International Journal of Advanced Studies in Computer Science & Engineering
IJASCSE, Volume 3, Issue 3, 2014

A Novel Secure Steganographic Method Based on Zero Tree Method

Seyyed Amin Seyyedi, Nick Ivanov
Department of electronic computers, Belarusian State University of Informatics and Radioelectronics
Minsk, Belarus.

***Abstract*—a secure steganographic method is proposed for embedding secret messages into gray scale images in frequency domain based on partitioning approach. The cover image is divided into 8×8 non-overlapping blocks and integer wavelet transform through lifting scheme is performed for each block. In order to find proper location for embedding secret message, the zero tree method is applied to each block. The lossless data compression encoding applied to secret message to obtain high secrecy, high payload and authentication. Secret message embedded in cover image without degrading the quality of the original image. Simulation result reveals that, the proposed method has achieved better performance in terms of high data embedding payload, high imperceptibility of stego-image and secure against statistical attack compared with existing methods.**

Keywords: Steganography, Discrete Wavelet Transform through Lifting Scheme, Zero Tree Method, Arithmetic Coding, Statistical Attack, Image Quality Metrics.

I. INTRODUCTION

As the internet becomes main communication channel to transmit wide verity of data, there is a great need for security of information to prevent unauthorized access. Data hiding is a science that its aim is hiding the information in a media such as image without any remarkable trace on that media [1-2]. Steganography is a branch of data hiding. The objectives of steganography methods are secret communication and concern to undetectability and data payload [3].

Steganography is the art and science of transmission the secret message in such a way that the existence of information is undetectable [4-5].Steganography schemes can be classified into two board categories namely spatial-domain techniques and frequency-domain techniques [3-4]. Spatial domain techniques have a little complexity and more data payload relate to frequency domain but less secure against steganalysis methods. Frequency domain methods especially wavelets take advantage of the Human Visual System (HVS), low sensitivity to modifying in high and middle frequency coefficients.

Steganalysis is the science of detecting secret message. The goal of steganalysis method is to detect presence of secret message. Recently various types of steganalysis methods have been developed [6]. The detection ability of steganalysis scheme depends on the payload of hidden message. Hence, this fact imposes an upper bound limit for embedding payload, such that if the hidden data size is less then that upper bound, one may assert that the stego-image is safe and the statistical methods cannot detect it [6, 7]. A secure transfer of secret message with appropriate payload without ruining the invisibility is the aim of this study.

This article presents a frequency domain image steganography technique based on integer wavelet transform through lifting scheme of the cover image. In addition to achieve higher security and payload, arithmetic coding applied to the secret message before embedding it. Zero Tree Method (ZTM) is performed in frequency domain to find proper location of secret message. Secret message embedded in cover image without degrading the quality of the original image.

II. RELATED WORKS

Various image steganographic methods have been proposed in the literature.

Xinpeng Zhang [8] described a novel coding method for digital steganography in which the amount of bit alterations introduced into a cover medium significantly reduced, leading to less distortion and enhanced security against steganalysis. The proposed method works in a running manner thereby representing the secret bits by a series of consecutive cover bits. Filliping of one cover can be used to insert several consecutive secret bits. The channel noise is fatal for secret data extraction because any cover bit error will cause several bit errors in the extracted message.

Abdelwahab [9] proposed data hiding technique in Discrete Wavelet Transform (DWT) domain where 1-level DWT is performed on both secret and cover images. Each of sub bands is divided to 4×4 non-overlapping blocks. Block of secret message fit into cover blocks to determine the best match. The disadvantage of this method is extracted data not totally identical to the embedded version.

Raja [10] proposed an adaptive steganography using integer wavelet transform. His 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 methods against statistical attacks are disadvantages of this method.

Bhattacharyya [11] proposed a novel steganography scheme base on integer wavelet transform domain through lifting scheme. The Pixel Mapping Method (PMM) used to

embed 2 bit secret message in selected sub band to form the stego-image. The disadvantage of this method is low quality of stego-image and payload size.

Reddy [12] proposed wavelet based non LSB steganography. The cover image is divided into 4×4 non-overlapping blocks, Discrete and Integer Wavelet Transform (DWT/IWT) is applied to each block. The 2×2 cell of HH sub band of transformed block are considered and manipulated with secret message bit pairs using identity matrix to generate stego-image. The disadvantages of this method are low quality of stego-image and fixed payload size.

In comparison with other methods mentioned earlier, proposed method provides better quality of stego-image, increases embedding payload, especially, secure against steganalysis attacks.

III. PARAMETERS FOR EVALUATING STEGANOGRAPHIC ALGORITHMS

The performance of steganographic algorithms is evaluated by some benchmarks. Imperceptibility (fidelity), payload and security are three main parts of steganographic methods which are described below: [3, 4, 13]

A. *Imperceptibility*

Fidelity refers to inability of human eyes to distinguish between cover image and stego-image. 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) between the cover image (C) and the stego-image (S) is defined as follows:

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

The PSNR is computed using the following formula:

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

where Max denote the maximum pixel value of the image. A higher PSNR value indicates the better quality of used stego algorithm. HVS is unable to distinguish the images with PSNR more than 36 dB [10].

B. *Payload*

Payload refers to the amount of information that can be hidden in the cover image. The embedding rate is mostly given in absolute measurement (such as the size of the secret message) or in relative measurement called the data embedding rate (given mostly in bits per pixel or bpp, etc.)

.

C. *Security*

There are many approaches in defining the security of a steganographic method. Zollner [14] theoretically proved that a steganography system is secure, if secret message has a random nature and it is independent form cover image and stego-image. Cachin [15] defined a steganographic method 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 (security) $D(P_c \parallel P_s)$ is defined by:

$$D(P_c \parallel P_s) = \int P_c \log \frac{P_c}{P_s} \leq \varepsilon \qquad (3)$$

Thus, for a completely secure stego system, D=0 and if D≤ε, then stego system is ε-secure. In short, security of a stego system is defined in terms of undetectability. A steganographic method is said to be undetectable or secure if the existent statistical tests cannot distinguish between the cover and the stego-image [4, 13].

IV. THE PROPOSED IMAGE STEGANOGRAPHIC METHOD

A secure steganography technique is proposed for hiding secret message into cover image. In this article, a frequency domain steganography is adopted for hiding appropriate amount of data with high security, good visibility and no loss of secret message. The cover image partitioned into non overlapping 8×8 blocks and 2D Integer Wavelet Transform through Lifting schemes (IntLWT) is performed for each block. This can overcome the difficulty of floating point conversion that occurs after embedding. In addition to achieve higher security and payload, arithmetic coding is applied to the secret message before embedding secret message. ZTM is performed in frequency domain to identify proper location of secret message. The block diagram of proposed method is shown in figure 1.

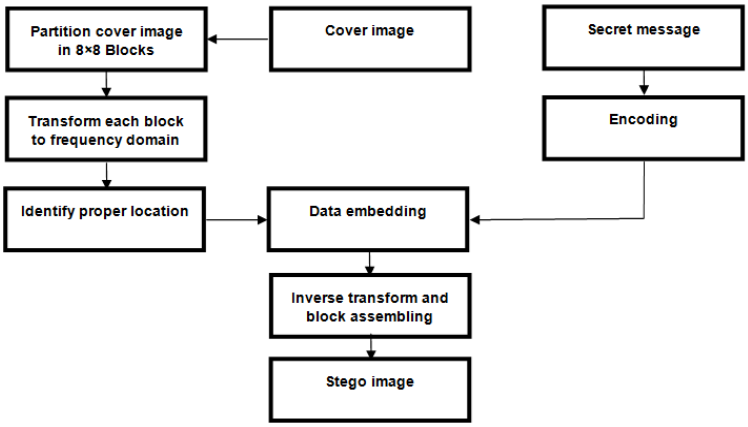


FIGURE 1 BLOCK DIAGRAM OF PROPOSED METHOD

A. *Discrete Wavelet Transform*

Multi Resolution Analysis is the main theory in wavelets that analyzes a signal in frequency domain in detail. In this transform, spatial domain is passing through low pass and high pass filter to extract low and high frequencies respectively. Applying one level 2D wavelet transform on image, decompose the cover image into four non overlapping sub bands by namely LL1, LH1, HL1 and HH1 as shown in figure 2. The sub bands LL1 include the low pass coefficient and presents a soft approximation of image. Other three sub bands show respectively horizontal, vertical and diagonal details. Approximation sub band is processed further to obtain the next coarser scale of wavelet coefficient until determine scale N is attained. When N scale is attained we will have 3N+1 sub bands.

Since human eyes are much sensitive to the low frequency part (LL sub-image), LL is the most important component in the decomposition process.

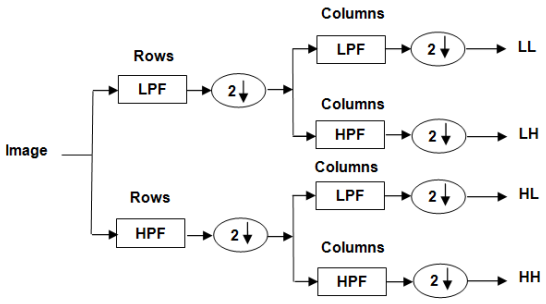


FIGURE 2 ONE LEVEL 2D DISCRETE WAVELET TRANSFORM

1) *Integer Wavelet Transform through Lifting Schme*

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 phase a) Split phase, b) Predicate phase, c) Update Phase. Figure 3 represent the generic scheme. An advantage of lifting scheme is that they do not require temporary storage in calculation step and the inverse transform has exactly the same complexity as the forward transform [16, 17].

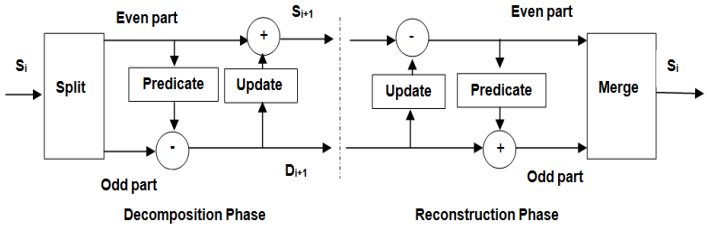


FIGURE 3 THE LIFTING SCHEME

In many image processing applications the input data consists of integer samples. Unfortunately wavelet filters return floating point values as wavelet coefficients. When one hides data in their coefficients any truncations of the floating point values of the pixels that should be integers may make the loss of the hidden information which may lead to the failure of the data hiding method. To overcome the difficulty of floating point can be applied integer wavelet transform.

In this paper biorthogonal Cohen-Daubechies-Feauveau (CDF 2.2) lifting scheme was chosen as a case study. The integer forward transforms formula of CDF 2.2 as follows [17]:

$$\text{Splitting: } \begin{cases} S_i \leftarrow x_{2i} \\ d_i \leftarrow x_{2i+1} \end{cases}, \tag{4}$$

$$\text{Predicate: } d_i \leftarrow d_i - \left\lfloor \frac{1}{2}(s_i + s_{i+1}) + \frac{1}{2} \right\rfloor, \tag{5}$$

Update: $s_i \leftarrow s_i + \left\lfloor \frac{1}{4}(d_{i-1} + d_i) + \frac{1}{2} \right\rfloor$, (6)

x denotes the original signal and inverse transform as:

Inverse update $s_i \leftarrow s_i - \left\lfloor \frac{1}{4}(d_{i-1} + d_i) + \frac{1}{2} \right\rfloor$, (7)

Inverse predicator $d_i \leftarrow d_i + \left\lfloor \frac{1}{2}(s_i + s_{i+1}) + \frac{1}{2} \right\rfloor$, (8)

Merging $\begin{cases} x_{2i} \leftarrow s_i \\ x_{2i+1} \leftarrow d_i \end{cases}$. (9)

B. Encryption

To achieve more security and payload, lossless compression coding is applied to secret message. Normally, a string of characters such as the words "Hello Dear" is represented using a fixed number of bits per character, as in the ASCII code. When a string is converted to arithmetic encoding, frequently used characters will be stored with fewer bits and not-so-frequently occurring characters will be stored with more bits, led to get shorter code in total. Arithmetic coding differs from other forms of lossless encoding such as Huffman coding in that rather than separating the input into component symbols and replacing each with a code, arithmetic coding encodes the entire message into a single number [18].

C. Data Embedding

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. In order to identify proper location of secret message, ZTM applied on each block after transformation.

1) Zero Tree Method

ZTM in frequency domain is an effective image compression algorithm [19]. Natural images in general have a low pass spectrum. 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. ZTM use a series of decreasing thresholds and compare the wavelet coefficients with those thresholds. If the magnitude of a coefficient is smaller than a given threshold T, the node is called insignificant with respect to given threshold. Otherwise, the coefficient is significant. The zero tree structure is shown in figure 4.

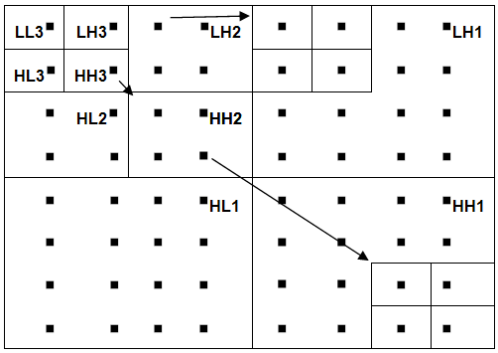


FIGURE 4 ZERO TREE STRUCTURE

2) Embedding algorithm

In accordance to ZTM method, there are spatially related between lowest frequency coefficient at the node and children of each tree node in the next frequency sub band. The ZTM is developed based on decreasing the wavelet coefficients with scale. The proposed method, exploits this property for embedding secret message only in root coefficients. The coefficient named as a Root Coefficient (RC) that the value of coefficient and its descendants are less than threshold. In proposed method threshold value for each block is calculated in three levels.

Propose secret message embedding scheme comprises the following steps:

Input: *Cover image C of size* $M_c \times N_c$ *and n-bit secret message SE.*

Output: *Stego- image S.*

Step 1: Read cover image C.

Step 2: Read the secret message SE and perform arithmetic coding.

Step 3: Partition the cover image C into 8×8 blocks Bl (i, j).

$$C = \sum_{i=1}^{M_c/8} \sum_{j=1}^{N_c/8} Bl(i, j) \quad (10)$$

Step 4: Transform each blocks to frequency domain (3-levels)

$$Temp(i, j) = IntLWT \quad Bl(i, j) \quad (11)$$

Step 5: Apply ZTM to find RCs for embedding secret message bits

$$T_0 = 2^{\lfloor \log_2 \max(temp) \rfloor}, \quad (12)$$

$$T_n = \frac{T_{n-1}}{2} \quad (13)$$

Temp and n denotes the coefficient values in each block and number of level respectively.

Step 6: Embed SE bit by bit into RCs in each block.
Step 7: Apply Inverse Wavelet Transform (IWT) for each block.
Step 8: Assemble stego-image S from blocks.

V. EXPERIMENTAL RESULT

In this section, some experiments are carried out to assess the efficiency of the proposed scheme. 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. All experiments are conducted on image database University of Granada [20] and University of Wisconsin-Madison [21]. Some results of proposed method are presented on four well know 512×512 gray scale images respectively "Barbara", "peppers", "Baboon" , and "Lena" are shown in figure 5. Howbeit the results presented here confined to four well know images. The proposed method tested on other sets [20, 21] of gray scale images and the results obtained were statistically relevant. Steganography performance is analysed using benchmarks mentioned in section III.

FIGURE 5 COVER IMAGES

Table 1 shows the imperceptibility and ε-secure analysis of proposed method with various payload sizes. According to the results shown in table 1, increasing the payload rate, make conflict with imperceptibility metrics and security metrics.

Also several sizes of gray scale images "Lena" and "Peppers" used to compare proposed method to the Bhattacharyya and Reddy methods. The maximum payload and quality of stego-image are used as measures of comparison. Table 2 compares the maximum embedded payload of the proposed method with Bhattacharyya [11] and Reddy [12] methods. Figures 6 (a, b) shows the various payloads vs. PSNR value of proposed method, Bhattacharyya method and Reddy method for 128×128 and 256×256 cover image "Lena". CA(S), CH(S), CV(S), CD (S) in figures 6 (a, b) 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 terms of maximum payload and quality of stego-image on the same payload.

To compare the imperceptibility and security of proposed method with Reddy method, author did the experiments on the [20] image data base. Table 3 shows results, according to it proposed method in same payload size is more imperceptible and secure than Reddy one.

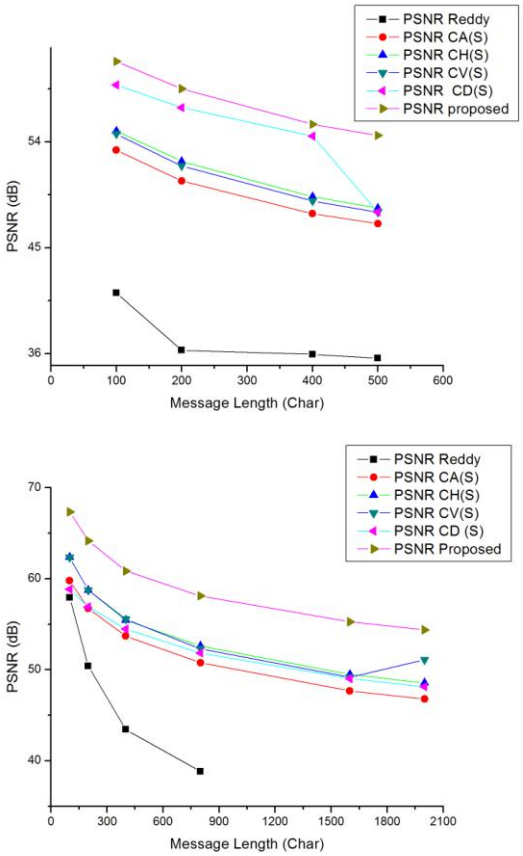


FIGURE 6 A, B) PAYLOAD VS. PSNR VALUE FOR 128×128 AND 256×256 COVER IMAGE "LENA"

A. *Security analysis of proposed method*

During the embedding process in the cover image some statistical variations are arises. The warden may exploit this approach to detect secret message in suspected image. The steganographic method is secure if existing statistical tests cannot distinguish between the cover and the stego-image. Avcibas [22, 23] proposed steganalysis method based on hypothesis that steganography schemes leave statistical evidence that can be exploited for detection with the aid of image quality metrics. He developed a discriminator for cover image and stego-images using an appropriate set of IQMs. There are twenty-six image quality metrics. These quality metrics are categorized into six groups according to the type of information [24].

In order to select appropriate set of IQMs, He 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.

TABLE I. CALCULATION OF VARIES IMAGE SIMILARITY METRICS FOR ANALYZING FIDELITY AND SECURITY OF STEGO-IMAGES

image	Parameters	Length of embedding message (in Char)					
		100	500	1000	5000	10000	15000
Barbara	PSNR	73.9847	66.6084	63.6462	56.5558	53.6449	52.0214
	MSE	0.0026	0.0142	0.0281	0.1437	0.2809	0.4083
	D	1.03E-07	6.06E-07	1.40E-06	6.48E-06	1.20E-05	1.99E-05
Peppers	PSNR	74.1208	66.6049	63.7829	56.5369	53.5677	51.8984
	MSE	0.0025	0.0142	0.0272	0.1443	0.286	0.42
	D	1.29E-07	6.28E-07	1.35E-06	2.16E-05	2.69E-05	1.45E-05
Baboon	PSNR	75.6230	68.1832	62.8931	56.0556	53.3218	51.7554
	MSE	0.0018	0.0099	0.0334	0.1613	0.3026	0.4341
	D	7.11E-08	3.84E-07	7.77E-07	3.62E-06	7.72E-06	1.67E-05
Lena	PSNR	73.5830	66.0754	63.0062	56.1847	53.3821	51.6504
	MSE	0.0028	0.0161	0.0325	0.1565	0.2984	0.4447
	D	8.83Ee-08	4.95E-07	1.04E-06	5.42E-06	1.12E-05	1.75E-05

TABLE II. COMPARISON THE EMBEDDING PAYLOAD OF THE PROPOSED METHOD WITH BHATTACHARYYA AND REDDY METHODS

Image	Size	Reddy embedding Payload (bit)	Bhattacharyya embedding payload (bit)	Payload of proposed method (bit)
Lena	128×128	2048	2240	5145
	256×256	8192	9536	20622
	512×512	32768	40048	82578
Peppers	128×128	2048	2832	5223
	256×256	8192	4440	20694
	512×512	32768	46776	83846

The IQM scores are computed from images and their Gaussian filtered versions with $\delta = 0.5$ and mask size 3×3 for selected IQMs [24, 25] as shown in figure 7.

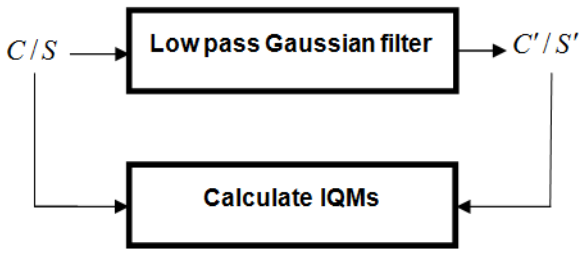


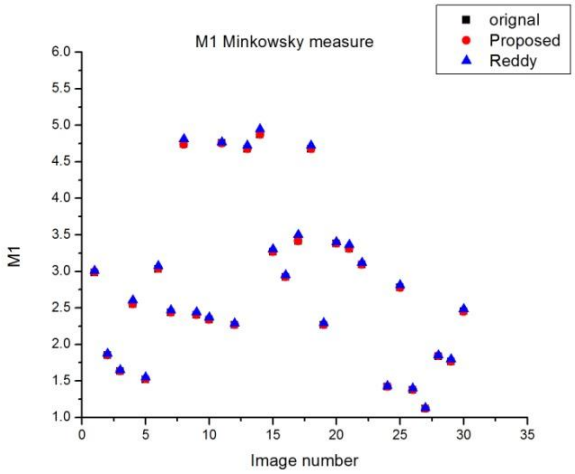
FIGURE 7 CALCULATION IQM SCORES

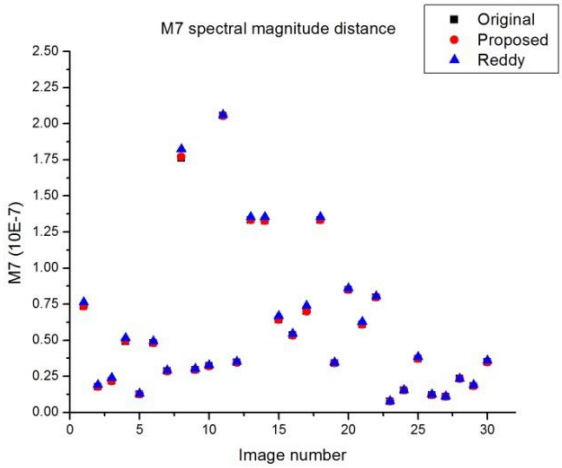
The variations in IQMs for proposed and Reddy method with embedding the 4096 bytes in cover images were considered. From experimental results it can be perceived that statistical difference between cover images and stego- images of proposed method is less than Reddy method. Therefore proposed method is more secured than Reddy method. The warden can't distinguish stego-image from cover image.

The variations in IQMs for M1, M7, M8 and M9 are shown in figure 8 (a-d).

TABLE III. COMPARISON SIMILARITY AND SECURITY METRICS OF PROPOSED METHOD WITH REDDY METHOD

Payload (Byte)	Metrics	Proposed Method		Reddy Method	
		Mean	Std. Dev.	Mean	Std. Dev.
4096	PSNR	57.33274	0.120827	37.42022	4.232482
	MSE	0.461819	0.012776	18.35051	18.47957
	D	6.14E-06	3.95354E-06	1.97E-04	0.000159913
2916	PSNR	58.72104	0.485491	39.34985	4.197206
	MSE	0.087817	0.009703	11.88142	12.97983
	D	4.47E-06	2.97832E-06	3.36E-04	0.000195
1936	PSNR	60.49476	0.550876	41.95772	4.22369
	MSE	0.05847	0.007308	6.81037	9.224583
	D	2.91E-06	2.00756E-06	1.97E-04	0.00016





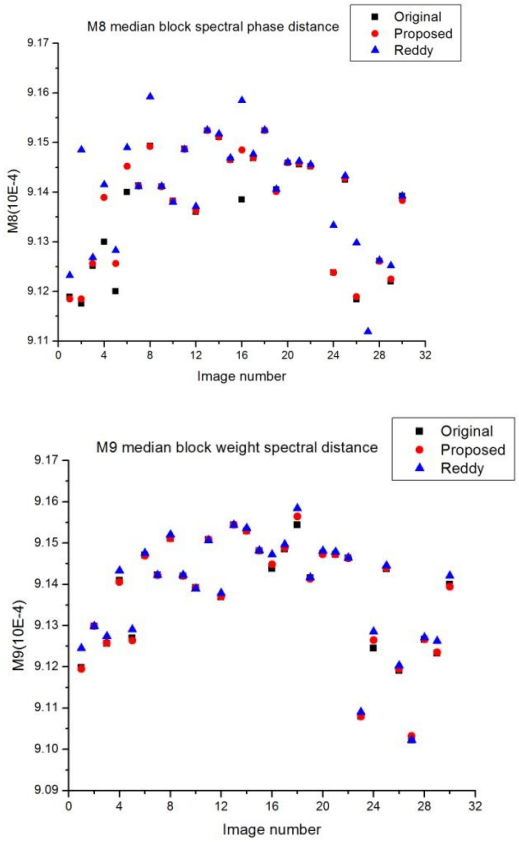


FIGURE 8 (A-D) VARIATION IN IQMS FOR PROPOSED AND REDDY METHODS

VI. CONCLUSION AND FUTURE WORK

As the objectives of steganography methods are satisfying the appropriate payload and transition of the confidential information in lossy channels in an undetectable manner. These objectives are conflicted with each other. A secure steganography method for embedding reasonable amount of secret messages into cover image without producing any major changes has been proposed. Arithmetic coding applied on secret message in order to obtain high secrecy, high payload and authentication. Embedding payload of the proposed method in most cases is higher than that of existing method. The PSNR value after embedding of the secret message in RCs of the cover image is also higher than values of existing method. Also proposed method is secured (undetectable) against statistical and visual attacks. As shown in Tables I and II, cover image is significantly influences the result obtained from the proposed system. Because applying a steganographic technique on two images is not guarantee the same results. Hitherto this resource has not been completely considered in the proposed embedding techniques. The next approach will try classify cover images in order to helps Sender satisfy steganographic objectives.

REFERENCES

[1] N.F Johnson, and S Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE Computer, vol. 31, no.2, pp. 26–34, 1998.

[2] S.H Seyedi, H Aghaeinia, and A Sayadian, " A new Roubst Image Adaptive Steganography Mothod in Wavelet Transform", IEEE electronic engineering (ICEE), pp.1-5, Tehran, Iran, 2011.

[3] 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.

[4] 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, pp.142-172, 2011.

[5] C.S Lu, "Multimedia Security: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property", Idea Group Publishing, 2005.

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

[7] R Chandramouli, and N.D Memon,"Steganography Capacity: a Steganalysis Perspective", SPIE Security Watermarking Multimedia Contents, vol.5020, pp.173–177, 2003.

[8] X Zhang, and Sh Wang, "Dynamical Running Coding in Digital Steganography", IEEE Signal Processing Letters, vol. 13, no.3, pp.165-168, 2006.

[9] A.A Abdelwahab, and L.A Hassaan, "A Discrete Wavelet Transform Based Technique for Image Data Hiding", National Radio Science Conference(IEEE), pp.1-9, Tanta, Egypt, 2008.

[10] 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 (COMSWARE), pp.614-621, Bangalore, India, 2008.

[11] 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.597-605, 2010.

[12] 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.

[13] R Roy, S Changder, A Sarkar, and N.C Debnath, "Evaluating Image Steganography Techniques: Future Research Challenges", Computing, Management and Telecommunications (ComManTel), pp.21-24, Ho Chi Minh, Vietnam, 2013.

[14] 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, pp.345-355, Portland, USA, 1998.

[15] C Cachin, "An Informationtheoretic Model for Steganography", Information and Computation, vol.192, no.1, pp.41-56, 2004.

[16] W Sweden, "The Lifting Scheme. A Construction of Second Generation Wavelets", SIAM J. Math. Anal., vol. 29, no.2, pp.511–546, 1997.

[17] 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), pp.6251-6253, Japan, 1997.

[18] S Amir, "Introduction to Arithmetic Coding Theory and Practice", Imaging Systems Laboratory HP Laboratories: Palo Alto HPL-2004-76, 2004.

[19] J Shapiro,"Embedded Image Coding Using Zero Tree of Wavelet Coefficients", IEEE Transaction on Signal Processing, vol. 41, no.12, pp.3445-3462, 1993.

[20] Image database of University Granada: http://decsai.ugr.es/cvg/dbimagenes/g512.php

[21] Image database of University Wisconsin-Madison http://homepages.cae.wisc.edu/~ece533/images/

[22] 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.

[23] 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.

[24] I Avcibas, B Sankur, and Kh Sayood, "Statistical Evaluation of Image Quality Measures", Journal of Electronic Imaging, vol.11, no.2, pp.206-223, 2002.

[25] S.N Mali, P.M Patil, and R.M Jaluekar, "Robust and secure image adaptive data hiding", Digital Signal Processing, vol.22, no.2, pp.314-323, 2012.