A New Steganography Method based on Optimal Coefficients Adjustment Process (OCAP)

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

Mashallah Abbasi Dezfouli
Department of Computer Engineering,Science and Research Branch
Islamic Azad University
Khouzestan, Iran

Mohammad Hossein Yektaie
Islamic Azad University Of Abadan Branch
Abadan, Iran

ABSTRACT
Steganography is the technique for hiding secret information in other data such as multimedia images, text, audio. 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. The existing methods hide the information using constant bit length in integer wavelet coefficients. The main drawback of the existed methods is overflow of pixels may occur in integer wavelet domain after embedding. This may probably results bit error while recovering secret information. This paper uses variable bit length based on float wavelet coefficients to hide the data in a particular positions using secret key and Optimal Coefficients Adjustment Process (OCAP). The system combines an float wavelet transform and the variable rate of embedding and embeds secret data in a random order using a secret key only known to both sender and receiver to maximize performance of this steganographic method. to obtain an optimal mapping function to reduce the difference error between original coefficients values and modified values, OCAP algorithm is proposed. From the experimental results it is seen that the proposed methods achieve a much higher visual quality as indicated by the high psnr in spite of hiding a larger number of secret bits in the image. Moreover, extraction of the secret information is independent of original cover image.

General Terms
Optimal Coefficients Adjustment Process, secret information.

Keywords
Steganography, float wavelet coefficients, variable rate, psnr, OCAP

1. INTRODUCTION
Today's large demand of internet applications requires data to be transmitted in a secure manner[1]. Security is a major concern of communication[2].

The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users[3].

Recently steganography has attracted more and more, researchers in security. Steganography is a branch of information hiding[4] and Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages[5,6,7,8]. Steganography is information security tool which stores the secret information in any media file in such way that no one else except the sender of the information and the intended receiver can only suspect the existence of any sort of information[9].

The media with and without hidden information are called stego media and cover media, respectively [10]. an image is an array of numbers that represent light intensities at various points (pixels).These pixels make up the image raster data[11]. Image steganography has been found quite attractive, as compared to audio steganography, because the Human Visual System (HVS) is less sensitive to altered images than the auditory system to changes to audio signals[12]. The rest of the paper is organized as follows. Section 2 deals with a brief discussion of the exists algorithm . Section 3 discusses our new algorithm. Section 4 presents the detailed experimental results and comparisons. Finally, section 5 is the conclusion.

2. RELATED WORKS
Great variety of techniques in the field of steganography in images is presented, which aims to reach all of them are high capacity, security, and robustness [13]. These three criteria are in conflict with each other and simultaneously achieve all three simultaneously is very difficult and perhaps impossible . According to the application, they must compromise between established . Steganography algorithms include the step of putting confidential information at the transmitter and extract confidential information from the media outlets are carrying the destination. In this section we will introduce some of the methods of steganography. For this purpose, methods, field methods in both spatial and transform domain techniques will be examined. In spatial domain techniques, secret message can be placed in a carrier medium, without prior hide the confidential information on a carrier medium, the conversion takes place in the private placement is a direct bearing on the media[14]. Least significant bit (LSB) insertion is a common, simple approach to embedding information in a cover image [15]. Sharma and Shryvstava [16] algorithm have the least bit of technique and genetic algorithms are used. Turned the area into a domain are the carriers of the media. It may become discrete cosine transform, Fourier or wavelet is. Then the secret message is replaced by the coefficients of the transform and the inverse transform coefficients are taken from . Btachyra and colleagues [17] have shown that the algorithm combined with wavelet and discrete cosine transform are used.

3. PROPOSED METHOD
There are two basic operations involved in steganography,namely, embedding a secret message and its extraction.

The embedding algorithm describes how to hide a message into the cover object and the extraction algorithm illustrates

how to extract the message from the steganography object[18]. 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. The existing methods hide the information using constant bit length in integer wavelet coefficients. The main drawback of the existed methods is overflow of pixels may occur in integer wavelet domain after embedding. This may probably results bit error while recovering secret information. Proposed method uses variable bit length based on float wavelet coefficients to hide the data in a particular positions using secret key and useing Optimal Coefficients Adjustment Process (OCAP) to maximize performance of this steganographic method.to obtain an optimal mapping function to reduce the difference error between original coefficients values and modified values OCAP algorithm is proposed. in this method, we try to make the best using of the coefficients have.For this purpose we present a new method, which we proceed to describe it. wavelet transform is applied to the cover image to get the wavelet coefficients. the wavelet coefficients is splitted into RGB planes .The obtained wavelet coefficients from the RGB planes, select one or two or three planes according to the secret key and Each selected plane is decomposed into blocks according to the secret key.The selected coefficients are classified based on green table(CCGT)(Table 1.). then The number of bits that are to be replaced, it is clear(1). The result is placed in the matrix, called Power matrix.We create two source matrix and decimal value of secret message bits matrix based on power matrix .We subtract the decimal value of secret message bits matrix from matrix source . The result is a matrix cover.While the greater number of bits have been replaced, the coefficients are little changed.After replacement, inverse wavelet transform applied to restore the image (Fig 1) and (Fig 2).

Table 2. Classification of coefficient based on green table(CCGT)

Number of bits	Value of wavelet coefficients
1	0-1
2	2-3
3	4-7
4	8-15
5	16-31
6	32-63
7	64-127

$$N=\begin{cases}1 & 0<\text{coefficient}<1\\ \text{Log(coefficient)} & 1<\text{coefficient}<\max(\text{coefficient})\end{cases}$$

N is number of bits that are to be replaced.

Step 1: wavelet transform is applied on the original image and create Original Matrix.

$$\begin{pmatrix} OC1 & OC2 \\ OC3 & OC5 \\ OC6 & OC7 \end{pmatrix}$$

Original Matrix

Step 2: Select the desired rows and columns based on random key and generated coefficient Matrix.

$$\begin{pmatrix} C1 & C2 \\ C3 & C5 \\ C6 & C7 \end{pmatrix}$$

Coefficient Matrix

Step 3: the Power matrix can be created based on coefficient Matrix and CCGT table.

$$\begin{pmatrix} PC1 & PC2 \\ PC3 & PC5 \\ PC6 & PC7 \end{pmatrix}$$

Power Matrix

Step 4: Create a source matrix based on the Formula 2.

Formula 2

$$Sp_{i,j}=2^{p}{}_{i,j}$$

IN Formula 2 pi, j of elements of Power matrix, and Spi, j elements of source matrix.

Step 5: The secret message can be converted to an array of bits. based on the Power matrix and the formula 3 the secret message matrix created .

Formula 3

$$ms_{i,j}=dec(mpc_{i,j})/2$$

In Formula 3, msi, j is elements of secret message matrix and dec (mpci,j) is the decimal bits secret message. we

calculate the number of bits is variable and based on the number of Power matrix be determined.

Step 6: Create a cover matrix based on the Formula 4

Formula 4

$$cov_{i,j} = Sp_{i,j} - ms_{i,j}$$

In Formula 4, covi, j is elements of cover matrix.

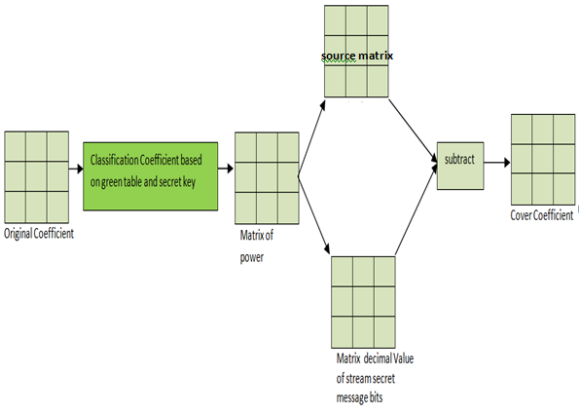

Fig1 :Proposed algorithm

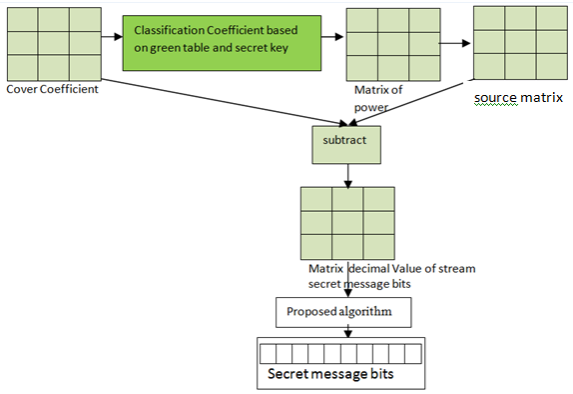

Fig2:Proposed Extract algorithm

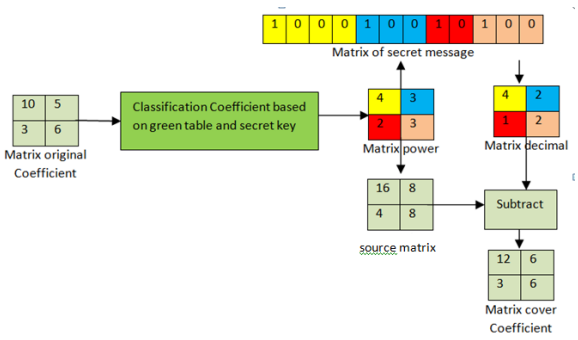

Fig 3: An example of hiding data bits inside based proposed method.

4. RESULTS AND DISCUSSION

The experimental results presented in this section describe the performance of our proposed technique. Three common requirements, security, capacity and imperceptibility, may be used to rate the performance of steganographic techniques. Generally speaking, a good steganographic technique should have good visual imperceptibility and a sufficient capacity of hidden secret data[19].

Security

For the security requirement this technique has presented two different ways to deal with the issue Using secret keys and variable bit length.The steganographic method proposed in this paper are very secure as variable number of bits are hidden in different coefficient of wavelet.This method embeds secret information in a random order using a secret key only known to both sender and receiver So it is very difficult to find out the hidden data from the stego image. The same stego image can also bear different secret image for different receiver depending on their secret key.

Capacity

Capacity means the amount of message that can be embedded. Table 2. show Average PSNR values and Embedding Rate achieved using standard images.We have to make a compromise between capacity and PSNR. maximum value of Embedding Rate by using method is 0.46 and PSNR is 46.44.

Imperceptibility

The medium after being embedded with the covert data should be indiscernible from the original medium[20]. A larger PSNR indicates that the quality of the stego image is closer to the original one. Normally human's eyes find it hard to distinguish between the distortions on a stego image compared to original image when its PSNR value is greater than 30 dB. for embedding then value of PNSR is equal to 46.75 which is higher than threshold value (30dB). Theoretically, the higher the PSNR value is. the better the image processing is; however, practically, there are some problems reported in [21]. we use the Peak Signal-to-Noise Ratio (PSNR) measurement to evaluate the difference between the stego and cover images.

Blind

Usually universal methods do not require the knowledge of the details of the embedding operations. Therefore, it is also called blind method.in proposed method The embedded information can be extracted from stego image without the knowledge of original image by considering the same secret key.

We implemented our algorithm in MATLAB and carried our experimentations with different standard Colored images. In this paper we selected 512x512 "Lena" jpeg image to perform our testing. Fig 4 has been shown cover image, Fig 5 has been shown stego image.

Our experimental results have shown that the proposed method provides an efficient way for embedding large amount data into cover images without making noticeable distortions

Table 2. Comparison of performance of two steganography algorithms

Embedding Rate		0.01	0.02	0.05	0.20	0.25	0.35
PSNR	Me	64.87	61.51	55.22	49.14	48.01	46.75
	[22]	64.33	57.4	54.38	46.48	42.62	38.44

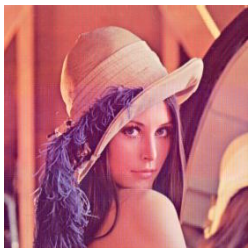

Fig 4.Cover Image

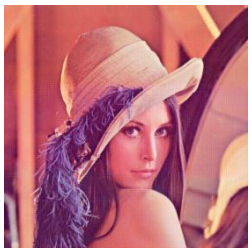

Fig 5. Stego image

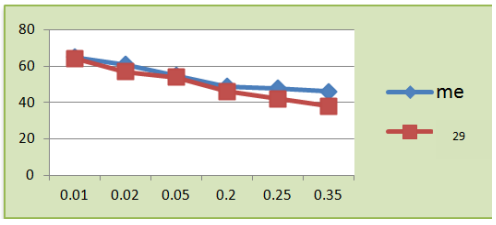

Fig 6 . Method quality performance in comparison with [22]

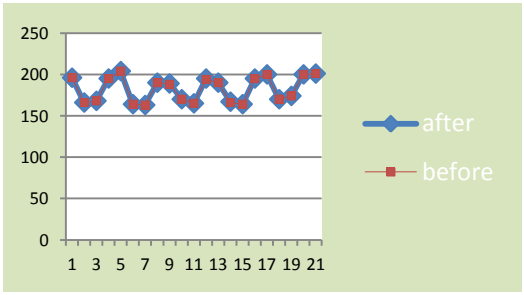

Fig 7 - Illustration of blue color before placement and after placement

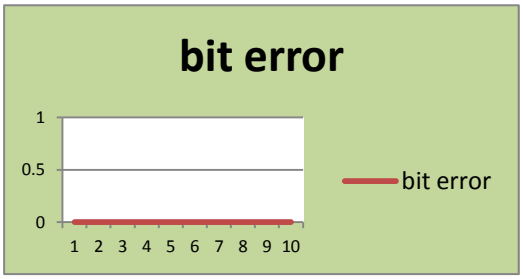

Fig 8 - Illustration of bit error based on proposed method

5. CONCLUSION

The existing methods hide the information using constant bit length in integer wavelet coefficients. The main drawback of the existed methods is overflow of pixels may occur in integer wavelet domain after embedding. This may probably results bit error while recovering secret information.This paper uses variable bit length based on float wavelet coefficients to hide the data in a particular positions using secret key and Optimal Coefficients Adjustment Process (OCAP).The system combines an float wavelet transform and the variable rate of embedding and embeds secret data in a random order using a secret key only known to both sender and receiver to maximize performance of this steganographic method.to obtain an optimal mapping function to reduce the difference error between original coefficients values and modified values OCAP algorithm is proposed. They tested the algorithm with different images to estimate the quality of the stego image. They achieved a better PSNR. The steganographic methods proposed in this paper are:

- ✓ very secure
- ✓ capacity is good.
- ✓ PSNR obtained is approximately maximum compared to the existing algorithm which confirm imperceptibility of the host and the stego image.
- ✓ The proposed system also reduces the difference between original coefficients values and modified values by using the adaptive float coefficient adjustment.
- ✓ Blind steganogeraphy method
- ✓ computational complexity is normal

Or entirely In this research, we introduced a novel steganography technique to increase the capacity and the imperceptibility of the image after embedding.By using this method the data hiding capacity is improved and secrecy of the embedded data bits can be provided. It is also seen that the stego image formed is of good quality.

Future works:

1) our secret information can first be encrypted by using any standard encryption algorithm and then embedded. In this way we provide an extra layer of security to our systems.

2) may be carried out to increase the capacity and enhance the visual quality of the stego image by improving the PSNR value.

6. REFERENCES

[1] Jayaram P, Ranganatha H R, Anupama H S," INFORMATION HIDING USING AUDIO TEGANOGRAPHY – A SURVEY", The International

Journal of Multimedia & Its Applications (IJMA) Vol.3, No.3, August 2011

[2] Dhanya Job, 2Varghese Paul," Digital Image Steganography using Elliptical Curve Cryptography for Secured Data Transmission", Volume 3, Issue ICASE13, April 2013, ISSN Online: 2277-2677

[3] Seyyed Amin Seyyedi,Rauf.Kh Sadykhov,"Digital Image Steganography Concept and Evaluation", International Journal of Computer Applications (0975 – 8887) Volume 66– No.5, March 2013

[4] Shen Wang, Bian Yang and Xiamu Niu," A Secure Steganography Method based on Genetic Algorithm", Volume 1, Number 1, January 2010

[5] Souvik Bhattacharyya, Indradip Banerjee and Gautam Sanyal," A Survey of Steganography and Steganalysis Technique in Image, Text, Audio and Video as Cover Carrier", Volume 2, No. 4, April 2011 Journal of Global Research in Computer Science REVIEW ARTICLE

[6] Moazzam Hossain, Sadia Al Haque, and Farhana Sharmin," Variable Rate Steganography in Gray Scale Digital Images Using Neighborhood Pixel Information", The International Arab Journal of Information Technology, Vol. 7, No. 1, January 2010

[7] Dr. Monisha Sharma1 and Mrs. Swagota Bera2," A REVIEW ON BLIND STILL IMAGE STEGANALYSIS TECHNIQUES USING FEATURES EXTRACTION AND PATTERN CLASSIFICATION METHOD", International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), Vol.2, No.3, June 2012

[8] Hamdy A. Morsy, Zaki B. Nossair, Alaa M. Hamdy, Fathy Z. Amer," JPEG Steganography System with Minimal Changes to the Quantized DCT Coefficients", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-1, Issue-6, January 2012

[9] Sandeep Singh, Aman Singh, "A Review on the Various Recent Steganography Techniques", IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013 ISSN (Online) : 2277-5420 www.IJCSN.org

[10] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi," A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing °c 2011 ISSN 2073-4212 Ubiquitous International Volume 2, Number 2, April 2011

[11] Nitin Jain, Sachin Meshram, 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

[12] Zhang Tao1, Zhang Yan2, Li Wenxiang1, Ping Xijian1," STEGANALYSIS OF LSB MATCHING EXPLOITING HIGH-DIMENSIONAL CORRELATIONS BETWEEN PIXEL DIFFERENCES", 2009 Fifth International Conference on Natural Computation 978-0-7695-3736-8/09 $25.00 © 2009 IEEE DOI 10.1109/ICNC.2009.195

[13] Saddaf Rubab, M. Younus," Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal of Computer Applications (0975 – 8887) Volume 39– No.14, February 2012

[14] Khosravi Sara 1 , Abbasi Dezfoli Mashallah 2 , Yektaie Mohammad Hossein 3," A NEW STEGANOGRAPHY METHOD BASED ON HIOP (HIGHER INTENSITY OF PIXEL) ALGORITHM AND STRASSEN'S MATRIX MULTIPLICATION", Volume 2, No. 1, January 2011 Journal of Global Research in Computer Science RESEARCH PAPER Available Online at www.jgrcs.info

[15] Saddaf Rubab, M. Younus," Improved Image Steganography Technique for Colored Images using Wavelet Transform", International Journal of Computer Applications (0975 – 8887) Volume 39– No.14, February 2012

[16] Sharma VK, Shrivastava V. 2010. Improving the performance of least significant bit substitution steganography against rs steganalysis by minimizing detection probability. International Journal of Information and Communication Technology Research. Volume 1 No. 4, August 2011 ISSN-2223-4985:148-156

[17] Bhattacharya T, Dey N, Chaudhuri B. 2012. A session based multiple image hiding technique using dwt and dct. International Journal of Computer Applications (0975 – 8887) Volume 38– No.5:18-21

[18] Najran N. H. Al_Dawla,M. M. Kazi,K. V. Kale," Steganography Enhancement by combining text and image through Wavelet Technique", International Journal of Computer Applications (0975 – 8887) Volume 51– No.21, August 2012

[19] Arun Rana1, Nitin Sharma2, Amandeep Kaur3," IMAGE STEGANOGRAPHY METHOD BASED ON KOHONEN NEURAL NETWORK", ISSN: 2248-9622 www.ijera.com Vol. 2, Issue 3, May-Jun 2012, pp.2234-2236

[20] G. Bindu, K. Srilakshmi," A NOVEL APPROACH OF LSB STEGANOGRAPHY FOR RETREIVING TEXT FROM AUDIO", G Bindu et al ,Int.J.Computer Technology & Applications,Vol 3 (4), 1384-1387, ISSN:2229-6093

[21] Yıldıray YALMA,Ismail ERT¨URK," A new color image quality measure based on YUV transformation and PSNR for human vision system", Turk J Elec Eng & Comp Sci (2013) Turkish Journal of Electrical Engineering & Computer Sciences http://journals.tubitak.gov.tr/elektrik/

[22] S. Premkumar,L. Dinesh," Efficient Algorithm for Steganography Technique Combined with Image Cryptography for Secure Application", International Journal of Computer Applications (0975 – 8887) Volume 49– No.13, July 2012