A Secure Steganography Method Based on Integer Lifting Wavelet Transform

Seyyed Amin Seyyedi[1,3], Vasili Sadau[2], Nick Ivanov[3]
(Corresponding author: Seyyed Amin Seyyedi)
Department of Computer, Maku Branch, I.A.U, Maku, Iran[1]
5861993548, Maku, Iran
Department of Intelligent Systems, Belarusian State University[2]
No 4 St.Nezavisimosti, 220030, Minsk, Belarus
Department of Electronic Computing Machines, Belarusian State University of Informatics and Radioelectronics[3]
No 6 P.Brovki, 220013, Minsk, Belarus
(Email: amseyyedi@gmail.com)
(Received Nov. 18, 2013; revised and accepted July 20 & Nov 6, 2014)

Abstract

Steganography plays an important role in secret communication in digital worlds and open environments like Internet. Undetectability and imperceptibility of confidential data are major challenges of steganography methods. This article presents a secure steganography method in frequency domain based on partitioning approach. The cover image is partitioned into 8×8 blocks and then integer wavelet transform through lifting scheme is performed for each block. The symmetric RC4 encryption method is applied to secret message to obtain high security and authentication. Tree Scan Order is performed in frequency domain to find proper location for embedding secret message. Secret message is embedded in cover image with minimal degrading of the quality. Experimental results demonstrate that the proposed method has achieved superior performance in terms of high imperceptibility of stego-image and it is secure against statistical attack in comparison with existing methods.

Keywords: Cryptography, discrete wavelet transform, lifting scheme, steganography, statistical attack, tree scan order

1 Introduction

With development of the Internet and information processing techniques, data hiding has attracted lots of attention. Data hiding is a science of concealing information in a host medium that can be text, image, audio, video, etc without leaving any remarkable trace on the host medium [12, 35].Among the different kinds of digital media, the digital image is commonly used as a host image to convey side information in it. Hence, image hiding investigating is actual issue. Depending on the relationship between embedded information and the cover image, data hiding techniques are classified into steganography and watermark methods [15]. The major goal of steganography is to enhance communication security by inserting secret message into the digital image vs. copyright preserving; authentication and robustness are objectives of watermark techniques [9, 12].

Steganography is the art and science of transmission the secret message in such a way that the existence of information in container is undetectable [19, 21]. The word steganography is originally composed of two Greek words "steganos" and "graphia", which means "covered" and "writing" respectively. The notation of steganography was first introduced with the example of prisoners secret message by Simmons in 1983 [35].

There are a number of steganographic schemes hiding a secret message in an image file; these schemes can be classified according to the format of the cover image [13, 20] or the method of hiding.

Steganographic schemes in term of hiding method can be classified into two board categories namely spatial-domain techniques and frequency-domain techniques. In spatial domain techniques, the secret messages are embedded directly into cover image [8, 11, 14, 18, 22, 33, 34, 36]. The advantages of spatial domain methods are simple implementation, high payload and provide easy way to control, stego-image quality. The limitation of this approach is vulnerable to every slight steganalysis methods. Frequency domain techniques are popular data hiding approach [2, 6]. In frequency domain methods, the cover image converted into frequency domain coefficients before embedding the secret message in it. The most used transforms are the Fast Fourier Transforms (FFT), Discrete Cosines Transform (DCT), and Discrete Wavelet Transforms (DWT). Ability for high resistance against

steganalysis methods and signal processing manipulations are advantages of frequency domain techniques to spatial domain ones. But transformations into frequency domain are computationally complex. Wavelets transform is a thriving branch of these methods. Some of these techniques try to achieve the high payload hiding and low distortion in cover image.

The effort to detect the presence of secret message is called steganalysis. The steganalyst is assumed to control the transmission channel and watch out for suspicious material [19]. A steganalysis method is considered as successful, and the respective steganographic system as broken, if the steganalyst be able to detect the existence of the secret message. The detection ability of statistical analysis scheme depends on the volume of hidden message [10, 23]. Hence, a secure transfer of secret message based on wavelet transform with appropriate payload without ruining the invisibility and detection by steganalyst is the aim of this study.

This study devoted to frequency domain issues; therefore it is necessary to mention relevant methods in this domain. Kang et al. [16] proposed a steganographic method based on wavelet and modulus function. First, an image is divided into blocks of prescribed size, and every block is decomposed into one-level wavelet. Then, the capacity of the hidden secret data is coordinated with the number of wavelet coefficients of larger magnitude. Finally, secret information is embedded by modulus function. Lai et al. [17] proposed an adaptive data hiding method based on Haar wavelet transform. The cover image is divided 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 LSB method. Safy et al. [27] to enlarge capacity of hidden data proposed the modification of Lai's method. Abdelwahab et al. [1] proposed data hiding technique in DWT where 1-level DWT is applied to both cover and secret images. Each of sub bands is divided into 4×4 non-overlapping blocks. Block of secret message is compared with cover blocks to determine the best match. The disadvantage of this method is that extracted data not totally identical to the embedded version. Raja et al. [25] proposed an adaptive steganography using integer wavelet transform. Their scheme embeds the payload in non-overlapping 4×4 blocks of the low frequency sub band. Two pixels at a time are chosen based on condition number of each block one on either side of principal diagonal. Low embedding capacity and not considering reliability of method against statistical attacks are disadvantages of this method. Bhattacharyya et al. [5] proposed a novel steganographic scheme based on Integer Wavelet Transform (IWT) through lifting scheme. The Pixel Mapping Method (PMM) is used to embed 2 bits of secret message into selected sub band to form the stego-image. The disadvantage of this method is low quality of stego-image and low payload size. Reddy et al. [26] proposed wavelet based non LSB steganography. The cover image is divided into 4×4 non-overlapping blocks, DWT/IWT applied to each block. The 2×2 cells of HH sub band are considered and manipulated with secret message bit pairs using identity matrix to generate stego-image. Seyedi et al. [28] proposed a new robust image adaptive steganography method in frequency domain. The proposed steganography method embeds the secret data in the blocks of an image that seems to be noisy based on the bit plane complexity of each block and does not destroy the co-occurrence matrix of wavelet coefficient. They used the one-third and rounding methods for embedding data in wavelet coefficients, and retain the co-occurrence matrix of wavelet coefficient. In comparison with methods mentioned earlier, our method provides better quality of image with reasonable payload, especially, high secrecy against steganalysis attacks.

This article presents frequency domain image steganography technique based on IWT through lifting scheme (LWT). In addition, to achieve higher security and authentication 56-bit key RC4 encryption method applied to the secret message before embedding procedure. Tree Scan Order (TSO) is performed in frequency domain to find the proper location of secret message. Secret message is embedded in cover image without degrading the quality of the original image.

The rest of this article organized as follows. Section two discusses the IWT based on lifting scheme. Section three presents a cryptography method. Section four presents the proposed image steganography technique. Section five presents experimental results and analysis. Conclusion is given in section six.

2 Integer Wavelet Transform Based on Lifting Scheme

Wavelets are special functional base for signal decomposition. As shown in Figure 1, applying two dimensional wavelet transform to an image represents it in four bands called LL, HL, HL, and HH. The LL band contains low pass coefficients and three other bands represent high pass coefficients of the image, including horizontal, vertical and diagonal features of the original image. The same decomposition can be applied to LL band.

Generally, wavelet filters have floating point coefficients, hence, when the input data consist of a set of integers (as in the case for images), the resulting filtered output has float point format, which does not allow exact reconstruction of the original image. However, exploiting wavelet transform with integer output provides exact inverse transform. Particularly, lifting scheme can be completely realised with integers. Above all, lifting scheme does not require temporary storage in the calculation steps [31].

In this paper biorthogonal Cohen-Daubechies Feauveau (CDF 2/2) lifting scheme was chosen as a case study.

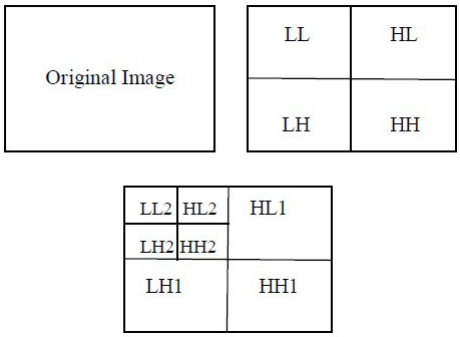

Figure 1: One level and two levels 2D wavelet transform

3 Cryptography and Steganography

One of the approaches to increasing security level of steganographic system is cryptography. Usually symmetric encryption method is recommended for steganographic methods. The symmetric encryption is a method that uses the identical key to encrypt and decrypt a secret message. In secure transmission of confidential data between parties, each party must agree on shared secret key. Based on Kerckhoffs principle [24], the security of encrypted data depends on the secrecy of the key. If attacker gains knowledge of the secret key, he can use the key to decrypt all the data. There are several algorithms for symmetric key encryption, one of them is RC4 [30].

In this paper symmetric encryption method RC4 with 56-bit key is utilized to encrypt secret message.

4 Proposed Method

In this article, a wavelet domain steganography is adopted for hiding reasonable amount of secret data with high security, good visibility and no loss of secret message. The cover image is partitioned into non-overlapping 8×8 blocks and 2D Integer LWT (IntLWT) is applied to each block. TSO is performed in transformed blocks to identify proper location of secret message. In addition, to achieve higher security and authentication 56-bit key RC4 encryption method is applied to the secret message before embedding it. The block diagram of proposed data embedding process is shown in Figure 3.

4.1 Embedding Region

The main idea behind the proposed algorithm is that secret message bits embed in proper frequency coefficients without visually degrading the quality of the original image. The TSO is applied to each transformed block to identify proper location of secret message.

4.2 Tree Scan Order

In the wavelet transform of an image, the energy in sub bands decreases as the level decomposition increases. Wavelet coefficients in upper sub bands have larger values [29]. It is possible be an edge. For human vision, the edge region has higher priority to embed the data than the smooth region. The trick is now to exploit the dependency between the wavelet coefficients across level decomposition. When 8×8 block of an image is wavelet transformed in three levels, ten sub bands will obtain as shown in Figure 3. In tree scan order upper sub (LL3) band is main root sub band. Figure 3 shows tree scanning order.

TSO use a series of decreasing thresholds and compares the wavelet coefficients with those thresholds. If the magnitude of a coefficient is smaller than a given threshold the node is called insignificant with respect to given threshold. Otherwise, the coefficient is significant. Initial threshold is calculated as:

$$T_1 = 2^{\lfloor log_2 max(B(i,j)) \rfloor} \quad (1)$$

$$T_n = \frac{T_n - 1}{2} \quad (2)$$

here $max(\cdot)$ signifies the maximum coefficient value in 8×8 block of an image and $B(i, j)$ denotes coefficients in 8×8 block.

In accordance to tree scan structure, there are spatially relation between lowest insignificant frequency coefficient at the node and children of each tree node in the next frequency sub band. The TSO is developed based on decreasing the wavelet coefficients with level of decomposition. The proposed method exploits this property for embedding secret message only into root coefficients. The coefficient is named as Root Coefficient (RC) if the value of the coefficient and its descendants are less than the threshold. RCs are the proper coefficients for embedding secret message. In proposed method threshold value for each block is calculated in three levels (T_3).

4.3 Embedding and Extracting Algorithms

Proposed secret message embedding algorithm for security point of view data transmission comprises the steps shown in Algorithm 1.

The extraction procedure consists of steps shown in Algorithm 2.

5 Experimental Results

Some experiments were conducted to assess the efficiency of the proposed method based on data payload, fidelity and security benchmarks [19]. The method has been simulated using the MATLAB 8.1 (R2013a) tools on Windows 7 version 6.1 platform. The secret message was generated randomly and RC4 of Microsoft encryption utility

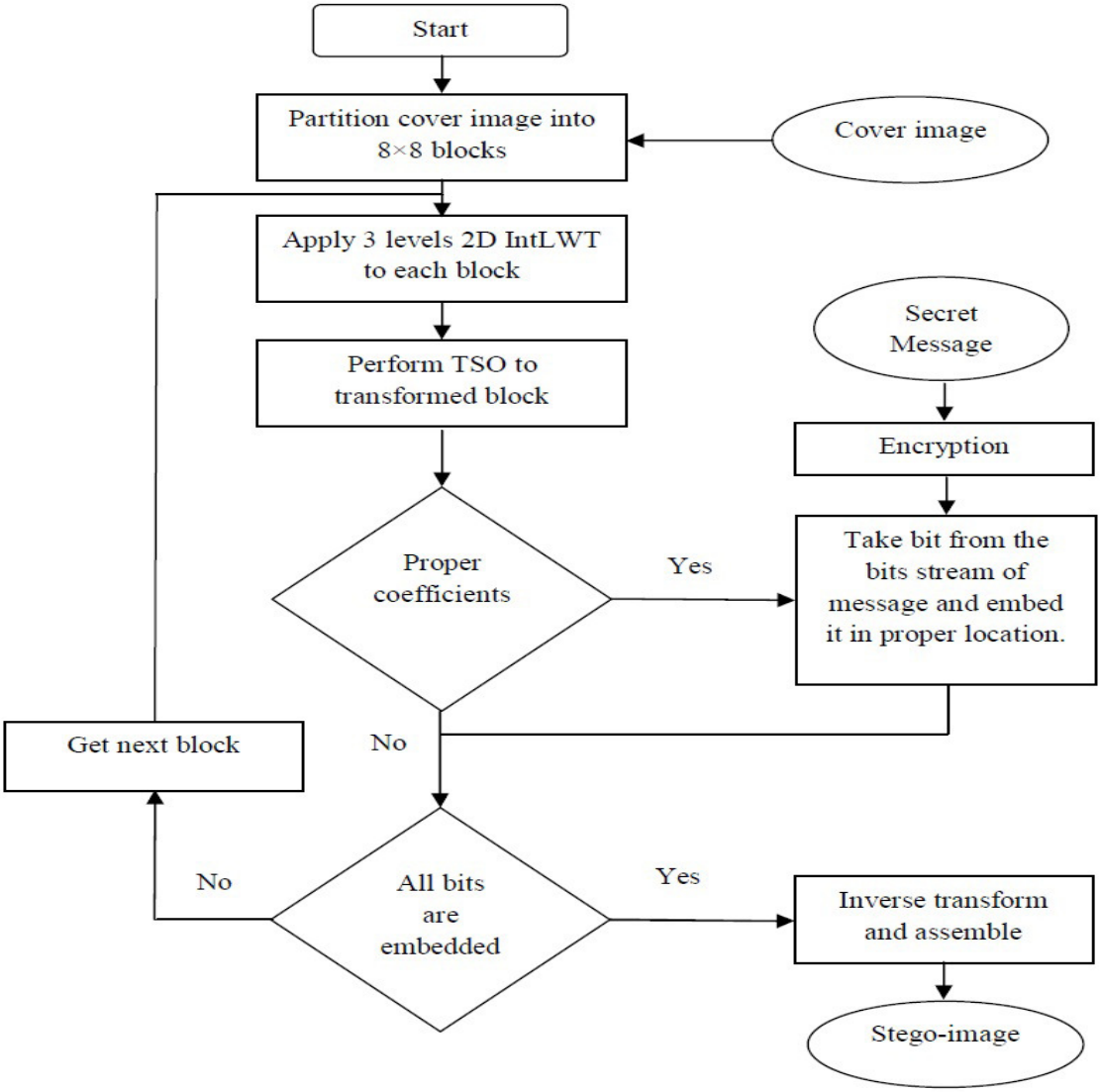

Figure 2: Data embedding process

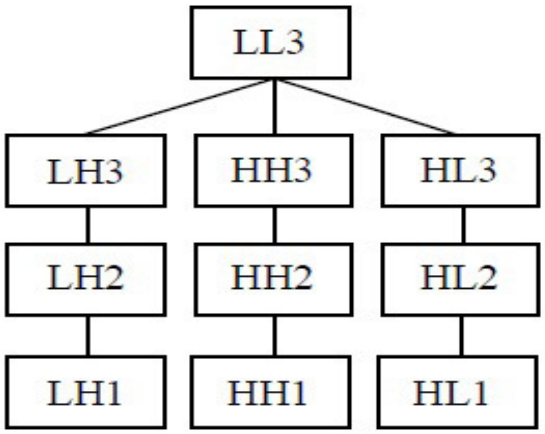

Figure 3: Tree scanning order

Table 1: Calculation of varies image similarity metrics of proposed method

Similarity metrics	Length of embedding message (byte)							
	500		1000		5000		10000	
512x512	Mean	St.Dev.	Mean	St.Dev.	Mean	St.Dev.	Mean	St.Dev.
PSNR	65.09	0.676	62.11	0.654	55.31	0.492	52.454	0.502
MSE	0.02	0.003	0.04	0.006	0.19	0.022	0.37	0.043

Algorithm 1 Embedding algorithm

1: Input: Cover image C of size $M \times N$ and secret message SE.
2: Output: Stego-image S.
3: Begin
4: Read cover image C.
5: Read the secret message SE and perform the RC4 encryption method on SE.
6: Partition C into 8×8 non-overlapping blocks.
7: Perform three levels IntLWT on each block.
8: Apply TSO to find RC coefficients for embedding secret message bits.
9: Embed SE bit by bit into RCs.
10: Perform inverse wavelet transform to each block.
11: Assemble stego-image S from blocks.
12: End

Algorithm 2 Extracting algorithm

1: Input: Stego-image S of size $M \times N$.
2: Output: Secret message SE.
3: Begin
4: Partition stego-image S into 8×8 non-overlapping blocks.
5: Apply three levels IntLWT to each block.
6: Find RCs and extract 1-LSB in each RC.
7: Decrypting extracted message by secret key.
8: End

program was used to encrypt the secret message. All experiments were conducted on image database of Granada University [32].

Usually, data payload of steganographic method is one of the evaluation criteria. Data payload refers to the amount of information that can be hidden in the cover image. The embedding rate is usually given in absolute measurement such as the size of the secret message or in bits per pixel, etc. It depends on the embedding function, size of cover image, and may also depend on properties of the cover image. Figure 4 shows the maximum data payload of proposed method.

Fidelity (imperceptibility) refers to inability of human eyes to distinguish between cover image C and stego-image S. Usually the fidelity of stego-image measures by various image similarity metrics such as Mean Square Error (MSE), and Peak Signal to Noise Ratio (PSNR). Mean Square Error (MSE) is a simple non-perceptual error metric that is obtained from the cover image C and stego-image S where lower value are assumed to be indicative of lesser detectability. The is calculated using following formula:

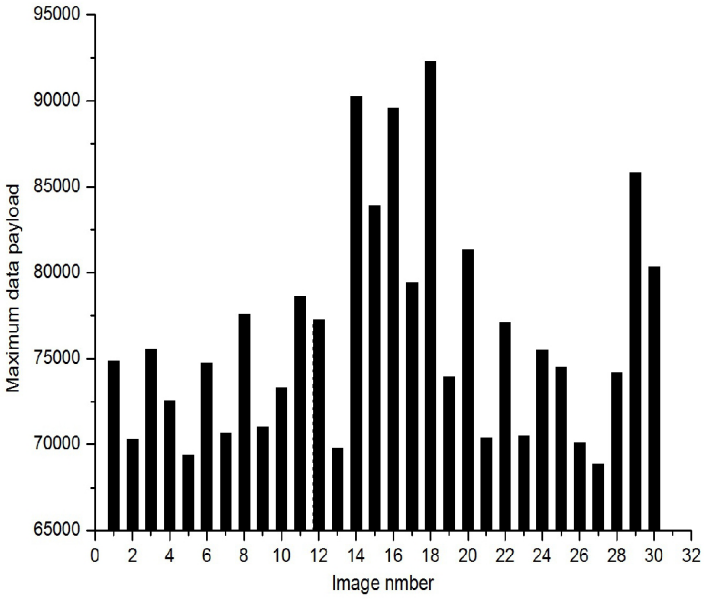

Figure 4: Maximum data payload of proposed method for several images

$$MSE = \frac{1}{(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} (C_{ij} - S_{ij})^2. \quad (3)$$

The peak signal-to-noise ratio (PSNR) is calculated using following formula:

$$PSNR = 20log_{10} \frac{Max}{MSE} dB, \quad (4)$$

where Max denotes the maximum pixel value of the image. A higher PSNR value indicates the better quality of stego algorithm. Human visual system is unable to distinguish the images with PSNR more than 36 [22].

Table 1 shows the imperceptibility metrics of proposed method with various payload sizes. In order to compare proposed method with the Bhattacharyya, Reddy, and Lai methods several sizes of gray scale image Lena is used. Table 2 shows the various payloads vs. PSNR value of proposed method, Bhattacharyya method, Reddy method

Table 2: Comparison PSNR value after embedding in cover image of Lena image

Image size	Message (Byte)	CA(B)	CH(B)	CV(B)	CD(B)	Reddy Method	Lai Method (K=1)	Proposed Method
128x128	100	53.29	54.91	54.66	58.83	41.16	56.39	59.02
	200	50.66	52.35	51.994	56.90	36.29	52.76	56.19
	400	47.89	49.34	48.97	54.49	35.95	48.36	53.65
	500	47.03	48.36	48.03	48.02	35.61	47.51	52.65
256x256	100	59.77	62.36	62.34	58.83	57.93	64.83	64.75
	200	56.73	58.74	58.75	56.90	50.38	60.24	62.33
	400	53.69	55.43	55.55	54.49	43.43	57.81	59.31
	800	50.77	52.66	52.31	51.84	38.83	53.42	56.37
	1600	47.67	49.49	49.16	49.04	N/A	49.87	53.52
	2000	47.77	48.56	51.09	48.12	N/A	48.74	52.58

and Lai method for 128×128 and 256×256 cover image Lena. CA (B), CH (B), CV (B), CD (B) in Table 2 respectively denotes Approximation Coefficient, Horizontal Coefficient, Vertical Coefficient, Diagonal Coefficient of Bhattacharyya method. As shown, proposed method results are better related to the other methods in term of quality of stego-image on the same payload.

Security of steganographic system is defined in term of undetectability. There are many approaches in defining the security of a steganographic method [19]. Zollner [8] theoretically proved that a steganographic system is secure, if secret message has a random nature and is independent from the cover image and stego-image. Cachin [7] defined a steganographic method (by Kullback-Leibler KL divergence) to be ϵ-secure ($\epsilon \geq 0$), if the relative entropy between probability distribution of cover image (P_C) and stego-image (P_S) are at most ϵ. The detectability (D) is defined by:

$$D(P_C||P_S) = \int P_C log \frac{P_C}{P_S}. \quad (5)$$

Thus, for a completely secure stego system D=0 and if $D \leq \epsilon$, then stego method is named ϵ-secure. In short, security of a stego method is defined in terms of undetectability. A steganography method is said to be undetectable or secure if the existence statistical tests cannot distinguish between the cover and the stego-image [17].

To compare the imperceptibility and security of proposed method with other methods, we did the experiments on the image data base [32]. Table 3 compares similarity and security metrics of proposed method with Lai and Reddy methods. According to it proposed method in same payload size is more imperceptible and secure than Reddy and Lai methods.

According to the results shown in Table 3, increasing the payload rate make conflict with imperceptibility metrics and security metrics.

5.1 Security Analysis of Proposed Method through Image Quality Metrics

Steganographic method is said to be undetectable or secure if the existence statistical tests cannot distinguish between the cover and the stego-images. During the embedding process in the cover image some statistical variations are arises. The stego-image is perceptually identical but is statistically different from the cover image. The attacker uses these statistical differences in order to detect the secret message. Recently various types of steganalysis methods for specific purposes have been developed in order to test the steganographic methods and detecting the stego-image from the cover image [23].

Avcibas et al. [3, 4] showed that embedding of secret message leaves unique artifacts, which can be detected using Image Quality Metrics (IQMs). There are twenty six different measures that are categorized into six groups as Pixel difference, Correlation, Edge, Spectral, Context, and Human visual system. Avcibas developed a discriminator for cover image and stego-image using a proper set of IQMs. In order to select appropriate set of IQMs, they used analysis of variance techniques. The selected IQMs for steganalysis are Minkowsky measures M1 and M2, Mean of the angle difference M4, Spectral magnitude distance M7, Median block spectral phase distance M8, Median block weight spectral distance M9, Normalized mean square HVS error M10. The IQMs scores are computed from images and their Gaussian filtered versions with $\alpha = 0.5$ and mask size 3×3.

The variations in IQMs for proposed method, Lai and Reddy methods with embedding the 4000 characters in cover images are computed. From experimental results it can be perceived that statistical difference between cover images and stego-images of proposed method is less than Lai and Reddy methods. Therefore, proposed method is more secured than Lai and Reddy methods. The warden cannot distinguish stego-image from cover image. The variations in IQMs for M7 and M9 are shown in Table 4.

Table 3: Comparison similarity and security metrics of proposed method with Lai and Reddy methods

Payload (Byte)	Metrics	Lai Method (K=1)		Reddy Method		Proposed Method	
		Mean	St.Dev.	Mean	St.Dev.	Mean	St.Dev.
500	PSNR	59.85	2.49	46.28	6.16	69.09	0.68
	MSE	0.078	0.041	3.485	4.632	0.02	0.003
	D	3.81E-03	6.922E-03	1.460E-04	1.560E-04	1.02E-06	4.87E-07
1000	PSNR	56.62	2.47	42.40	5.55	62.12	0.65
	MSE	0.163	0.084	7.420	9.165	0.04	0.006
	D	3.82E-03	6.99E-03	2.76E-04	2.69E-04	2.19E-06	1.12E-06
2000	PSNR	53.38	2.28	38.70	4.96	59.18	0.6
	MSE	0.337	0.16	15.672	19.217	0.079	0.011
	D	3.83-03	6.989E-03	4.82E-04	3.69E-04	5.37E-06	4.3E-06
4000	PSNR	50.12	2.1	34.97	4.7	56.24	0.506
	MSE	0.7	0.311	35.932	45.768	0.115	0.018
	D	3.85E-03	6.98E-03	9.88E-04	6.6E-04	1.36E-05	1.34E-05

Table 4: IQMs variation for M7, M9

M7: Spectral magnitude distance				
Image number	Original	Proposed Method	Reddy Method	Lai Method
1	0.4723	0.4723	0.5089	0.4740
2	0.0685	0.0690	0.0753	0.0691
3	0.1258	0.1263	0.1368	0.1278
4	0.3477	0.3479	0.3781	0.3393
5	0.1207	0.1210	0.1296	0.1240
6	0.3208	0.3213	0.3420	0.3080
7	0.6414	0.6415	0.7169	0.6279
8	0.6084	0.6085	0.6584	0.6047
9	0.1862	0.1865	0.2008	0.1866
10	0.1566	0.1568	0.1714	0.1571
M9: Median block weight spectral distance				
Image number	Original	Proposed Method	Reddy MEthod	Lai Method
1	9.1477	9.1477	9.1479	9.1478
2	9.1045	9.1095	9.1112	9.1055
3	9.1269	9.1268	9.1304	9.1274
4	9.1400	9.1394	9.1404	9.1396
5	9.1191	9.1194	9.1214	9.1189
6	9.1392	9.1394	9.1398	9.1388
7	9.1481	9.1481	9.1486	9.1478
8	9.1472	9.1473	9.1482	9.1469
9	9.1485	9.1484	9.1505	9.1478
10	9.1236	9.1236	9.1284	9.1236

6 Conclusions

The major goal is addressed to security of stego algorithm. The proposed method exploited the property of tree scanning order under the integer wavelet transformation with lifting scheme and blocking approach of cover image. The confidential information could be sent in lossy channels using proposed method because it does provide sufficient secrecy and stability against statistical attack. Two layers of security are used to preserve secrecy of embedded message. Furthermore, if an attacker successes to extract secret message he will not be able to read it. The quality of stego-image occurs to be better in comparison with considered methods.

References

[1] A. A. Abdelwahab and L. A. Hassaan, "A discrete wavelet transform based technique for image data hiding," in *International Conference on Networking and Media Convergence*, pp. 1–9, Tanta, Egypt, Mar. 2008.

[2] A. Al-Ataby and A. Fawzi, "A modified high capacity image steganography technique based on wavelet transform," *The International Arab Journal of Information Technology*, vol. 7, no. 4, pp. 358–364, 2010.

[3] 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, pp. 2749–2757, 2005.

[4] I. Avcibas, N. Memon, and B. Sankur, "Steganalysis using image quality metrics," *IEEE Transaction on Image Processing*, vol. 12, no. 3, pp. 221–229, 2003.

[5] S. Bhattacharyya and G. Sanyal, "Data hiding in images in discrete wavelet domain using PMM," *International Journal of Electrical and Computer engineering*, vol. 5, no. 6, pp. 597–606, 2010.

[6] K. Blossom, K. Amandeep, and S. Jasdeep, "Steganographic approach for hiding image in DCT domain," *International Journal of Advances in Engineering & Technology*, vol. 1, no. 3, pp. 72–78, 2011.

[7] C. Cachin, "An information theoretic model for steganography," *Information and Computation*, vol. 192, no. 1, pp. 41–56, 2004.

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 496–474, 2003.

[9] R. Chandramouli, M. Kharrazi, and N. Memon, "Image steganography and steganalysis concepts and practice," in *Digital Watermarking*, pp. 35–49, Seoul, Korea, Oct. 2003.

[10] R. Chandramouli and N. D. Memon, "Steganography capacity: A steganalysis perspective," *Security Watermarking Multimedia Contents*, SPIE 5020, pp. 173–177, 2003.

[11] C. C. Chang, J. Y. Hasiao, and C. S. Chan, "Finding optimal least significant bit substitution in image hiding by dynamic programming strategy," *Pattern Recognition*, vol. 36, no. 7, pp. 1583–1598, 2003.

[12] 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, pp. 727–752, 2010.

[13] M. Fallahpour, D. Megias, and M. Ghanbari, "Reversible and high-capacity data hiding in medical images," *IET Image Process*, vol. 5, no. 2, pp. 190–197, 2011.

[14] W. Hong, T. S. Chen, and C. W. Luo, "Data embedding using pixel value differencing and diamond encoding with multiple-base notational system," *The Journal of Systems and Software*, vol. 85, pp. 1166–1175, 2012.

[15] L. Ch Huang, L. Y. Tseng, and M. S. Hwang, "A reversible data hiding method by histogram shifting in high quality medical images," *Journal of Systems and Software*, vol. 86, no. 3, pp. 716–727, 2013.

[16] Z. Kang, J. Lin, and Y. He, "Steganography based on wavelet transform and modulus function," *Journal of Systems Engineering and Electronics*, vol. 18, no. 3, pp. 628–632, 2007.

[17] B. L. Lai and L. W. Chang, "Adaptive data hiding for images based on harr discrete wavelet transform," in *Advances in Image and Video Technology,Lecture Notes in Computer Science*, pp. 1085–1093, Hsinchu, Taiwan, December 2006.

[18] Y. P. Lee, J. C. Lee, W. K. Chen, K. C. Chang, I. J. Su, and C. P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing," *Information Sciences*, vol. 191, pp. 214–225, 2012.

[19] B. Li, J. He, and J. Q. Shi, "A survey on image steganography and steganalysis," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 2, no. 2, pp. 142–172, 2010.

[20] G. Liang, S. Wang, and X. Zhang, "Steganography in binary image by checking data-carrying eligibility of boundary pixels," *Journal of Shanghai University*, vol. 11, no. 3, pp. 272–277, 2007.

[21] C. S. Lu, *Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property.* USA: Idea Group, 2005.

[22] H. C. Lu, Y. P. Chu, and M. S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," *A new steganographic method of the pixel-value differencing*, vol. 50, no. 5, pp. 424–426, 2006.

[23] A. Nissar and A. H. Mir, "Classification of steganalysis techniques," *Digital Signal Processing*, vol. 90, no. 6, pp. 1758–1770, 2010.

[24] D. Omerasevic, N. Behlilovic, and S. Mrdovic, "Cryptostego a novel approach for creating cryptographic keys and messages," in *Signals and Image Processing (IWSSIP)*, pp. 83–86, Bucharest, Romania, July 2013.

[25] 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," in *Communication Systems Software and Middleware (COMSWARE)*, pp. 614–621, Bangalore, India, Jan 2008.

[26] H. S. M. Reddy and K. B. Raja, "Wavelet based non LSB steganography," *International Journal Advanced Networking and Applications*, vol. 3, no. 3, pp. 1203–1209, 2011.

[27] R. O. El Safy, H. H. Zaye, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," in *International Conference on Networking and Media Convergence*, pp. 111–117, Cario, Egypt, March 2009.

[28] S. H. Seyedi, H. Aghaeinia, and A. Sayadian, "A new robust image adaptive steganography method in wavelet transform," in *IEEE Electrical Engineering*, pp. 1–5, Tehran, Iran, May 2011.

[29] J. Shapiro, "Embedded image coding using zero tree of wavelet coefficients," *IEEE Transaction on Signal Processing*, vol. 41, no. 12, pp. 3445–3462, 1993.

[30] N. Smart, *Cryptography: An Introduction.* USA: McGraw-Hill College, 2004.

[31] W. Sweden, "The lifting scheme: A construction of second generation wavelets," *SIAM Journal on Mathematical Analysis*, vol. 29, no. 2, pp. 511–546, 1997.

[32] University of Granada, *Miscelaneous Gray Level Test Images (512 × 512)*, July 3, 2015. (http://decsai.ugr.es/cvg/dbimagenes/g512.php)

[33] C. M. Wang, N. I. Wu, C. S. Tsai, and M. S. Hwang, "A high quality steganographic method with pixel-value differencing and modulus function," *The Journal of Systems and Software*, vol. 81, no. 1, pp. 150–158, 2008.

[34] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image steganographic scheme based on pixel-value

differencing and LSB replacement methods," *IEEE Proceedings of Vision, Image and Signal Processing*, vol. 152, no. 5, pp. 611–615, 2005.

[35] N. Wu and M. S. Hwang, "Data hiding: Current status and key issues," *International Journal of Network Security*, vol. 4, no. 1, pp. 1–9, 2007.

[36] N. I. Wu, K. C. Wu, and C. M. Wang, "Exploring pixel-value differencing and base decomposition for low distortion data embedding," *Applied Soft Computing*, vol. 12, no. 2, pp. 942–960, 2012.

Seyyed Amin Seyyedi took his PhD degree in Methods and Systems of Information Protection, Information Security from Belarusian State University of Informatics and Radioelectronics in 2014. He is a member of computer department in Islamic Azad University. He has published one monograph and more than twenty publications in national and international scientific journals and conferences.His research interests include image steganography and watermark.

Vasili Sadau took his PhD degree in engineering science from National Academy of Belarus in 1984. Now he is Professor of Belarusian State University. He has published one monograph and more than sixty publications in national and international scientific journals and conferences.His research interests include the problems of information security in computer systems.

Nick Ivanov 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.