JOURNAL OF THEORETICAL PHYSICS & CRYPTOGRAPHY

www.IJTPC.org/Publications

Steganography Method Based On Variable Bit Rate(VBR)

Fariba Ghorbany Beram
Sama Technical and Vocational, Training College Islamic Azad University, Shoushtar Branch, Shoushtar, Iran.

ABSTRACT

Steganogeraphy is the science and art of concealing secret information. The purposes of Steganogeraphy is security,resistance and transparency. In this field there are the methods of place scope and changing scope. The methods of changing scope highten the resistance of Steganogeraphy algorithms. The host media under changing is applied for changing the wavelet and a result a lot of coefficient are prodced. A kind of technique in this article is presented which uses the afore mentioned techniques in statum shape and its result provides the mentioned purposes. The coefficients in the suggested method are clustered in such a way that the changing scope of coefficients not to be changed before and after the placing. Since the scope of coefficient is unsteady they involve a bit rate into themselves that causes capacity increasing. Not using the fixed bits brings about increasing security. The coefficients originsted from converting wavelet based on suggested technique change in a way that is nearly consistent with the human's visual system. Becausw the change originated from placing the secret information in the image to felt less. The implementation findings show that the suggested technique has improved the objectives of Steganogeraphy in comparison to the other present methods.

Keywords

Steganography, wavelet transform, coefficients, vbr.

1. Introduction

The modern physics, Conceal information security in various fields in recent years gained a lot of attention [1]. steganography is one of the techniques that can secure admission for transfer of confidential information provided. The term steganography is Greek word (meaning cover) and graphy (writing) are shown[2]. Some researchers believe that science steganography And a number of art it is known[3]. This is perhaps the best definition of the steganography Is a combination of science and art. have presented it as some resources steganography : is the art and science of secret communication, in which the secret message in a cover media so that there is no hidden message is undetectable [4]. Invisible inks in the past been one of the most common techniques for steganography [6]. The general procedure for steganography can be expressed, is shown in Figure 1.

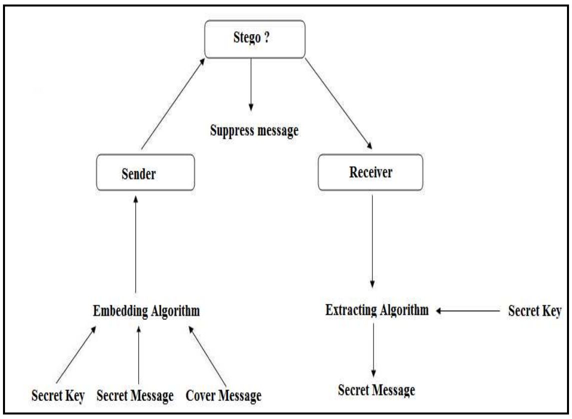

Figure 1 - General Procedure's steganogeraphy (6)

2. The proposed method

Media that are used in steganography include audio, video, image, etc. In this study we image the media outlets either use masking confidential data. In the proposed method, the combined spatial and transform domain techniques. Each domain methods into the field where there are features which will be discussed later. In the proposed method, the least bit of simple placement of confidential information obtained from wavelet coefficients is used. Steganogeraphy algorithm consists of two stages placement of confidential information on the object carrier and extract information from the object they are carrying. The presented method describes the overall block diagram of Figure 2. In this method, the sender selects the host image and the message is placed in the proposed algorithm.

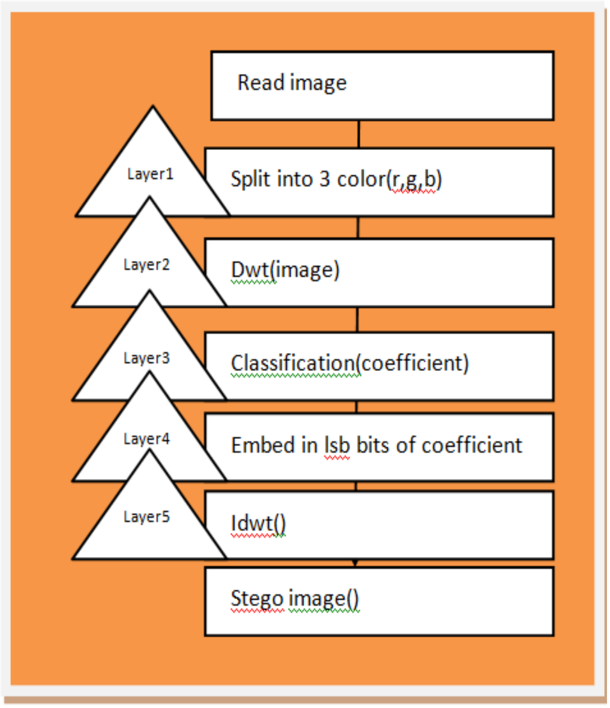
Read image
Layer1
Split into 3 color(r,g,b)
Layer2
Dwt(image)
Layer3
Classification(coefficient)
Layer4
Embed in lsb bits of coefficient
Layer5
Idwt()
Stego image()

Figure 2-block diagram

Layer technique is proposed:

First layer: Divided into three sub-band image is colored red, green, blue.

Second layer: wavelet transform of each of the three color bands are used.

third layer: classification coefficients of wavelet transform.

Fourth layer: Low valuable bits of embedded secret information in the clustering coefficients.

The fifth layer:invert discrete wavelet transform from the coefficients.

The first layer :

The image is composed of pixels. Each pixel is marked with a number, so the computer image as a collection of figures in various areas of the picture, replaced by different intensities of light. A series of multi-bit per pixel. The number of bits in the color scheme, the bits are called. Digital color images to a specific twenty-four bits are stored in files and color models RGB, which is known as the main color, are used. All twenty-four-bit color of the pixel image of the three primary colors red, green and blue are derived (Figure 3). The image is composed of pixels. Each pixel is marked with a number, so the computer image as a collection of figures in various areas of the picture, replaced by different intensities of light. A series of multi-bit per pixel. The number of bits in the color scheme, the bits are called. Digital color images to a specific twenty-four bits are stored in files and color models RGB, which is known as the main color, are used. All twenty-four-bit color of the pixel image of the three primary colors red, green and blue are derived (Figure 3). The combination of these three colors in each pixel of a twenty-four-bit binary number that is eight bits of red, eight-bit byte of blue and green are related. Image steganography, by changing the system, which operates pixel values. The human visual system is not sensitive to slight discoloration. steganogeraphy weakness of the human visual system has to recognize small changes and puts the secret message in images (7).

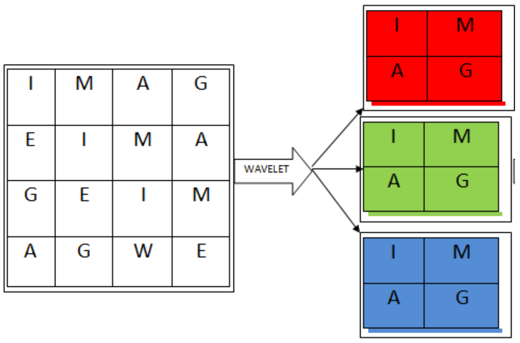

Figure3 - resolution color image sub-bands of red, green, blue

The second layer:

The media have become the first carrier to convert the field amplitude (Figure3). It may become the discrete cosine transform , Fourier or wavelet , then the secret message in the conversion coefficients , the coefficients of the inverse transform is taken of placement and (8) . Recently in the field of steganography algorithms have been proposed , using wavelet transform has received much attention . Haar wavelet was introduced first by the personal name . Haar wavelet transform into different types , one of which is wavelet (9). Haar transform wavelet due to the simplicity of implementation and speed of implementation, it is very popular (10).

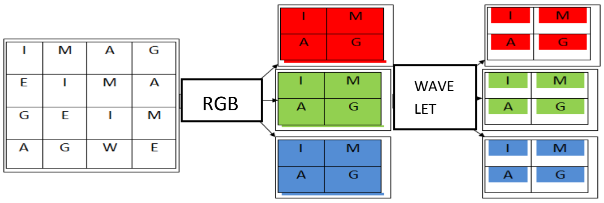

Figure 4 - Getting the wavelet transform of each of the color bands

Wavelet 2, has two steps:

The first stag, the pixels are scanned from left to right in the horizontal direction and the sum of neighboring pixels to the left and subtract neighboring pixels are placed on the right side of Figure 5

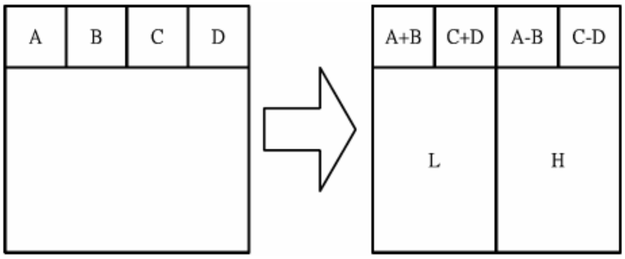

Figure 5 - Horizontal Operation

The second stage, Pixels are scanned from top to bottom in the vertical direction and then sum up the result of the subtraction neighbors next door are placed at the bottom of this operation is depicted in Figure6.

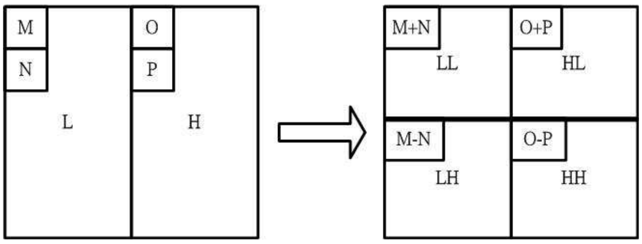

Figure 6 - Vertical Operation

Third layer:

The majority of existing methods for the placement of a certain number of bits are used, which decreases the security, because it retrieves a specified number of bits, the hidden data can be retrieved. It was the weakness of us can use a variable bit rate, which means that a variable number of bits can be placed on the coefficients of wavelet transform. How many bits per coefficient is given, the basis for the proposed method is presented. If the ratio is between one and two, one bit per coefficient can be placed. The number of possible modes for the ratio between one and two in Table 1 and Table 2, the best and worst levels of the coefficients of variation for the coefficients in Table3 is shown.

Table 1 - Number of possible modes for the one bits of secret message bits array

0	1

Table 2 - Rate of quantities between 1 and 2

Coefficient The bits of the message	coefficient after insertion		After insertion of a factor is the rate coefficient
			1
0	2-0	2	1
1	2-1	1	0

Table 3 -Coefficients of the best-and worst-case rate of change ratios between 1 and 2

Coefficient	The rate coefficient
1	
0	Best
1	At worst

If the ratio is two to four, with two bits per coefficient can be replaced, so the number of possible modes of four states in Table 4, Table 5, Table 6 are related to the coefficients between two and four.

Table 4 - Number of possible modes for the two bits of secret message bits array

00	01	10	11

Table 5 - Rate of quantities between 2 and 4

Coefficient The bits of the message	coefficient after insertion		After insertion of a factor is the rate coefficient	
			2	3
00	4-0	4	2	1
01	4-0.5	3.5	1.5	0.5
10	4-1	3	1	0
11	4-1.5	2.5	0.5	0.5

Table 6 -Coefficients of the best-and worst-case rate of change ratios between 2 and 4

Coefficient		The rate coefficient
3	2	
0	0.5	Best
1	2	At worst

If the ratio is four to eight, three bits per coefficient can be replaced, so the number of possible modes of eight cases in Table 7, Table 8, Table 9, the coefficients of four to eight.

Table 7 - Number of possible modes for the three bits of secret message bits array

000	001	100	110	100	101	110	111

Table 8 - Rate of quantities between 4 and 8

Coefficient	coefficient after insertion		After insertion of a factor is the rate coefficient			
			4	5	6	7
000	8-0	8	4	3	2	1
001	8-0.5	7.5	3.5	2.5	1.5	0.5
100	8-1	7	3	2	1	0
011	8-1.5	6.5	2.5	1.5	0.5	0.5
100	8-2	6	2	1	0	1
101	8-2.5	5.5	1.5	0.5	0.5	1.5
110		5	1	0	1	2
111		4.5	0.5	0.5	1.5	2.5

Table 9 -Coefficients of the best-and worst-case rate of change ratios between 4 and 8

Coefficient				The rate coefficient
7	6	5	4	
0	0	0	0.5	Best
2.5	2	3	4	At worst

As observed, the value of the coefficient, the number of bits determines placement. When the ratio is one to two, the number of bits that can accommodate, it is a bit. If the ratio of two to four, the number of bits inserted two bits and generally the ratio between2n-1 to 2n-1, the number of bits of the secret message in the index is placed n (Figure 7).

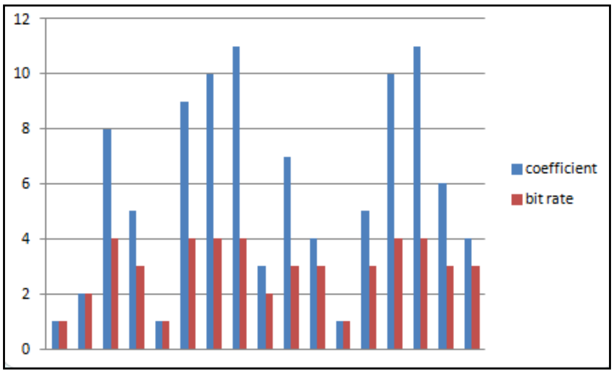

Figure 7- Relation coefficients and bit rate

Fourth layer :

Paste the least bit, one of the earliest methods of steganography. For example, if the pixel value is 57, it is possible to change the value to 58 or 56. In this way the least bit data input bit is replaced with (12).

host data	$(57)_{10}=(111001)_2$
message	0
stego data	$(56)_{10}=(1110000)_2$

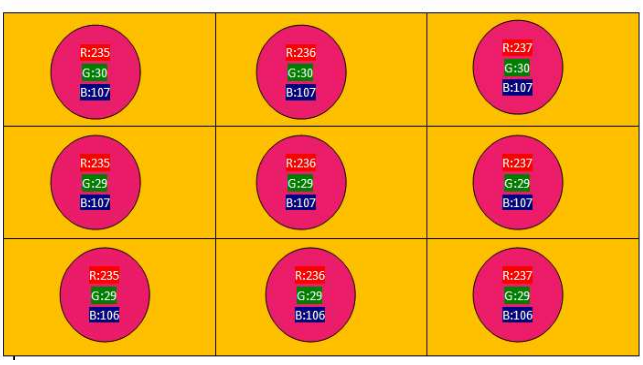

Figure8 - bits per pixel using the least

The following numerical example by replacing the least bit displays.

Advantages

- High capacity: the number of bits of the secret message, this method can be carried in the media, has been placed.

- Easy to implement (13) .

- Its use does not create tangible change in the media after placement.

Disadvantages

- Low security: information hidden in the media, with little gain valuable bits, uncovered.

In Figure9 it is observed that each image pixel has three colors, red, blue and green, as seen, for a unit change in each of the colors red, green and blue colore d circles does not create tangible change.

Proposed Insertion Algorithm

1. Reading selected image and separate it into three sub-bands of red, green and blue is broken (first layer).

2. The Haar wavelet transform is used for each color bands and a set of coefficients is generated (the second layer)

3. clustering coefficients are generated variable bit rate that can be placed at any rate, to be determined (the third layer).

4. less valuable bits per coefficients are used to embed (fourth layer).

5. image wavelet coefficients is used for the lining.

6. stego image is created and is sent to the destination.

Proposed Extraction Algorithm

7. read cover image and separate it into three sub-bands of red, green and blue is broken (first layer).

8. The Haar wavelet transform is used for each color bands and a set of coefficients is generated (the second layer).

9. clustering coefficients are generated variable bit rate that can be placed at any rate, to be determined (the third layer).

10. less valuable bits of each coefficient is retrieved (fourth layer).

3. RESULTS AND DISCUSSION

In this paper we have used the image of 1024 x 768 and 300,000 bits of data that we have. The results show the implementation capacity and transparency (Figure 9 and 10).

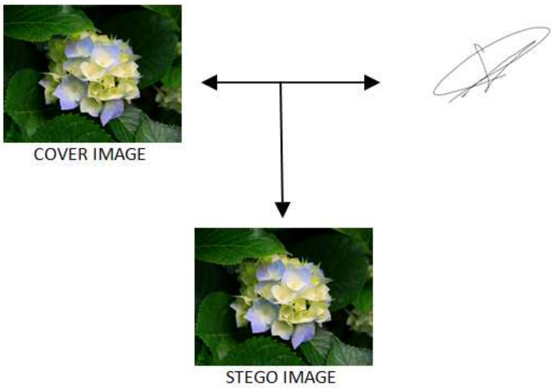

Figure 9- cover image and the original image

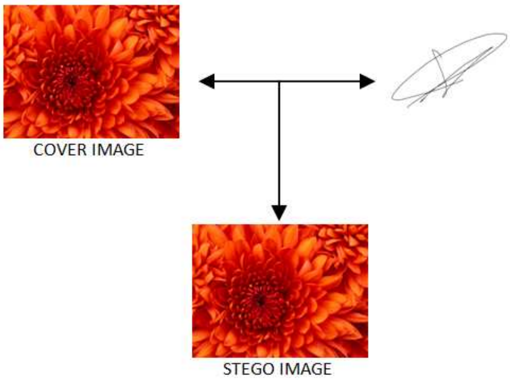

Figure 10 - cover image and the original image

The algorithms proposed evaluation criteria:

Capacity

Security

Transparency

The algorithms presented have tried all three meet the above objective, but with increased capacity, low security and tangible change will come. Therefore, a compromise between these objectives should be established.

Different aspects of the proposed technique has been evaluated and tested, capacity, security, transparency, low computational complexity of embedding and extracting. The capacity of the proposed algorithm is the number of bits set in the coefficients depend on the value of the coefficient. The larger the coefficient, the greater the number of bits per coefficient can be placed. The security parameters, we have established a review of placement with a variable number of bits. Since the ratio of the number of bits that can be placed at the specified index. Change or no change in the amount of bits of a coefficient depends on the message, it is because even if the original image is available, the coefficients can be identified carrying the message, which is due to the security algorithm. Transparency, dependence on the number of bits inserted into the index causing many bits are sometimes placed in an index and the index has not changed. The low computational complexity of embedding and extracting (using floating point coefficients of the wavelet transform) coefficients of wavelet are the decimal values of the correction coefficients of some of the methods they use. In the proposed algorithm, the coefficients for the placement of the decimal point is used, which reduce the computations. We were able to use encryption algorithms for secret messages(14,15).

5. CONCLUSIONS

Steganography is the science and art to hide the secret information. Many algorithms have been presented in steganography techniques, Each of them have strengths and weaknesses points. Steganography purposes of security, robustness and capacity of which three are located at three vertices of a triangle, each note entail ignoring others. For this purpose, field methods in both spatial and transform domain techniques will be examined. transform domain techniques into the steganography algorithms raising resistance. For this purpose, the host medium, the conversion, for example, wavelet transform is used(dwt). It is created as a result of many coefficients. In this paper, a technique is presented, which form a layer of the techniques he uses. The goals are the result of supply. The proposed methods such as clustering coefficients in the range of quantities do not change before and after placement. Since the range is variable coefficients can accommodate variable bit rate that will increase capacity and the lack of a fixed number of bits is increased security. The proposed technique is based on the wavelet transform coefficients are modified in such a way that roughly corresponds to the human visual system, to change the placement of confidential information in the image is less. The results show that the implementations of the technique presented steganography purposes as compared to other existing methods are improved.

REFERENCES

[1]-Ekhande S, Sonavane S,J Kulkarni. Universal Steganalysis Using Feature Selection Strategy for Higher Order Image Statistics. International Journal of Computer Applications (0975 - 8887),1:52-55

[2]-Blossom K, Amandeep K, Jasdeep S.2011. STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN. International Journal of Advances in Engineering & Technology,1:72-78

[3]-Banerjee I, Bhattacharyya S.2012. A Procedure of Text Steganography Using Indian Regional Language. I. J. Computer Network and Information Security, Published Online August 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijcnis:65-73

[4]-Stuti Goel, Arun Rana , Manpreet Kaur.2013. A Review of Comparison Techniques of Image Steganography. Global Journal of Computer Science and Technology Graphics & Vision.13:8-14

[5]-Pujari S, Mukhopadhyay S.2012. An Image based Steganography Scheme Implying Pseudo-Random Mapping of Text Segments to Logical Region of Cover Image using a New Block Mapping Function and Randomization Technique . International Journal of Computer Applications (0975 – 8887) 50:40-46

[6]-Sharma V, Kumar S.2013. A New Approach to Hide Text in Images Using Steganography . International Journal of Advanced Research in Computer Science and Software Engineering .3:701-708

[7]Khosravi S, Abbasi Dezfoli M, Yektaie MH. 2011. A new steganography method based on hiop(higher intensity of pixel) algorithim and strassen's matrix multiplication. Journal of Global Research in Computer Science RESEARCH PAPER Available Online at www.jgrcs.info. Volume 2, No. 1:6-12

[8]Kumar S, Raja B,Chhotaray R, Pattnaik S.2011. Steganography Based on Payload Transformation.IJCSI International Journal of Computer Science Issues,8:241-248

[9]Prabakaran G,Bhavani R.2013.A HIGH SECURE AND ROBUST IMAGE STEGANOGRAPHY USING DUAL WAVELET AND BLENDING MODEL. Journal of Computer Science, 9 (3): 277-284, 2013

[10]Chen P, Lin H.2006. A dwt based approach for image steganography. International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[11]-Dengre A, Gawande D.2013.Effect of Audio Steganography based on LSB insertion with Image Watermarking using AVI video. International Journal of Application or Innovation in Engineering & Management,2:363-370

[12]-Lifang Y, Yao Z, Rongrong N,Ting L.2010.Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm. EURASIP Journal on Advances in Signal Processing Volume 2010, Article ID 876946,:1-6

[13]-Ajinkya J, Atul S,Gavali D, Kurkute S.2013. Edge Adaptive Steganography Using DWT.International Journal of Engineering and Advanced Technology (IJEAT),2:648-652

[14] Dragan Vidakovic, Jelena Kaljevic,and Dusko Parezanovic, “Preparing for a (RSA) Digital Signature “ ,IJTPC(ISSN: 2322-3138), Vol. 2, March 2013.

[15]Yong-Jin Kim, Yong-Min Kim , Yong-Jin Choe , Hyong-Chol O,”An Efficient Bilinear Pairing-Free Certificateless Two-Party Authenticated Key Agreement Protocol in the eCK model”, IJTPC(ISSN: 2322-3138), Vol. 3, July 2013