emad T. Khalaf and Norrozila Sulaiman, "A Robust Data Hiding Technique based on LSB Matching", World Academy of Science, Engineering and Technology 58 2011.

[3] Jayeeta Majumder and Sweta Mangal, " An Overview of Image Steganography using LSB Technique", National Conference on Advances in Computer Science and Applications with International Journal of Computer Applications (NCACSA 2012).

[4] Parisa Gerami, Subariah Ibrahim and Morteza Bashardoost, " Least Significant Bit Image Steganography using Particle Swarm Optimization and Optical Pixel Adjustment", International Journal of Computer Applications (0975 – 8887) Volume 55– No.2, October 2012.

[5] Xin Liao, Qiao-yan Wen, Jie Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution", ELSIVER, J. Vis. Commun. Image R., 2011.

[6] Youssef Bassil, "Image Steganography Method Based on Brightness Adjustment", Advances in Computer Science and its Applications (ACSA), ISSN: 2166-2924, Vol. 2, No. 2, 2012.

[7] Arpan Ghorai, Dibyendu Chowdhury and Satyajit Das, "Design and Implementation of Public Key Steganography", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[8] Sharon Rose Govada, Bonu Satish Kumar, Manjula Devarakonda, and Meka James Stephen, " Text Steganography with Multi level Shielding", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 3, July 2012.

[9] Nitin Jain, Sachin Meshram, and Shikha Dubey, "Image Steganography Using LSB and Edge – Detection Technique",International Journal of Soft

Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3, July 2012.

[10] Ashish kumari , Shyama Sharma , Navdeep Bohra," Implementation of IMAGE STEGANOGRAPHY Based on Random LSB", IJCSMS International Journal of Computer Science and Management Studies, Vol. 12, Issue 01, January 2012.

[11] Gandharba Swain, and Saroj Kumar Lenka, " A Technique for Secret Communication Using a New Block Cipher with Dynamic Steganography", International Journal of Security and Its Applications Vol. 6, No. 2, April, 2012.

[12] M. Soleimanpour, S. Talebi and H. Azadi-Motlagh, " A Novel Technique for Steganography Method Based on Improved Genetic Algorithm Optimization in Spatial Domain", Iranian Journal of Electrical & Electronic Engineering, Vol. 9, No. 2, June 2013.

[13] Amin Hashemi Pour, and Ali Payandeh, "A New Steganography Method Based on the Complex Pixels", Journal of Information Security, 3, 202-208, 2012.

[14] Manish Mahajan and Navdeep Kaur, " Adaptive Steganography: A survey of Recent Statistical Aware Steganography Techniques", I. J. Computer Network and Information Security, 10, 76-92, Sept. 2012.

[15] Manjunath Gadiparthi, Keshav Sagar, Divya Sahukari and Rakesh Chowdary, "A High Capacity Steganographic Technique based on LSB and PVD Modulus Methods", International Journal of Computer Applications (0975 – 8887), Volume 22– No.5, May 2011.

[16] Yeuan-Kuen Lee, and Ling-Hwei Chen, " An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement", 1999.

[17] Kazem G., Shahrokh G. and Saeed R. "LSB^{++}: An Improvement to LSB^{+} Steganography", IEEE TENCON Conf. Pag. 364-368, Bali, 2011.

[18] Thamir R. Saeed and Shaymaa Abd-Elghany, " EFFICIENT ADAPTIVE STEGANOGRAPHY ALGORITHM", Accepted for publication in International Journal of Pure and Applied Research in Engineering and Technology, 2013

[19] N. Provos and P. Honeyman, ”Hid and Seek: An Introduction to Steganography,” *IEEE Security and Privacy* , Vol. 1 Issue 3, Pag. 32-44, 2003.

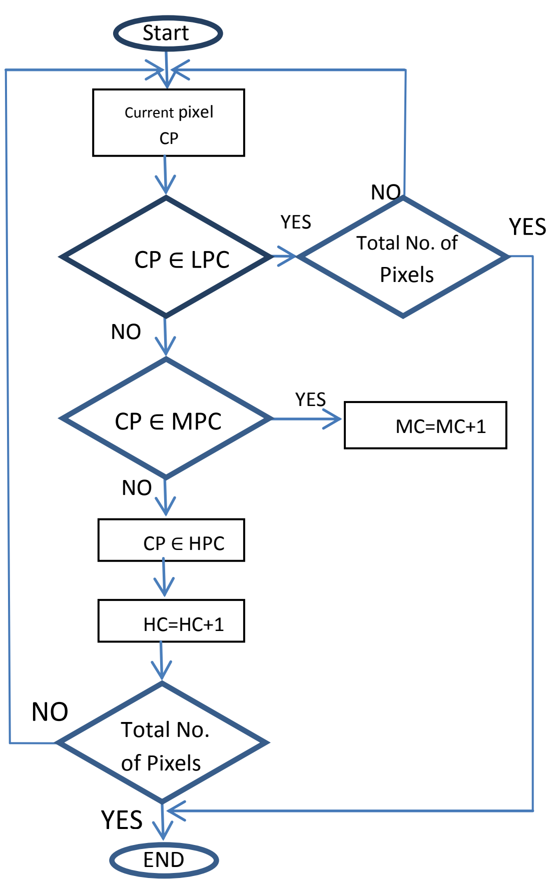


Figure (1) The architect of the cover-image pixels

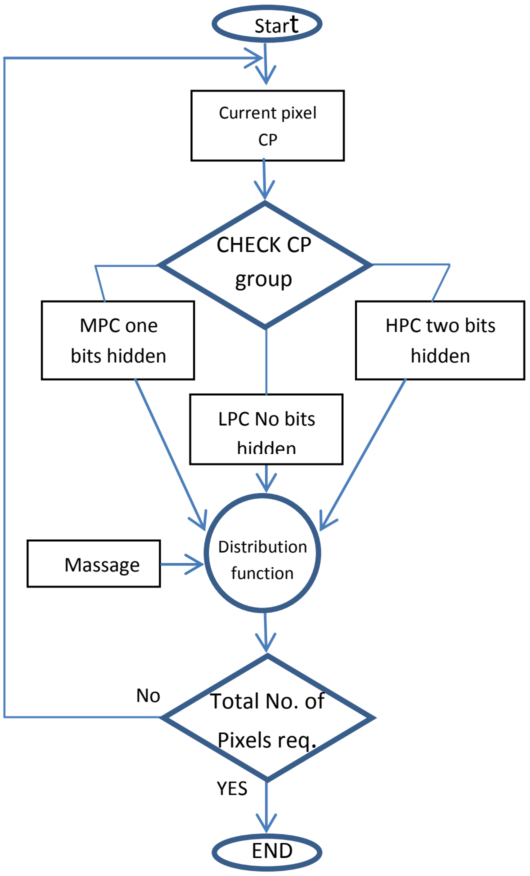


Figure (2) The flowchart of proposed algorithm

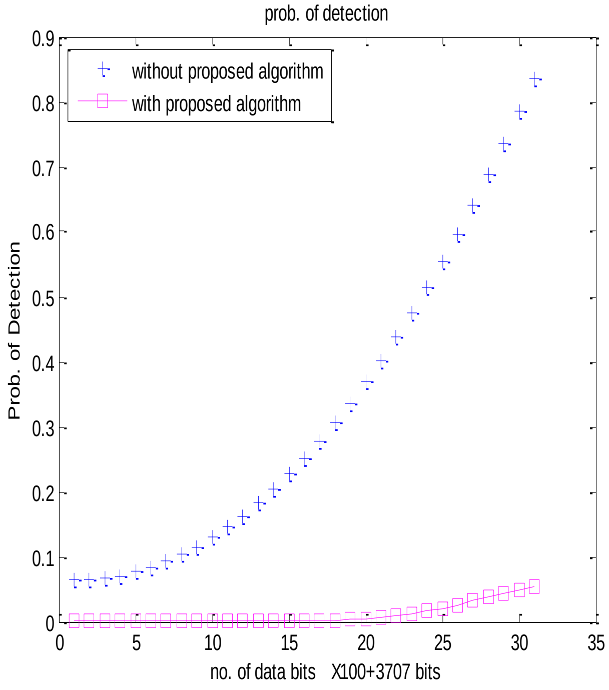
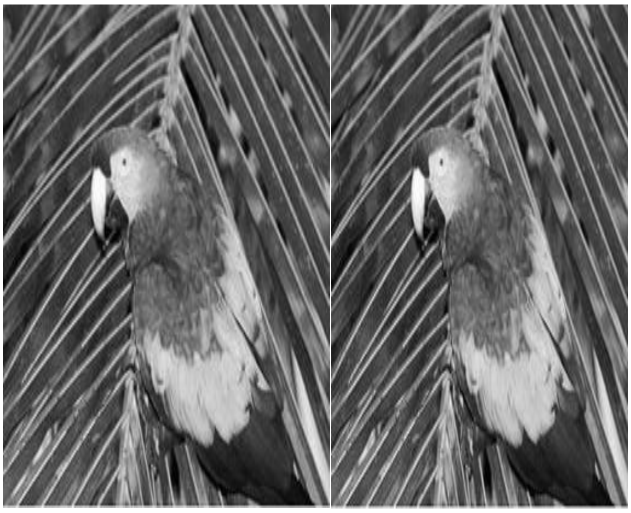


Figure (4) Prob. Of Detection with and without a proposed Algorithm



a-before hiding text

b-after hiding text

Figure (3) Cover-Image before and after hiding text