International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.183-194
http://dx.doi.org/10.14257/ijsia.2014.8.4.17

High Payload and Secure Steganography method Based on Block Partitioning and Integer Wavelet Transform

Seyyed Amin Seyyedi[1] and Nick Ivanov[2]

[1]*Department of Computer, Maku Branch, I.A.U, Maku, Iran*
[1,2]*Department of Electronic Computing Machines, Belarusian State University of Informatics and Radioelectronics*
amseyyedi@gmail.com, ivanovnn@gmail.com

Abstract

Steganography is a branch of information hiding. Payload volume and security of confidential data are major challenges of steganography methods. This article presents high volume payload and secure steganography technique based on integer wavelet transform. The cover image is partitioned into 8× 8 non overlapping blocks, then each transformed block partitioned into two subsets and secret message is embedded in proper subset. To achieve higher security, Haar wavelet transform is applied to the secret message before embedding it. Experimental results indicate low degrading of the original image by hidden secret message of rather high volume.

Keywords: *Steganography, Integer Wavelet Transform, Steganalysis, Embeddable Subset*

1. Introduction

The security of information becomes the main challenges in communication environment. Steganography is technique of hiding confidential data in any form of media in such a way that no one, except the intended recipient knows the existence of secret data [1, 2]. Current steganography techniques allow hiding information inside multimedia files. Among the different kinds of multimedia, the digital image is commonly used as a host image to convey side information in it. Hence, image hiding investigating is actual issue. Steganalysis is the art and science of detecting a secret message. Its goal is to detect a presence of secret message [3]. The ability of steganalysis methods depend on the volume of payload of hidden message. Hence, this fact imposes an upper bound limit for embedding data, such that if the hidden data size is less than that upper bound, one may assert that the stego-image is safe and the steganalysis methods cannot detect it [3, 4].

A steganography method must satisfy three aspects, payload, security and fidelity. Payload refers to the amount of information that can be hidden in the cover image. Security refers to impossibility of successful attack to detect hidden information. Fidelity (imperceptibility) refers to inability of human eyes to distinguish between cover image and stego-image. Increasing payload rate is in conflict with fidelity and security. The major goal of steganography techniques is to enhance communication security by increasing embedding rate [4, 5].

Many methods of steganography are proposed in literature. The least significant bit (LSB) method is a popular type of steganography in spatial domain. Most existing approaches use pseudo random generator to select embedding region and K bits of LSB to increasing embedding rate without considering the image contains. Increasing the K leads to significant distortions in smooth areas of cover image [6-9].

ISSN: 1738-9976 IJSIA

D. Wu and D. Tsai [10] proposed a steganography method based on pixel value differencing. In the embedding process a cover image is partitioned into non overlapping blocks of two consecutive pixels. Each block is classified by its difference value. The small difference values denote the smooth area and big one indicate the edge area. Therefore embedding amount of secret message depends on the characteristics of each block. This method provided a way to produce stego-image by simple LSB replacement methods.

B. Lia and L. Chang [11] proposed an adaptive data hiding based on Haar wavelet discrete transform. The cover image is partitioned into 8×8 non overlapping blocks, then Haar wavelet transform is performed on each blocks. A data hiding capacity function is used to determine the volume of embedding secret message in transformed sub bands. The secret message is embedded by using LSB method. R. El Safy and H. Zayed [12] proposed similar method with modification of capacity function.

In comparison with mentioned methods, proposed method provides better quality of stego-image, increased embedding payload, and higher security against steganalysis attacks.

This article presents high payload and secure steganography technique based on block partitioning followed by integer wavelet transform. Blocks are divided into subsets and secret message is embedded in the proper one. In addition to achieve higher security and authentication, Haar wavelet transform is applied to the secret message before embedding procedure.

2. Related Work

This section briefly explains some introductory techniques that utilize in this article.

2.1. Cover Image Adjustment

During the embedding process in frequency domain, some coefficient will occur underflow/overflow after embedding secret message on these coefficients (in gray scale image underflow means the pixel value smaller than 0 and overflow means that the pixel values exceed maximum value 255). In this case lower/higher values will be clipped and the secret message bits are lost. To overcome the underflow/overflow difficulty, need to be applying histogram modification on the cover image before the embedding process. Hence, the cover image pixels $C(i, j)$ are adjusted as follow: [11, 13]

$$C'(i,j) = \begin{cases} C(i,j) - N/2 & if \quad C(i,j) \geq 255 - N/2 \\ C(i,j) + N/2 & if \quad C(i,j) \leq N/2 \end{cases} \tag{1}$$

where $C'(i, j)$ denotes the adjusted pixel in spatial coordinates i, j. N is the argument to modify histogram of an image. The value of N is set to 30.

2.2. Integer Lifting Wavelet Transform

Multi Resolution Analysis is the main theory in wavelets that analyzes a signal in frequency domain in detail. One level 2D wavelet transform on an image decomposes the cover image into four sub bands, namely LL1, HL1, LH1 and HH1. The sub band LL1 includes the low pass coefficient and presents a soft approximation of image. Other three sub bands show horizontal, vertical and diagonal details respectively. Approximation of sub bands is processed further to obtain next coarser scale of wavelet coefficient until determine scale N is attained. N scale transforms yields 3N+1 sub bands. Basically a digital image consists of integer samples. Unfortunately wavelet filters return floating point values as wavelet coefficients. When one hides data in the coefficients any truncations of the floating

point values cause the corruption of the hidden information. To overcome this difficulty one can apply Integer Lifting Wavelet Transform (IntLWT) [14].

The lifting scheme is a technique for both designing wavelets and performing the discrete wavelet transform. The lifting scheme is method for decomposing wavelet transform into a set of stages. It's consists of three phases: a) Split phase, b) Predicate phase, c) Update phase. Figure 1 represents the generic scheme. An advantage of lifting scheme is that it does not require temporary storage in calculation step and the inverse transform has exactly the same complexity as the forward transform [14, 15]. In this paper Haar lifting scheme is chosen as a case study.

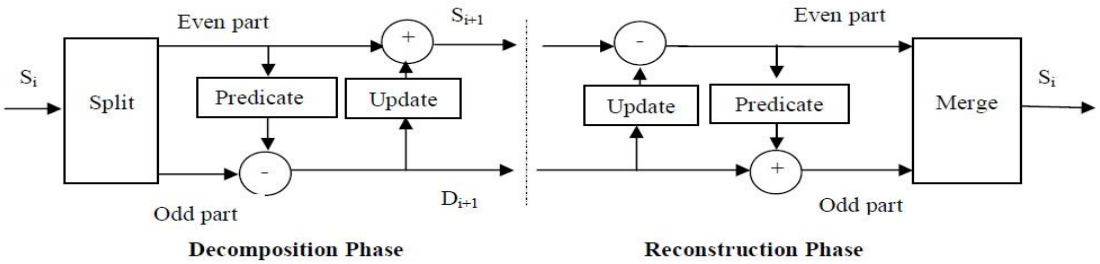

Figure 1. The Lifting Scheme

2.3. Rounding Method

Rounding method is one a way for embedding secret message bits in cover image. The pixel value is modifying into the nearest integer with the last LSB bits equal to the input bits. For example, assume that capacity of the current pixel is found to be 3 bits. Then, the current pixel is equal to 160 or $(10100000)_2$ and the input bits are equal to $(101)_2$. According to the rule described above, the value of pixel is changed into 157 or $(10011101)_2$. The mathematical representation of rounding method is [16]:

$$y = x + A \times (A \le B) - B \times (B < A), \tag{2}$$

$$A = \mathrm{mod}(\ m - x, 2^c), \tag{3}$$

$$B = \mathrm{mod}(\ x - m, 2^c)\ , \tag{4}$$

where y, x, m, and c denote the output value, input value, secret message and capacity respectively.

3. The Proposed Image Steganography Technique

An adaptive steganography technique based on IntLWT for hiding a large volume of data proposed in this article. The cover image is partitioned into 8×8 non overlapping blocks and 2D IntLWT applied to each block. The coefficients in each transformed block partitioned into embeddable (*E*) and unused (*U*) subsets. The subset partition is based on local threshold *T*. The coefficient $f(i, j)$ in block $B(k)$ belongs to subset *E*, if absolute value of coefficient $f(i, j)$ smaller than threshold *T*. The threshold *T* is defined as follows:

$$T = \frac{\max\ (B(k))}{2}. \tag{5}$$

where max (.) denotes as maximum value of coefficients in block $B(k)$.

The coefficients of subset *U* are not suitable to change because any modifications lead to more distortion of stego-image quality. The embeddable subset *E* for each block is undergone for embedding a secret message. The data hiding length (*L*) is computed based on absolute value of coefficients in *E* with the aid of following decision factor:

$$L = \begin{cases} 1 & if\ E_i = 0,1 \\ \lfloor \log_2 E_i \rfloor & otherwise \end{cases}, \tag{6}$$

where *i* denotes the coefficient index in subset *E* and *L* denotes the volume of messages that can be embedded into coefficient *i*.

The Figure 2 and 3 indicate the two-level Haar IntLWT coefficients of first 8×8 sub block of cover images Airplane and Baboon with volume of message that can be embedded in each coefficient. The blue coefficients in below figures represent elements of subset *U*.

81	72	-4	-1	9	-15	-42	8
92	72	-7	9	7	26	23	-3
-41	-40	4	5	-25	19	2	-18
47	-36	78	-15	-5	1	6	-4
-53	34	-42	-24	75	-12	11	8
51	-23	0	-10	27	-47	76	5
15	-90	17	-11	-41	-16	12	27
13	19	43	9	10	46	-19	2

81	72	2	1	3	3	5	3
92	72	2	3	2	4	4	1
5	5	2	2	4	4	1	4
47	5	78	3	2	1	2	2
-53	5	5	4	75	3	3	3
51	4	1	3	4	-47	76	2
3	-90	4	3	5	4	3	4
3	4	5	3	3	46	4	1

Figure 2. Transformed First 8×8 Block of Airplane and its Data Hiding Volume

161	187	-1	0	-7	7	17	4
153	179	0	-5	-5	-7	-10	-9
59	1	8	-6	1	-4	-2	1
47	2	-11	-3	1	-6	-5	-9
126	-4	2	-1	10	13	-10	3
127	2	-5	0	-11	-4	-2	6
99	2	2	2	-16	4	-3	3
89	-4	6	3	-10	1	-1	4

161	187	1	1	2	2	4	2
153	179	1	2	2	2	3	3
5	1	3	2	1	2	1	1
5	1	3	1	1	2	2	3
126	2	1	1	3	3	3	1
127	1	2	1	3	2	1	2
99	1	1	1	4	2	1	1
7	2	2	1	3	1	1	2

Figure 3. Transformed First 8×8 Block of Baboon and its Data Hiding Volume

As shown in the Figures 2 and 3 volume payload in first 8×8 sub block Baboon 38.26% more than the Airplane block, because the complexity in block Baboon is more than block Airplane.

In order to increase security and provide authentication before embedding the secret message in cover image, the Haar wavelet transform performed on secret message. The block diagram of proposed method is shown in Figure 4.

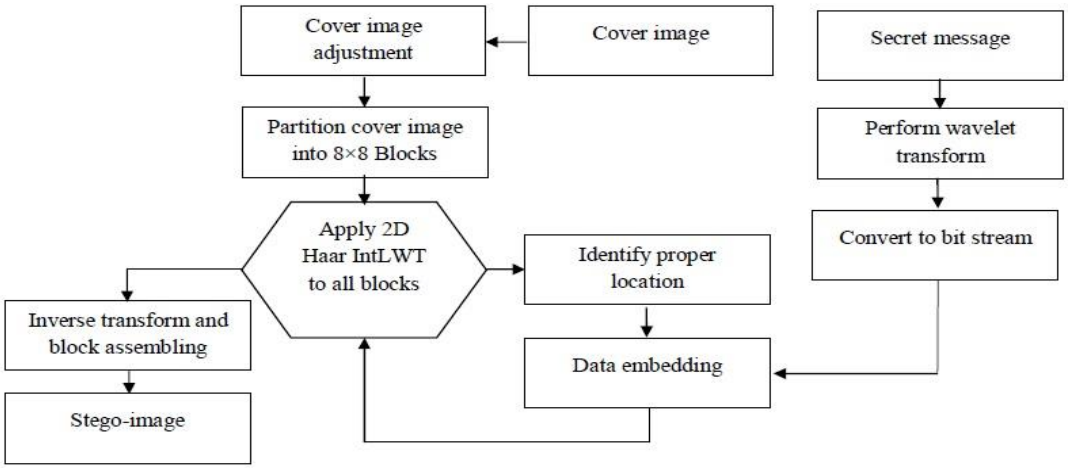

Figure 4. The Block Diagram of Proposed Method

3.1. Embedding Algorithm

Proposed algorithm for hiding a large volume of data is formalized by following steps:

Input: *Cover image C of size M × N and a secret message SE.*
Output: *Stego- image S.*
Step 1: Read cover image C.
Step 2: Read the secret message SE and perform one level integer Haar wavelet transform.
Step3: Apply cover image adjustment to C.
Step 3: Divide the cover image into 8× 8 blocks.
Step 4: Perform two levels Haar IntLWT to each block
Step 5: Divide coefficient in each block into subsets U and E.
Step 6: Compute value L from subset E by formula (6).
Step 7: If L=1 then use LSB to embed secret message bits, else use Rounding method.
Step 8: Perform inverse wavelet transform for each block.
Step 9: Assemble stego-image S from blocks.

4. Experimental Results

In this section, some experiments are carried out to assess the efficiency of the proposed scheme based on data payload, fidelity and security benchmarks [2, 17]. The proposed method has been simulated using the MATLAB 8.1 (R2013a) tools on Windows 7 version 6.1 platform. The secret message is generated randomly. Some results of proposed method are presented on six well known 512×512 gray scale images respectively Barbara, Peppers, Baboon, Lena, Airplane and Boat are shown in Figure 5. Howbeit the results presented here confined to six well known images. The proposed method tested on image database of BOSSBase (v0.92) [18] and the results obtained were statistically relevant.

Figure 5. Cover Images

Fundamentally, data payload of steganography method is one of the evaluation criteria. Data payload can be defined as the amount of information that can be hidden in the cover image. It depends on the embedding function, and may also depend on properties of the cover image. The embedding rate is mostly given in absolute measurement or in relative measurement called the data embedding rate (given mostly in bits per pixel, *etc.*).

Figure 6 shows the maximum payload rate of proposed method based on several block sizes. According to the results shown in Figure 6, the payload rate increases with increasing the block size.

Usually, fidelity (invisibility) of the steganography method measures by various image similarity metrics such as Mean Square Error (*MSE*) and Peak Signal to Noise Ratio (*PSNR*).

Mean squared error (*MSE*) between the cover image and the stego-image is defined as follows:

$$MSE = \frac{1}{(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} (C_{i,j} - S_{i,j})^2. \quad (7)$$

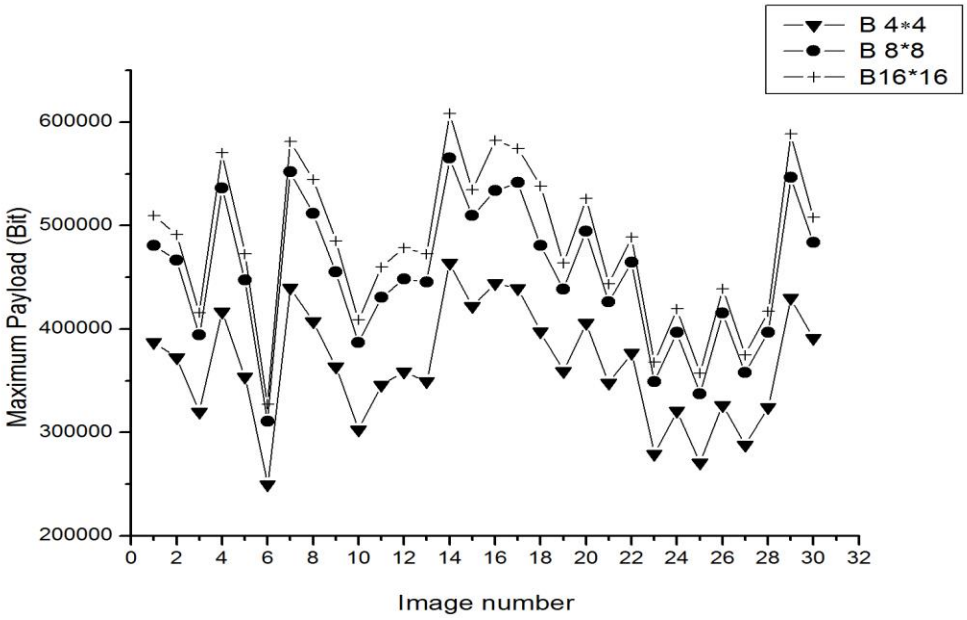

Figure 6. The impact of block size on payload

The *PSNR* is computed using the following formula:

$$PSNR = 10 \log_{10} \frac{Max^2}{MSE} dB, \quad (8)$$

where *Max* denotes the maximum pixel value of the image. A higher *PSNR* value indicates the better quality of a stego algorithm. Human visual system is unable to distinguish images with *PSNR* more than 36 *dB* [2].

Security of steganographic method is defined in term of undetectability. There are many approaches in defining the security of a steganographic method [17, 19, 20]. J. C. Cachin [21] defined a steganographic method (by Kullback-Leibler KL divergence) to be ε-secure ($\varepsilon \geq 0$), if the relative entropy between probability distribution of cover image (P_C) and stego-image (P_S) are at most ε. Then the detectability $D(P_C \parallel P_S)$ is defined by:

$$D(P_C \parallel P_S) = \int P_C \log \frac{P_C}{P_S} \quad (9)$$

Thus, for a completely secure stego system, $D = 0$ and if $D \leq \varepsilon$, then stego system is named ε -secure.

Table 1 shows maximum payload, imperceptibility metrics and ε-secure analysis of proposed method with various payload sizes for six well known cover images. According to the results shown in Table 1, increasing the payload rate, make conflict with imperceptibility metrics and security metrics and the maximum payload of cover image Baboon more than other cover images. Because the complexity of the image content Baboon more than other cover images.

Table 1. Calculation of Maximum Payload and Various Metrics to Analyze the Imperceptibility and Security of Proposed Algorithm

Cover images	Maximum payload (bit)	Metrics	Length of embedded message (byte)				
			20000	30000	35000	40000	50000
Barbara	480648	PSNR	43.33	41.45	40.59	39.84	38.89
		MSE	3.02	4.66	5.68	6.75	8.39
		ε-secure	1.31E-04	1.92E-04	2.36E-04	2.77E-04	3.58E-04
Peppers	418187	PSNR	44.01	42.26	41.73	41.38	40.64
		MSE	2.58	3.87	4.36	4.73	5.61
		ε-secure	8.33E-05	1.7E-04	1.98E-04	2.31E-04	2.99E-04
Baboon	616365	PSNR	40.94	39.57	39.07	38.72	38.07
		MSE	5.24	7.17	8.06	8.73	10.13
		ε-secure	3.05E-04	3.65E-04	3.92E-04	4.21E-04	4.76E-04
Lena	406040	PSNR	45.05	42.93	42.13	41.53	40.54
		MSE	2.03	3.31	3.98	4.57	5.73
		ε-secure	8.48E-05	1.42E-04	1.74E-04	2.01E-04	2.56E-04
Airplane	386830	PSNR	43.99	41.65	40.76	40.18	N/A
		MSE	2.59	4.44	5.45	6.23	N/A
		ε-secure	7.05E-05	1.06E-04	1.26E-04	1.45E-04	N/A
Boat	426192	PSNR	44.30	41.70	40.92	40.22	39,40
		MSE	2.42	4.40	5.25	6.18	7,47
		ε-secure	7.81E-05	1.42E-04	1.79E-04	2.28E-04	2.95E-04

Maximum payload, imperceptibility and ε-secure are used as a measure of comparison proposed method with D. Wu [10] and B. Lai [11] methods. Author did the experiments on image database [18]. Table 2 compares the mean values of maximum payload of the proposed method with D. Wu and B. Lai methods. The results obtained from comparison of proposed, D. Wu, and B. Lai methods indicate that maximum payload of proposed method is greater at 10.16% and 16.34% respectively in comparison with D. Wu and B. Lai methods.

Table 2. Comparison of Maximum Payload Value

Metric	Proposed method	Wu	Lai (k=1)
Max Payload (bit)	467266	422376	401615

Table 3 compares the imperceptibility and security measurement metrics of proposed method, D. Wu method and B. Lai (k=1) method for secret message with length 30000 bytes. According to the results shown in table 3, security of proposed method is increased 18.3% and 92.06% respectively in comparison with above method.

Table 3. Comparison of Imperceptibility and Security Measures

Metrics	Wu method		Lai method (k=1)		Proposed method	
	Mean	Std. Dev.	Mean	Std. Dev.	Mean	Std. Dev.
PSNR	41.13	1.492	40.25	1.268	42.06	1.338
MSE	6.247	4.790	5.758	1.492	4.2313	1.35
ε-secure	2.02E-04	1.2E-04	1.31E-03	3.4E-03	1.65E-04	8.81E-05

4.1. Security Analysis of Proposed Method

Steganography method is said to be undetectable or secure if the existence statistical tests cannot distinguish between the cover and the stego-image. A. Martin [22] had experimentally investigated that during the embedding process in the cover image some statistical variations are arises. But if these variations are very small it cannot be detected. The warden may exploit this approach to detect secret message in suspected image.

Avcibas [23, 24] proposed steganalysis method based on hypothesis that steganography schemes leave statistical evidence. Therefore warden can be exploited these hypothesis for detection with the aid of Image Quality Metrics (IQMs). He developed a discriminator for cover image and stego-image using an appropriative set of IQMs. These quality metrics are categorized into six groups according to the type of information [25]. In order to select appropriate set of IQMs, he used analysis of variance techniques. The selected IQMs for passive warden steganalysis are mean of the angle difference M4, median block spectral phase distance M8, median block weight spectral distance M9, normalized mean square HVS error M10. The IQM scores are computed from images and their Gaussian filtered versions with $\delta = 0.5$ and mask size 3×3 [25, 26].

The variations in IQMs for proposed method, D. Wu, and B. Lai methods with embedding the 30000 bytes in cover images were considered. From experimental results it can be perceived that statistical difference between cover images and stego-images of proposed method is negligible and less than other methods. Therefore proposed method is more secured against statistical attack and the warden cannot distinguish stego-image from cover image. The variations in IQMs for M8 and M9 are shown in Figure 7.

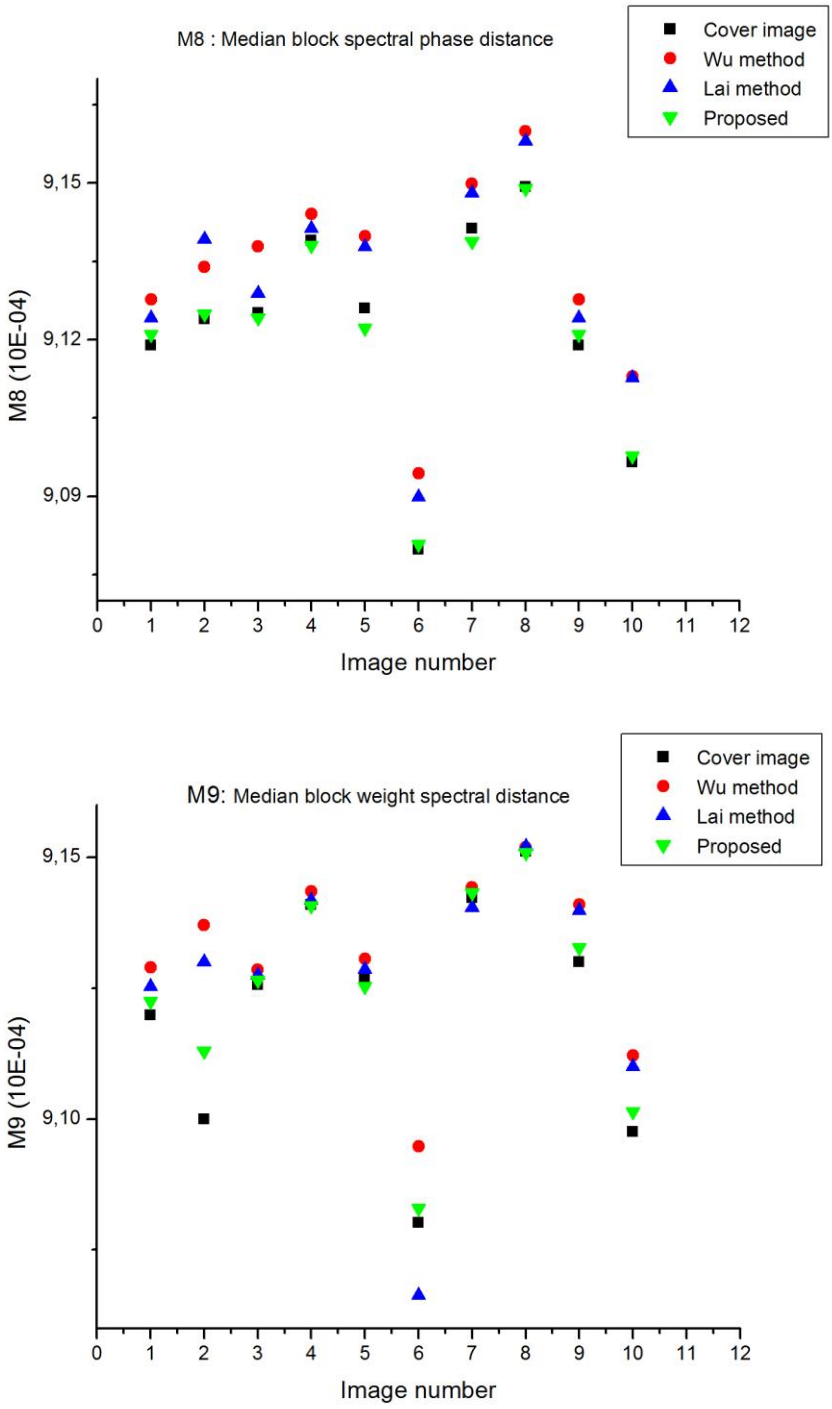

Figure 7. Variation in IQMs for Proposed Algorithm, Wu, and Lai Methods

5. Conclusion

Generally the steganography methods are concerned to primary objectives, maximum possible payload and imperceptibility of embedding data. The proposed method pre-adjusts

the cover image in order to insure that the pixel values not exceed its maximum value after embedding phase and hence the message will be correctly recovered. Wavelet transform is performed to both cover image and secret message to achieve perfect and secure embedding. Secure and high volume payload steganography method for embedding secret messages into cover image without producing any major changes has been proposed. The proposed method gives better embedding payload and perceptual quality of stego-image than Wu and Lai methods. Also there are several parameters which have an impact in aspect of proposed method such as level of decomposition, level of thresholds. This parameters lead to change the number of elements in subset *E*. With increasing the elements of *E*, payload increased. The sender must make the best tradeoff between requirements. This approach can be applied to color image and tested with other transform techniques.

References

[1] D. C. Lou, "Steganography Method for Secure Communications", Computers & Security, vol. 21, no. 5, **(2000)**, pp. 449-460.
[2] A. Cheddad, J. Condell, K. Curran and P.M. Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods", Digital Signal Processing, vol. 90, no. 3, **(2010)**, pp.727-752.
[3] A. Nissar and A. H. Mir, "Classification of Steganalysis techniques", Digital Signal Processing, vol. 90, no. 6, **(2010),** pp. 1758-1770.
[4] R. Chandramouli and N. D. Memon," Steganography Capacity: a Steganalysis Perspective", SPIE Security Watermarking Multimedia Contents, vol. 5020, **(2003)**, pp. 173–177.
[5] G. Swain, "Steganography in Digital Images Using Maximum Difference of Neighboring Pixel Values", International Journal of Security and Its Application, vol. 6, no. 6, **(2013)**, pp. 284-294.
[6] H. H. Zayed, "A High-Hiding Capacity Technique for Hiding Data in images Based on K-Bit LSB Substitution," The 30th International Conference on Artificial Intelligence Applications, **(2005)**, pp. 23-28.
[7] G. Swain and S. K. Lenka, "LSB Array Based Image Steganography Technique by Exploring the Four Least Significant Bits", Communication in Computer and Information Science, vol. 270, no. 2, **(2012)**, pp. 479-488.
[8] Y. Tsai, J. T. Chen and C. S. Chan, "Exploring LSB Substitution and Pixel-value Differencing for Block-based Adaptive Data Hiding", International Journal of Network Security, vol. 16, no. 5, **(2014)**, pp. 359-364.
[9] A. S. Jamdar, A. V. Shah, D. D. Gavali and S. L. Kurkute, "Edge Adaptive Steganography Using DWT", International Journal of Engineering and Advanced Technology, vol. 2, no. 4, **(2013)**, pp. 648-652.
[10] D. C. Wu and W. H Tsi, "A Steganographic Method for Images by Pixel-Value Differencing", Pattern Recognition Letters, vol. 24, no. 9, **(2003)**, pp. 1613-1626.
[11] B. L. Lai and L. W. Chang, "Adaptive Data Hiding for Images Based on Haar Discrete Wavelet Transform", Advances in Image and Video Technology, **(2006)**, pp. 1085-1093.
[12] R. El Safy, H. H. Zayed and A. El Dessouki, "An Adaptive Steganographic Technique Based on Integer Wavelet Transform", International Conference on Networking and Media Convergence, **(2009)**, pp. 111-117.
[13] K. B. Raja, S. Sindhu, T. D. Mahalakshmi, S. Akshatha, B. K. Nithin, M. Sarvajith, K. R. Venugopal and L. M. Patnaik, "Robust Image Adaptive Steganography Using Integer Wavelets", Communication Systems Software and Middleware and Workshops, **(2008)**, pp. 614-621.
[14] W. Sweden, "The Lifting Scheme. A Construction of Second Generation Wavelets", SIAM Journal of Mathematical, Analysis, vol. 29, no. 2, **(1997)**, pp. 511–546.
[15] G. Uytterhoeven, D. Roose and A. Bultheel, "Wavelet Transforms Using the Lifting Scheme", International Technical Conference on Circuits/Systems Computers and Communications (ITC-CSCC'99), **(1997)**, pp. 6251-6253.
[16] S. Sarreshtedari, M. Ghobi and S. Ghaemmeghami, "High Capacity Image Steganography in Wavelet Domain", The 7th Annual IEEE Consumer Communications and Networking, **(2010)**, pp. 1-5.
[17] R. Roy, S. Changder, A. Sarkar, and N.C Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges", Computing, Management and Telecommunications**, (2013)**, pp. 21-24.
[18] Image database of BOSSBase V (0.92), http://exile.felk.cvut.cz/boss/BOSSFinal/index.php.
[19] J. Zollner, H. Federrath, H. Klimant, A. Pitzman, R. Piotraschke, A. Westfeld, G. Wicke and G Wolf, "Modeling the Security of Steganographic Systems," Information Hiding Workshop, **(1998)**, pp. 345-355.
[20] B. Li, J. He, J. Huang and Y Shi, "A Survey on Image Steganography and Steganalysis", Journal of Information Hiding and Multimedia Signal Processing, vol. 2, no. 2, **(2011)**, pp. 142-172.
[21] C. Cachin, "An Informationtheoretic Model for Steganography", Information and Computation, vol. 192, no. 1, **(2004)**, pp. 41-56.

[22] A. Martin, G. Sapiro and G. Seroussi, "Is Image Steganography Natural", IEEE Transactions on Image Processing, vol. 14, no. 12, **(2005)**, pp. 2040-2050.
[23] I. Avcibas, N. Memon and B Sankur, "Steganalysis Using Image Quality Metrics", IEEE Transaction on Image Processing, vol. 12, no. 3, **(2003)**, pp. 221–229.
[24] I. Avcibas, N. Memon, M. Kharrazi and B Sankur, "Image Steganalysis with Binary Similarity Measures", EURASIP Journal on Advances in Signal Processing, vol. 2005, no. 1, **(2005)**, pp. 2749–2757.
[25] I. Avcibas, B. Sankur and K. Sayood, "Statistical Evaluation of Image Quality Measures", Journal of Electronic Imaging, vol. 11, no. 2, **(2002)**, pp. 206-223.
[26] S. N. Mali, P. M. Patil and R. M Jaluekar, "Robust and secure image adaptive data hiding", Digital Signal Processing, vol. 22, no. 2, **(2012)**, pp. 314-323.

Authors

Seyyed Amin Seyyedi, he received the M.E in software engineering from Islamic Azad University, Iran 2008. He is a member of computer department in Islamic Azad University. Now he is studying for PhD in Belarusian State University Informatics and Radioelectronics. His research interests include image steganography and watermark.

Nick Ivanov, he took his PhD degree in applied mathematics from National Academy of Belarus in 1978. Now he is Associate Professor of Belarusian State University Informatics and Radioelectronics. He was supervisor for several Graduate students. His research interests include discrete mathematics, image analysis, and image steganography.

