International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(1): 63-71
The Society of Digital Information and Wireless Communications, 2014 (ISSN: 2305-0012)

An Adaptive Steganographic Method in Frequency Domain Based on Statistical Metrics of Image

Seyyed Amin Seyyedi[1], 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

6, Brovki St, 220013, Minsk, Belarus

amseyyedi@gmail.com, ivanovnn@bsuir.by

ABSTRACT

Steganography is a branch of information hiding. A tradeoff between the hiding payload and quality of digital image steganographic schemes is major challenge of the steganographic methods. An adaptive steganographic method for embedding secret message into gray scale images is proposed. Before embedding the secret message, the cover image is transformed into frequency domain by integer wavelet. The middle frequency band of cover image is partitioned into 4×4 non overlapping blocks. The blocks by deviation and entropy metrics are classified into three categories: smooth, edge, and texture regions. Number of bits which can be embedded in a block is defined by block features. Moreover, RC4 encryption method is used to increase secrecy protection. Experimental results denote the feasibility of the proposed method. Statistical tests were conducted to collect related data to verify the security of method.

KEYWORDS

Steganography, Wavelet, Steganalysis, Image Quality Metrics.

1 INTRODUCTION

Nowadays the digital communication channels and Internet play important role in data transmission and sharing, hence there is a great need in providing security of information to prevent unauthorized access. This leads to new trends of confidential data transmission research. One of the methods increasing the privacy of data transmission is steganography. 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 insertion [1, 2]. The main difference between steganography and cryptography is in the suspicion factor. Combining cryptography with steganography ensures better private communication. The digital images, videos, audios and other digital files can be used as a carrier for information embedding. Steganographic methods can be classified into two broad categories namely spatial-domain techniques and frequency-domain techniques. In spatial domain techniques, the secret messages are embedded directly into cover image. The simplest spatial domain method is the LSB (Least Significant Bit) approach. In frequency domain methods, the cover image is converted into frequency ranges and then the secret message is embedded into one of them. A frequency domain method, especially wavelet methods is more secure than other ones [3].

Steganalysis is the art and science of challenging the security of steganographic methods. First problem in steganalysis is in detecting the existence of the secret message in carrier [4]. The ability of steganalysis method depends on the payload of hidden message. Hence, this fact imposes an upper bound limit for embedding data, such that if the size of hidden data is less than upper bound, one may assert that the carrier is safe and the known statistical analysis methods cannot detect it [4, 5]. Therefore, a tradeoff between the hiding payload of a cover image and the detectability and quality of a stego-image is the main problem in steganographic schemes. For this reason an adaptive steganographic method based on integer wavelet transform to make the best tradeoff between payload and other criteria is proposed. After preprocessing the cover image,

the middle frequency band is partitioned into 4×4 non overlapping blocks. Amount of payload is determined based on characteristics of each blocks. In order to achieve higher security and authentication RC4 encryption method 40-bit key applied on secret message in advance.

2 BACKGROUNDS

The section briefly explains some techniques utilized in this article.

2.1 Cover Image Adjustment

During the embedding process in frequency domain, some coefficients will befall underflow/overflow after embedding secret message into these coefficients (in gray scale image underflow means the pixel value is smaller than 0 and overflow means that the pixel exceeds maximum value 255). In this case, during inverse wavelet transform lower/higher values are to be clipped and the secret message bits eventually will be lost. To overcome the underflow/overflow difficulty, a preprocessing instructions on the cover image need to be applied before the embedding. Hence, the cover image pixels $C(i,j)$ are adjusted as follow: [6, 7]

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

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. One level 2D wavelet transform on an image, decomposes it into four bands, namely LL, HL, LH, and HH. The LL band represents the low pass coefficients and corresponds to soft approximation of image. Other three bands represent the high pass coefficient of the image that includes horizontal, vertical and diagonal features of the image respectively. The same decomposition can be repeated on the LL band. 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) [8].

The lifting scheme is a technique for both designing wavelet and performing the discrete wavelet transform. The lifting scheme decomposes wavelet transform into three phases, split, predicate and update respectively. Figure 1 represents the generic scheme. An advantage of lifting scheme is that it does not require temporary storage in calculation steps and the inverse transform has exactly the same complexity as the forward one. In this paper biorthogonal Cohen-Daubechies-Feauveau (CDF 2.2) lifting scheme is chosen as a case study. The integer forward transform formulas of CDF 2.2 are as follows [9, 10]:

$$\text{Splitting: } \begin{cases} S_i \leftarrow x_{2i} \\ d_i \leftarrow x_{2i+1} \end{cases}, \quad (2)$$

$$\text{Predicate: } d_i \leftarrow d_i - \left\lfloor \frac{1}{2}(s_i + s_{i+1}) + \frac{1}{2} \right\rfloor, \quad (3)$$

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

where x denotes the original signal, and inverse transform formulas are:

$$\text{Inverse update: } s_i \leftarrow s_i - \left\lfloor \frac{1}{4}(d_{i-1} + d_i) + \frac{1}{2} \right\rfloor, \quad (5)$$

$$\text{Inverse predicator: } d_i \leftarrow d_i + \left\lfloor \frac{1}{2}(s_i + s_{i+1}) + \frac{1}{2} \right\rfloor, \quad (6)$$

$$\text{Merging: } \begin{cases} x_{2i} \leftarrow s_i \\ x_{2i+1} \leftarrow d_i \end{cases} \quad (7)$$

2.3 Rounding Method

Rounding method is one of the ways for embedding secret message bits into cover image. The pixel value is modified into the nearest integer with the last LSB bits equal to the input bits. For example, assume that the data payload of the current pixel is found to be 3 bits. Then, the current pixel is equal to 102 or $(01100110)_2$ and the input bits are equal to $(100)_2$. According to the rule described above, the pixel value is altered to 100 or $(01100100)_2$. The mathematical representation of rounding method is [11]:

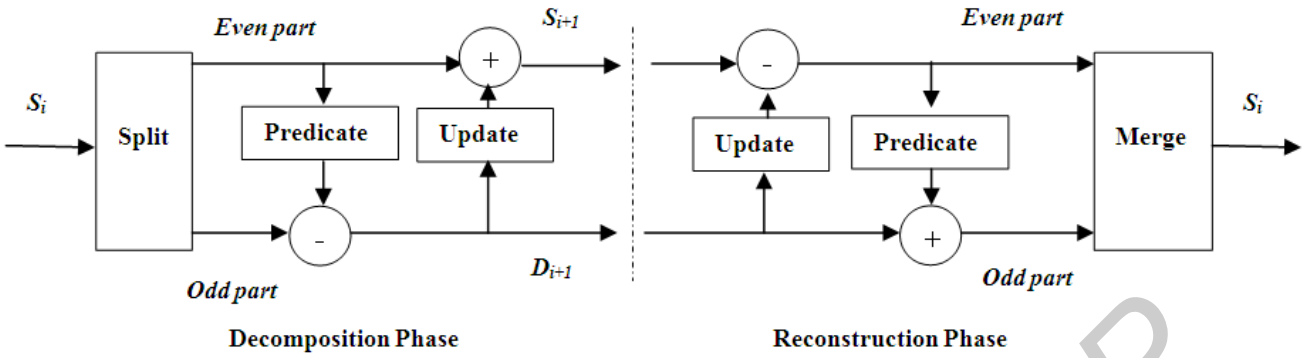


Figure 1 The lifting scheme

$$y = x + A \times (A \le B) - B \times (B < A), \quad (8)$$

$$A = \mathrm{mod}(m - x, 2^c), \quad (9)$$

$$B = \mathrm{mod}(x - m, 2^c) \quad (10)$$

For extracting data the receiver can use the following formula:

$$m = \mathrm{mod}(y, 2^c), \quad (11)$$

where y, x, m, and c denotes the output value, input value, secret message and payload respectively.

2.4 Pixel Mapping Method

Pixel Mapping Method (PMM) is a method for embedding two or four bits of secret message into the cover image. Data embedding is performed by mapping the secret message bits into each pixel based on some features of pixel. The state machine of pixel mapping method for embedding two bits is shows in figure 2. For example, assume that secret message bits are equal to $(11)_2$ Then, the current pixel is equal to 34 or $(00100010)_2$. According to the rule described in figure 2, the value of pixel is changed into 35 or $(00100011)_2$ [12].

2.5 Encryption

One of the approaches to satisfied security of steganographic system is cryptography. 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. 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. In this paper symmetric encryption method RC4 with 40-bit key is utilized to encrypt the secret message [6, 13].

3. THE PROPOSED METHOD

Payload in LSB method can be greatly improved by increasing the number of embedding bits. The more LSBs are used for embedding; more quality loss of stego-image is obtained, because pixels in an image cannot be undergone equal amounts of changes. The human eyes are very sensitive to changes of the gray value of pixels in smooth regions. A proper locations for hiding the secret message in digital images are regions with high contract, texture and high variations in its gray levels (edges), because this regions are very noisy and variations in these regions for hiding secret message is difficult to detect. An adaptive steganographic method based on Integer Lifting Wavelet Transform (IntLWT) is proposed in this article.

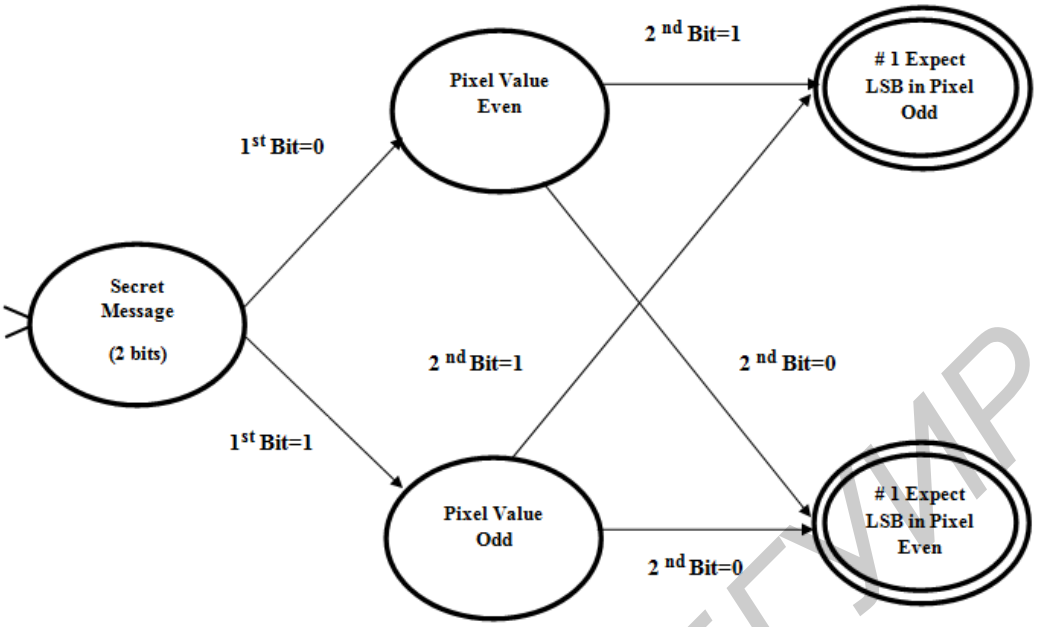


Figure 2 State machine for embedding two bits

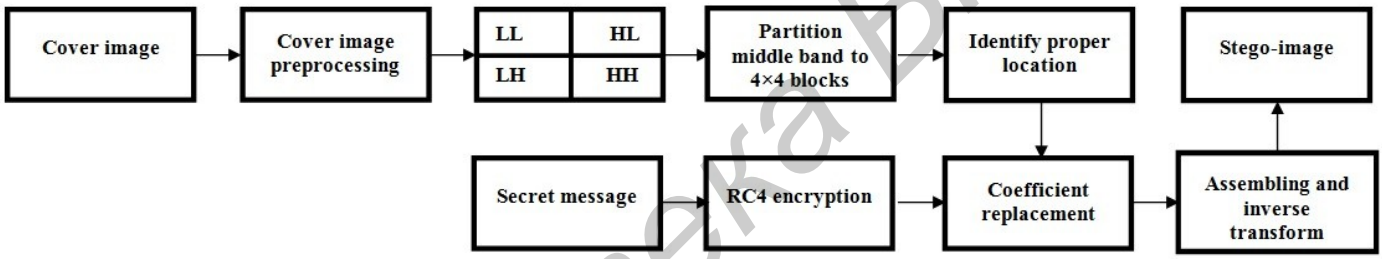


Figure 3 Block diagram of proposed method

After preprocessing the cover image, IntLWT is performed. The middle frequency band of cover image is partitioned into 4×4 non overleaping blocks. Each block is categorized to different regions according to statistical metrics. The secret message bits are embedded in blocks that contain edge and texture. The block diagram of proposed method is shown in figure 3.

3.1 Embedding Region

The cover images used in the proposed method are 256 gray-valued ones. After preprocessing of the cover image, the IntLWT is applied to it. The middle frequency band is partitioned into 4×4 non overlapping blocks. The Maximum Deviation (MD) and Entropy (En) are calculated for each block that respectively defined as:

$$\bar{X} = \frac{1}{16}\sum_{i=1}^{4}\sum_{j=1}^{4} w(i,j), \qquad (12)$$

$$MD(k) = Max\{|w(i,j) - \bar{X}|, \quad i,j = 1,2,3,4\}, \qquad (13)$$

where w is wavelet coefficients within block of dimension 4×4 and k is a block number.

$$En(k) = -\sum_{i=1}^{16} P_i \log_2 P_i \qquad (14)$$

where P is the probability of wavelet coefficients in each 4×4 blocks and k is the block number respectively.

MD and En are vectors that comprise maximum deviation and entropy of each block. The counter k corresponds to blocks and its length is equal to number of blocks. For example for 512×512 cover image, the number of 4×4 blocks in middle frequency (HL or LH) is 4096.

Each block of cover image is classified as smooth, edge and texture regions. The blocks in image for which $MD\ (k)$ is greater than threshold T_1 belong to non-smooth regions and others belong to smooth areas. The non-smooth regions for which

En (k) is greater than threshold T_2 is specified as edge, other belongs to texture. The thresholds T_1 and T_2 are defined as:

$$T_1 = \alpha \times mean(MD), \quad (15)$$

$$T_2 = mean(En), \quad (16)$$

where α $(0 < \alpha \leq 1)$ is a tradeoff factor that equilibrates payload and fidelity requirements.

3.2 Embedding Algorithm

The secret message embedding scheme to gain the reasonable tradeoff between hiding payload and quality of stego-image comprises of 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 the RC4 encryption method on SE.
Step3: Apply cover image adjustment by formula (1) to image C.
Step4: Perform one level IntLWT on the cover image.
Step5: Divide the middle frequency band into 4×4 blocks.
Step 6: Calculate *MD* and *En* values by formulas (13) and (14).
Step 7: Compute thresholds T_1, T_2 values by formulas (15) and (16).
Step 8: Apply coefficient replacement process for block *k* as:

IF *DM (k)* > T_1
  IF *En (k)*> T_2
    Embed 3 bits of secret message by rounding method into block *k*.
  Else
    Embed 2 bits of secret message by PMM into block *k*.
  End
End
IF all bits of secret message have been embedded
    Go to step 9
Else
    k=k+1, go to step 8
End.
Step 9: Assemble middle frequency band from blocks.
Step 10: Perform inverse wavelet transform to gain stego-image S.

4. EXPERIMENTAL RESULT

In this section, some experiments are carried out to assess the efficiency of the proposed method based on data payload and fidelity benchmarks [3]. The 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 were conducted on image database of BOSSBase (v0.92) [14].

Fundamentally, data payload of steganographic 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. The embedding rate is usually given in absolute measurement such as the size of the secret message or in bits per pixel, etc.

According to proposed method, the tradeoff factor α expresses the regulator related to the threshold value T_1 as shown in formula (15). So, the payload is linked directly to the tradeoff factors. Figure 4 shows the amount of payload for several values of α. If factor α goes to zero, the data payload increases.

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

The MSE between the cover image and the stego-image is defined as follows:

$$MSE = \frac{1}{(M \times N)^2} \sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) - S(i,j))^2. \quad (17)$$

The *PSNR* is computed using the following formula:

$$PSNR = 10 \log_{10} \frac{Max^2}{MSE} dB, \quad (18)$$

where *Max* denotes the maximum pixel value of the image. Higher *PSNR* value indicates the better quality of stego algorithm.

Cross-Correlation (*CC*) is a measure of similarity of two images computed as:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\mu_1)(S(i,j)-\mu_2)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(C(i,j)-\mu_1)^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}(S(i,j)-\mu_2)}}, \quad (19)$$

Values μ_1 and μ_2 are mean pixel values of the cover image and stego-image.

Table 1 presents the image similarity metrics versus different message sizes. According to the results shown in table 1, decreasing the α rate conflicts with similarity metrics, because in this case selected regions is not completely non-smooth. Figure 5 shows the cover images and stego-images Barbara and Airplane with their corresponding histogram after embedding 6500 byte with α =0.7

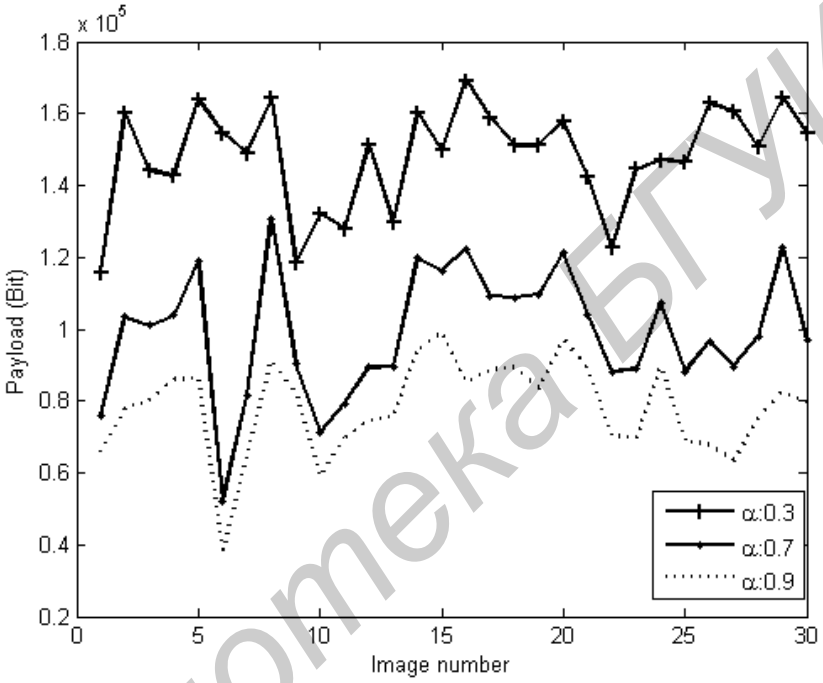


Figure 4 Amount of payload for several values of α

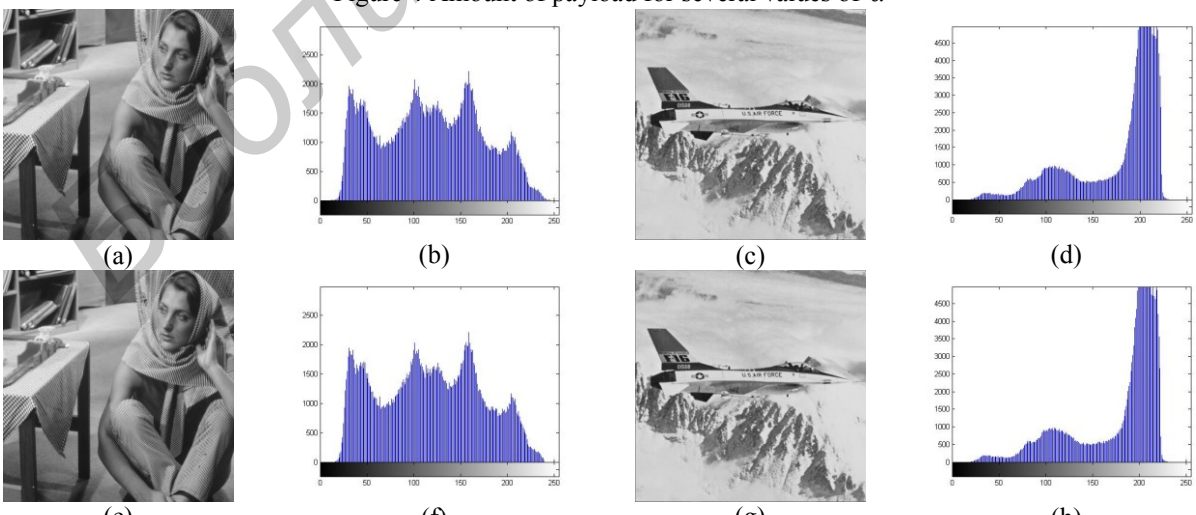


Figure 5 (a-d) Cover images Barbara and Airplane with their corresponding histogram, (e-h) stego-images and their corresponding histogram

Table 1 Calculation various similarity metrics for middle frequency HL band

Similarity Metrics	*α =0.3*				*α =0.7*			
	Length of embedding message (Byte)							
	5000		*10000*		*5000*		*6500*	
	Mean	*St. Dev.*	*Mean*	*St. Dev*	*Mean*	*St. Dev*	*Mean*	*St. Dev*
PSNR	42.49	2.091	39.43	1.566	43.37	3.775	42.43	3.347
MSE	4.159	2.558	7.979	3.755	4.294	4.264	5.018	4.599
CC	0.9996	0.0001	0.9994	0.0003	0.9997	0.0002	0.9996	0.0002

4.1 Steganalysis of proposed method through IQMs

Steganographic method is said to be undetectable or secure if the existence statistical tests cannot distinguish between the cover and the stego-image. During the embedding process in the cover image some statistical variations are arises. The stego-image is perceptually identical but statistically differs from the cover image. The attacker uses these statistical differences in order to detect the secret message. I. Avcibas et al. [15, 16] 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. I. Avcibas [17] 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 $\delta = 0.5$ and mask size 3×3 for selected IQMs [17, 18] as shown in figure 6.

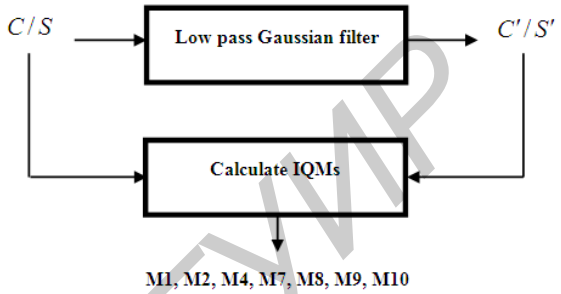
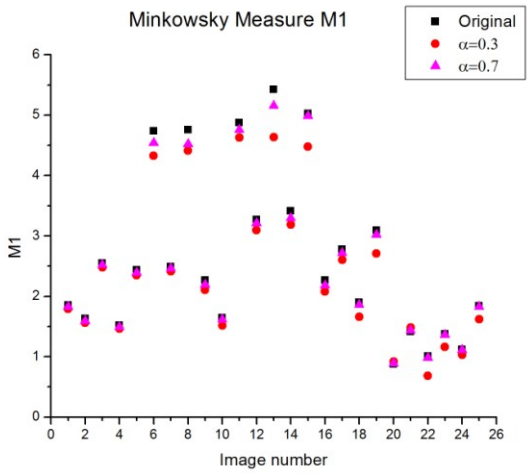
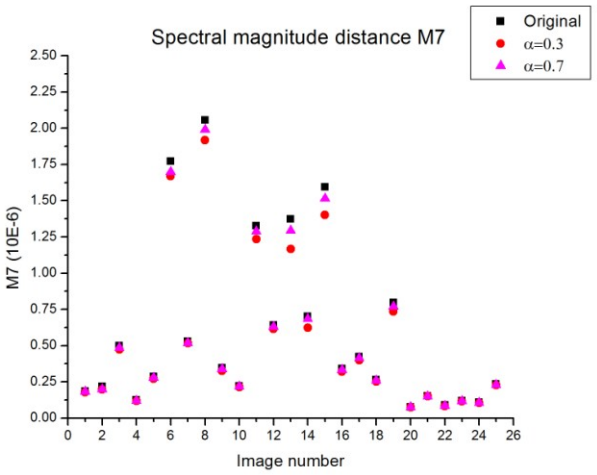


Figure 6 Calculation IQMs scores

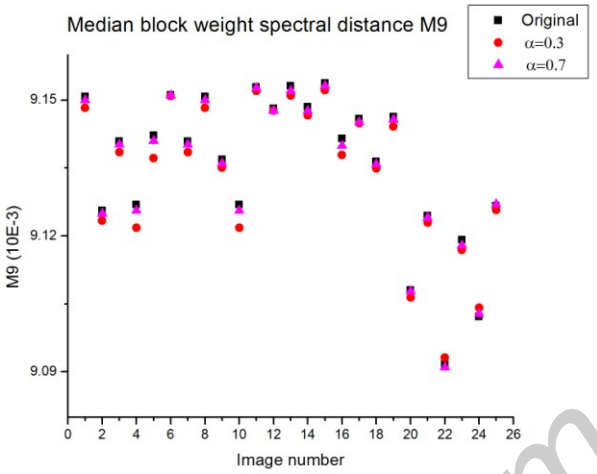
The variations in IQMs for proposed method with different rates of α (0.3, 0.7) with embedding the 9000 bytes in cover images were considered. From experimental results it can be perceived that difference IQMs between cover images and stego-images of proposed method with α=0.7 is less than for α=0.3. Therefore proposed method for α=0.7 is more secured than for α=0.3. For the α=0.7 the warden cannot distinguish stego-image from the cover image. The variations in IQMs for M1, M7 and M9 are shown in figure 7 (a-c).



(a)



(b)



(c)

Figure 7 Variations in IQMs

5- CONCLUSION AND FUTURE WORK

The main goal of image steganographic techniques is to maximize embedding payload while minimizing the distortion rate and detectability of stego-image. The proposed adaptive method utilizes the characteristic of human visions sensitivity to gray value variation. The secret message is embedded into HL middle frequency band of cover image by recognizing the edge and texture regions. Using integer wavelet transform and RC4 encryption technology can enhance the reliability, improve the resistibility. Also tradeoff factor α affects requirements of proposed method. This parameter equilibrates the amount of data payload and fidelity of the stego-image. The Sender can make the best tradeoff between requirements based on the appropriate selection of α. As shown in figure 4, the different cover images give different results in term of data payload and fidelity of stego-image. The new approach intends for selecting reasonable cover image for steganographic methods.

6 REFERENCES

1. Johnson, N.F., Jajodia, S.: Exploring Steganography Seeing the Unseen, IEEE Computer, vol.31, no.2, pp.26--34 (1998).
2. Lu, S.: Steganography and Digital Watermarking Techniques for Protection of Intellectual Property, Idea group publishing (2005).
3. Cheddad, A., Condell, J., Curran, K., Kevitt, P. M.: Digital Image Steganography: Survey and Analysis of Current Methods, Digital Signal Processing, vol.90, no.3, pp.727--752 (2010).
4. Nissar, A., Mir, A.H.: Classification of Steganalysis Techniques, Digital Signal Processing, vol.90, no.6, pp.1758--1770 (2010).
5. Chandramouli, R., and Memon, N.D.: Steganography Capacity: a Steganalysis Perspective, SPIE Security Watermarking Multimedia Contents, vol.5020, pp.173--177 (2003).
6. Al-Ataby, A., and Al-Naima, F.: A Modified High Capacity Image Steganography Technique Based on Wavelet Transforms, International Arab Journal of Information Technology, vol.7, no.4, pp.358--364 (2010).
7. Raja, K.B., Sindhu, S., Mahalakshmi, T.D., Akshatha, S., Nithin, B.K., Sarvajith, M., Venugopal, K.R., and Patnaik, L.M.: Robust Image Adaptive Steganography Using Integer Wavelets. In: proc 2008, Communication Systems Software and Middleware and Workshops (COMSWARE), pp.614--621. India (2008).
8. Walker, S.: A Premier of Wavelets and Their Scientific Applications, CRC Press (1999).
9. Sweden, W.: The Lifting Scheme, A Construction of Second Generation Wavelets, SIAM J. Math Anal, vol. 29, no.2, pp.511--546 (1997).
10. Uytterhoeven, G., and Roose, D., Bultheel, A.: Wavelet Transforms Using the Lifting Scheme. In: proc 1997 (ITC-CSCC'99) International Technical Conference on Circuits/Systems computers and communications, pp.6251--6253. Japan (1997).
11. Sarreshtedari, S., Ghobi, M., and Ghaemmeghami, S.: High Capacity Image Steganography in Wavelet Domain. In: proc. (2010) the 7th annual IEEE consumer communications and networking conference, pp.1--5. USA (2010).
12. Bhattacharyya, S., and Sanyal, G.: 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).
13. Smart, N.: Cryptography: An Introduction, McGraw-Hill College (2004).

14. Image database of BOSSBase V (0.92), http://exile.felk.cvut.cz/boss/BOSSFinal/index.php
15. Avcibas, I., Memon, N., and Sankur, B.: Steganalysis Using Image Quality Metrics, IEEE Transaction on Image Processing, vol.12, no.3,pp.221--229 (2003).
16. Avcibas, I., Memon, N., Kharrazi, M., and Sankur, B.: Image Steganalysis with Binary Similarity Measures, EURASIP Journal on Advances in Signal Processing, vol.2005, no.1, pp.2749--2757 (2005).
17. Avcibas, I., Sankur, D., and Sayood, Kh.: Statistical Evaluation of Image Quality Measures, Journal of Electronic Imaging, vol.11, no.2, pp.206--223 (2002).
18. Mali, S.N., Patil, P.M., and Jaluekar, R.M.: Robust and Secure Image Adaptive Data Hiding, Digital Signal Processing, vol.22, no.2, pp.314--323 (2012).