The International Journal of Engineering and Science (IJES)
|| Volume || 8 || Issue || 11 || Series I || Pages || PP 58-63|| 2019 ||
ISSN (e): 2319 – 1813 ISSN (p): 23-19 – 1805

Optimal Area Algorithm For Data Hiding In Digital Image

Abdulkreem Mohammed Salih , Baraa T. Sharef, Fahad LaythMalallah
Al-Dour Technical Institute-Northern Technical University
Department of Information Technology.Collage of Information Technology, Ahlia University, Manama, Kingdom of Bahrain,
Computer and Information, College of Electronics Engineering, Ninevah University, Mosul, Iraq,

----------ABSTRACT----------
Digital information hiding is the art of hiding the information in digital media. The method of information hiding plays an important role in the field of digital communication and the information security, as the transmission of information over the Internet has a possibility to be stolen from the third party. One of the solutions is embedding the information so that the target message will not be known to repel the attention of the thieves. In the proposed algorithm, hiding operation will be based on finding the optimal area for inserting the target message in a cover image using spatial domain by finding which part of cover image similar with the message data in level of bits. The proposed algorithm is able to achieve the improtant criteria of steganography, as well as security objectives were enhanced by the proposed algorithm especially by adding secret keys to the hiding operation, thus, the image quality of the stego image improved due to decreasing the number of original pixel modification during the message insertion.The proposed optimal area algorithm shows a significant result comparing with the experiments without using the optimal area algorithm.
Keywords: *Steganography, Information Security, LSB, Optimal Area, Mark Image.*

Date of Submission: 28-10-2019 Date Of Acceptance: 16-11-2019

I. INTRODUCTION

The Internet and digital data are one of the most important factors in communication and information technique. Message transmissions through the Internet have some issues in terms of protection, such as copyright protection and data security[1]. Therefore, designing a safe communication method to transmit messages through the Internet is considred as main challenge in the current researches. Cryptography as encryption with decryption data is one way of these methods, encryptions operation makes the target message suspicious enoughto attract eavesdroppers, while Steganographic techniques [2] overcomesthis issue by hidng the secret information in a cover image [3].Steganography can be defined as the art of invisible communication. This is implemented through hiding the information inside other information, thus hiding the existence of the communicated information. The word Steganography is derived from two-word, first word "STEGO" meaning "cover" and "GRAFIA" meaning "writing" [4] then defining as "covered writing". In image Steganography the information is hidden in a cover image. Steganography typically is utilized on computers since the digital data are sent and received [5]. There are two types of data hiding strategies; spatial domain strategies and frequency domain strategies. In the spatial domain [5]the inserting of message bits into the image is not only achieved in the least bit but also other bits in the pixel are utlized in a random manner. In [6], the secret messages are inserted into image pixels directly. In [7, 21] using the logical operation, algorithm embedded MSB of secret image in to LSB of cover image. The work as in [8] combines three operations in one processing step, these operations are compression, data hiding and partial encryption of images,where the data embed into the image according to the message size and partially encrypt the image and the message. Other papers focusedon the frequency-domain. In [9] the image is transformed to frequency domain, and then the messages are embedded in the transformed coefficients. In paper[12] data hiding is applied by a novel joint data-hiding and compression scheme for digital images using side match vector quantization (SMVQ) and image inpainting. lossless, a reversible, and a merged data hiding methods for images encrypted using public key in [13].The work in [14] proposes a novel coverless information hiding method based on MSIM, which utilizes the average value of sub-image's pixels to represent the secret information.

The rest of this paper is organized as follows:Section 2 views Optimal Area Substitution. Section 3 explains the Criteria of Steganography. In Section 4 the Embedding processing is described. Then, the expermental results and conclusion are discussed in Section 5 and 6 respectively.

1. Optimal Area Algorithm

The idea of Optimal Area Algorithm means redistributing the message data in the cover image in a way that depends on the selection of areas which contains the largest number of similarities between their data and message data. In optimal area substitution steganography, the message data is divided into eight sections, and the cover image is divided into eight sections. For each section of the message, the search algorithm finds a more relevant section (more similarity in bits between the message bits section and the cover image section). The similarity algorithm relies on comparing the bits of the message and the bits in pixels in the cover image. As shown in Table 1, let a 16-pixel image where each pixel is a byte representation, and the message bits contains 16 bits. To hide the binary value of message (1010110110101101), we will insert the message bits that are going to be inserted in the cover image pixel, Second position of pixels will used for insertion message data.First part of the message bits compare with each section in cover image,the comparison includes finding numbers of similar bit between them which called similar factor, at end choose the max similar factor,nthe section has maximum similar factor used for insertion the current section of message data.This procedurerepeated for other parts of the message data segments. The similarity factor (a pointer to the similarity between the message bits and the second bit of pixels in the cover image, for each similarity counter will increase by one). In this way, the number of bits that are changed in the image pixels will be reduced when the similarity occurs, where the pixel value will remain during insertion of the message bits.Key generated in Table(2) is(14825736) means that first section of message data will insert in section (1) of cover image, second section of message data will insert in section (4) of cover image, third section of message data will insert in section (8) of cover image , fourth section of message data will insert in section (2) of cover image , fifth section of message data will insert in section (5) of cover image , sixth section of message data will insert in section (7) of cover image , second section of message data will insert in section (4) of cover image , seventh section of message data will insert in section (3) of cover image,and last eighth section of message data will insert in section (6) of cover image.

Table1: Example for Optimal Area Substitution

Type	Pixel Image	Section No. of Cover Image	Message Sequence Bit	Similarity Factor	Total No. of Similar Bits	Sequence for Insertion
Without Using Redisbuted Algorithm	10010110	1	1	6	6	1
	01101101		0			
	10110101		1			
	11011110		0			
	01110101		1			
	10010010		1			
	10100010		0			
	10000001		1			
	10110101		1			
	01101101		0			
	10010000		1			
	11011110		0			
	10110101		1			
	10000101		1			
	00110111		0			
	10110011		1			
Using Redisbuted Algorithm	10010110	Part(1)	1	2	13	Part(1)
	01101101		0			
	10110101	Part(2)	1	2		Part(4)
	11011110		0			
	01110101	Part(3)	1	2		Part(8)
	10010010		1			
	10100010	Part(4)	0	2		Part(2)
	10000001		1			
	10110101	Part(5)	1	1		Part(5)
	01101101		0			
	10010000	Part(6)	1	1		Part(7)
	11011110		0			
	10110101	Part(7)	1	1		Part(3)
	10000101		1			
	00110111	Part(8)	0	2		Part(6)
	10110011		1			

2. Criteria Of Steganography

Three important factors are used to measure the acceptability of the Steganogaphy algorithm [10] these factors discussed in the following:

1- Steganography image quality:it can be measured by finding the Peak Signal to Noise Ratio value PSNR[10][11]as shown in Eq. (1):

$$\mathrm{PSNR} = 10\log 10\ 2552/\mathrm{RMSE}(1)$$

Where, the RMSE is root mean square error and equal to:

$$\mathrm{RMES} = 1/(\mathrm{M} * \mathrm{N})\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - f(i,j)]^2}(2)$$

Where,M and N are image dimensions (number of pixels) (M=N). When the changed bits reduce between the cover image and stego image(cover image after insertion), the PSNR will enhancement.

2- Security:it is indicating that the hidden bytes can not be detected, or the steganography method can not be discovered[15]. A secret key is added to the algorithm and the key arenumbers representthe index sections in the cover image that contain the section message bit sequently, for example in Figure 1 is (214825736). The first digit (2) in key is indicator for position of insertion bit in pixel and the other digits (14825736) are asequence of indexed section for cover image.

3- Robutness and Capacity:Robutness is a measurement of immunity from attacks and the capacity is measurement of how message data can be hidden in the cover image [19][20].

3. Embedding Processing

The proposed Steganography algorithm consists of the following processes as shown in Figure(1) andthese processes explain the procedure:

1- Spatial domain is used for cover image.
2- Divide cover image intoeight sections pixel.
3- Divide the message into eight sections as well.
4- For each section of message, the following steps have to be performed:
a) Find number of similarity bit with each section of cover image.
b) Choose the section that have the largest similarity bit.
c) Store the index nubmer of cover image section that have large similarity bits
d) Insert bit section of message in pixel of choosen section from cover image.
5- Take the stored indexed number and used it as a secret key.

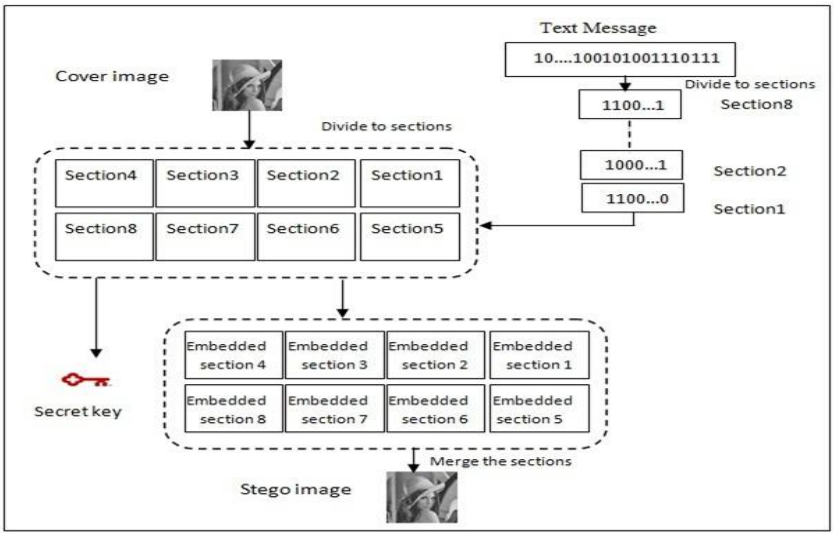

Figure (1) Embedding Processing

4. Expermental Results

Digital gray scale images of size (512*512) are used as a cover image in our proposed optimal area algorithm. In other side a message of size 128 kilo bits used for insertion in these images. Message bits divided into eight sections and each section contain 16 kilo bits. Moreover, cover image converted to asequence of eight sections. Two results are obtained, first results applied without using our proposed redisbuted algorithm as shown in table(1)

Table 1: Cover Gray-Image(512*512) & Msg 128 kilo bits (without our proposed algorithm)

Image	PSNR(db)	Secret Key	No. of Similar Bits
harbour	48.1332	2	65501
boat	48.1337	2	65509
airfield	48.1623	2	65939
barbara	48.1287	2	65433
bridge	48.0652	2	64468
goldhill	48.1472	2	65712
lena	48.1207	2	65313
peppers	48.5449	2	65421
Sailboat	48.5609	2	66093

While the second results by using the proposed optimal area algorithm as shown in table(2).

Table 2:Cover Gray-Image(512*512) & Msg 128 kilo bits (using distributed algorithm)

Image	PSNR	Secret Key	No. of Similar Bits	Increasing Rate in Similarity
harbour	48.1579	216825743	66123	0.9%
boat	48.1355	262714358	65698	0.3%
airfield	48.1653	276482153	66190	0.4%
barbara	48.1641	261587324	66190	1.2%
bridge	48.0805	265134278	64749	0.4%
goldhill	48.1736	217358246	65961	0.4%
lena	48.148	286153742	65987	1.0%
peppers	48.5767	271253864	66198	1.18%
Sailboat	48.7384	217345268	66759	1.0%

Secret key is obtained from position number of bit insertion (second bit) and the sequence of section insertion for example the secret key for harbour image mean that the first section cover image used for insertion the message data is section one, the second section is section six ,third section is section eight, …etc.

Increasing rate in similarity means the amount of increasingin similarity in bits of message and bits of cover image when using optimal area algorithm and without using it.The significant improvement can be seen in Figure (2).

Where asfigure (3) shows the significant results obtained by the propsed algorithm in variant PSNR For Images.

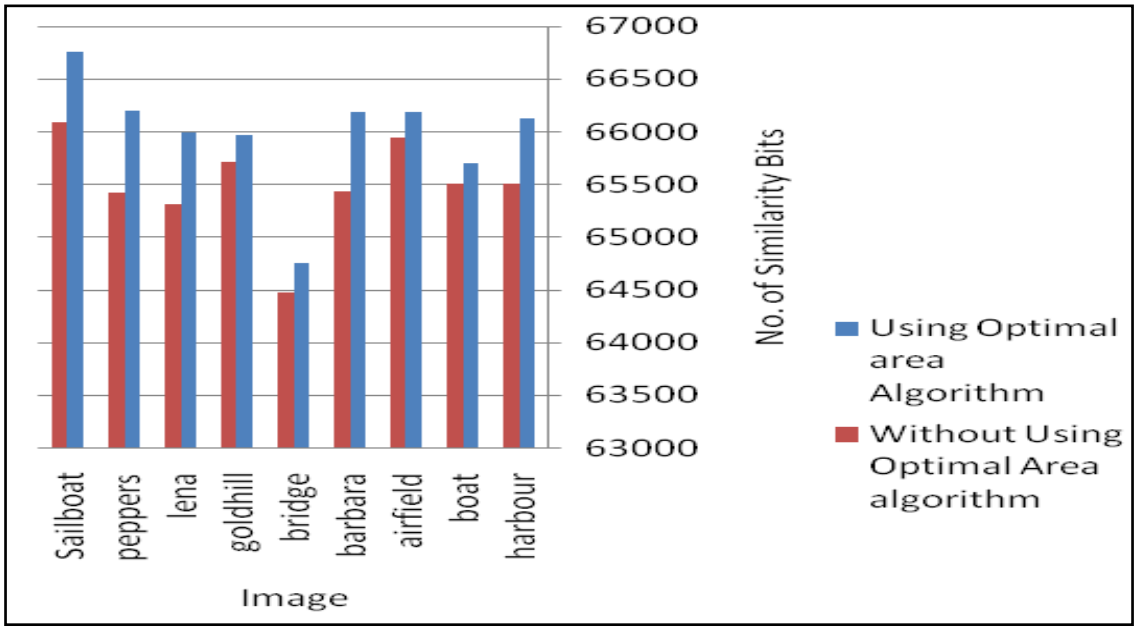

Figure 2: Variantincreasing of Similarity in Bits

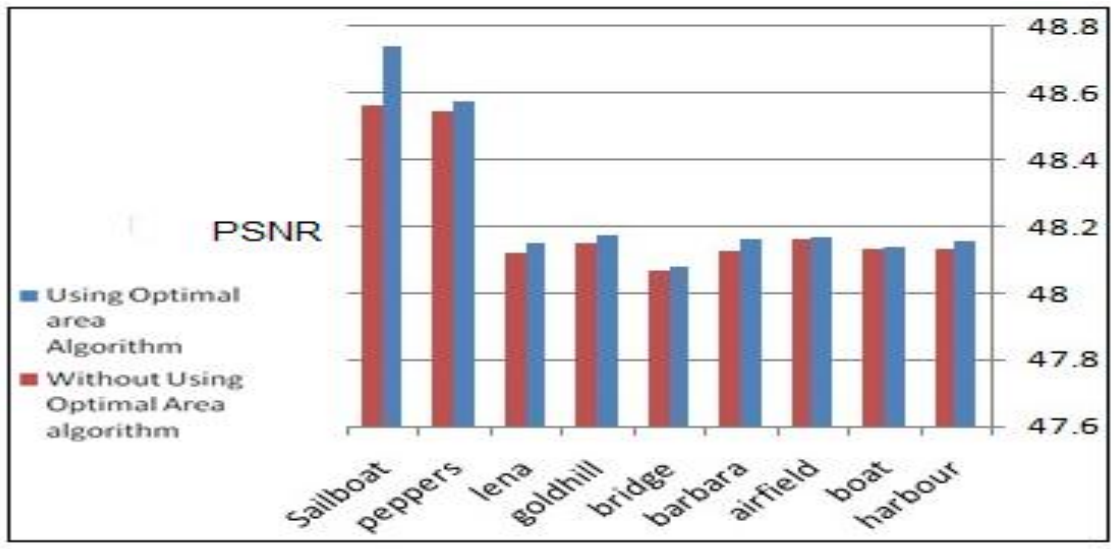

Figure 3: Variant PSNR in Images.

In Table(3) acomparsion between proposed algorithm with other papers by evualtion the value of PSNR for cover image, where these compared papers depended in Lena image as a standard image.

Table 3: Comparison of the proposed method (value of PSNR)

Image	Proposed algorithm	[9]	[16]	[17]	[18]
lena	48.148	40.08	40.783	40.69	38.37

II. CONCLUSION

The proposed algorithm focused on enhancement the criteria of stegography. The optimal area for insertion was the basis of the algorithm. By using the optimal area, the number of similarity bit increased after finding and choosing the optimal area for insertion, in this way the cover image will not be distributed significantly by the embedded signal. Many of benefits will be obtained, first one the value of PSNR will be increased since this value depend on the similar between cover image(before insertion message) and stegography image (after insertion message). As shown in table(1) and table(2) the value of PSNR increased

when using the propsedalgoritm. Security factor also increased by adding a secret key between sender and reciever, this secret key consists of numbers that indicate the order of the sections in which the message bits are inserted. The strength of the secret key is clear in both cases as shown in the table (1) and table (2). Increasing the rate in similarity value varies depending on the nature of the data in the message and the values of the cover image.

REFERENCES

[1]. T. Liu and Z. D. Qiu, "The survey of digital watermarking-based image authentication techniques," in Signal Process., Vol. 2, pp. 1556–1559, 2002.

[2]. D. Artz, "Digital steganographic: Hiding data within data," IEEE Internet Comput., Vol. 5, No. 3, pp. 75–80, 2001.

[3]. Ch. Yang, Ch. Weng, and Sh. Wang," Adaptive Data Hiding in Edge Areas of Images With Spatial LSB Domain Systems", IEEE Transactions ON Information Forensics and Security, Vol. 3, NO. 3,pp. (488-497), 2008.

[4]. H. Wang, Sh. Wang, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, Vol. 47 No. 10, pp. 76-82, 2004.

[5]. O. Mohammad ," Hiding Data in Images Using New Random Technique",IJCSI International Journal of Computer Science Issues, Vol. 9,pp.49-53, Issue 4, No 2, 2012.

[6]. C.Y. Yang, "Color Image Steganography based on Module Substitutions", Third International Conference on International Information Hiding and Multimedia Signal Processing Year of Publication: ISBN: 0-7695-2994-1, 2007.

[7]. V. Sharma , V. Shrivastava," A Steganography Algorithm For Hiding Image in Image By Improved LSB Substitution By Minimize Detection " ,Journal of Theoretical and Applied Information Technology, 15th February. Vol. 36 ,No.1, 2012.

[8]. W. Puech , "Image Encryption and Compression for Medical Image Security", Proceeding of IEEE Image Processing Theory, Tools and Applications, pp. 1–2, 2009.

[9]. Xin Liao, K. Li , and J. Yin, "Separable data hiding in encrypted image based on compressive sensing and discrete fourier transform",Multimedia Tools and Applications,Vol. 76, Issue 20, pp. 20739–20753, 2017

[10]. N. Batra , and P. Kaushik, " Data Hiding in Color Images Using Modified Quantization Table", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), Vol. 1, Issue 8, October 2012.

[11]. D. Saravanan, A. Doni , and A. Ajith," Image Information Hiding: An Survey", The SIJ Transactions on Computer Science Engineering and its Applications (CSEA), Vol. 1, No. 1, March-April 2013.

[12]. D. Qin, Ch Chang," A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting ", Ieee Transactions On Image Processing, Vol. 23, No. 3, March 2014.

[13]. X. Zhang, J. Long, Z. Wang, and H. Cheng,"Lossless and Reversible Data Hiding in Encrypted Images with Public Key Cryptography", IEEE Transactions on Circuits and Systems for Video Technology,Vol. 26 , pp.1622-1631 Issue: 9 , 2016.

[14]. Y. Cao,Z. Zhou, and Ch. Gao" Coverless Information Hiding Based on the Molecular Structure Images of Material", Tech Science Press,Vol. 56 , Issue: 2 ,pp.197-207, Issue: 9 , 2018.

[15]. A. M. Salih, S. H, Mahmood " Digital Color Image Watermarking Using Encoded Frequent Mark", Journal of Engineering, Baghdad University, Vol. 25 , Issue: 3 , pp.81-88, 2019.

[16]. N. Mohammed, N. Bibi , and I. Qasim " Digital watermarking using Hall property image decomposition method", Pattern Analysis and Applications, Vol. 21 , Issue: 4 , pp.997-1012, 2017.

[17]. N. Mohammed, N. Bibi ,"Digital image watermarking using partial pivoting lower and upper triangular decomposition into the wavelet domain", IET Image Proc 9(9):pp. 795–803,2015.

[18]. M. Ali, CH. Ahn ,"An optimized watermarking technique based on self-adaptive DE in DWT–SVD transform domain",Signal Process, Vol. 94, pp. 545-556 , 2014.

[19]. M. K. Hossen, S. Sarker , and Md. CH. Azad ," Hybrid Digital Watermarking Scheme Based on Discrete Wavelet Transform for Copyright Protection ",Advancement in Image Processing and Pattern Recognition, Vol. 1,Issue 2, pp. 1-10 , 2018.

[20]. A. M. Salih," Secured Watermarking Image Using Spread Spectrum", Tikrit Journal of Engineering Sciences,Vol. 23 , Issue: 3 ,pp.71-78, Issue: 9 , 2016.

[21]. F. L. Malallah, et al., "Hiding Secret Text inside a Dynamic Handwritten Signature as Steganography Application.", The Scientific Journal of Cihan University– Sulaimanyia (SJCUS), dx.doi.org/10.25098/1.1.111, Vol 1- Issue 1, 2017.

Abulkreem Mohammed Slaih" Optimal Area Algorithm For Data Hiding In Digital Image" The International Journal of Engineering and Science (IJES), 8.11 (2019): 58-63