International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

ANALYSIS OF NON-ADAPTIVE AND ADAPTIVE EDGE BASED LSB STEGANOGRAPHY FOR COLORED IMAGES

Rohini Sharma
Deptt. of I.T,
M.M.Engg. College,
M.M.University,
Mullana (Ambala).

Ekta Walia
Deptt. of I.T,
M.M.Engg. College,
M.M.University,
Mullana (Ambala).

Deepak Sharma
Deptt. of EIE,
M.M.Engg. College,
M.M.University,
Mullana (Ambala).

Abstract

Non-adaptive and adaptive algorithms are used for edge based LSB steganography and various papers present the results of there algorithms on gray-scale images only. This paper presents the results of analyzing the performance of non-adaptive and adaptive edge-based LSB steganography for colored images. Both these algorithms have been slightly modified for colored image implementation and are compared on the basis of various evaluation parameters like peak signal noise ratio (PSNR) and mean square error (MSE). Besides this, an algorithm has been designed and implemented to recover the original image from the stego-image.

Keywords: Adaptive least-significant-bit (LSB) substitution, pixel-value differencing (PVD), steganography, data embedding, data extraction.

1. Introduction

Digital data communication is an essential part of everyone's life. Data communications have some problems such as internet security, copyright protection [1] [2] etc. To avoid these problems, cryptography is one of the methods. However, encryption results in a disordered and confusing message and can attract eavesdroppers easily. Steganography methods [3]-[8] overcome this problem by hiding the secret information behind a cover media (video, audio or image) because the presence of information can not be noticed by any attacker. The least significant bit (LSB) substitution is a well known steganography method [9]-[11]. In this method, the secret data is embedded in the cover image by utilising LSB's of a pixel [12]. Wang et al. proposed a method of LSB substitution to improve the security and quality of the stego-image [13]. Various new LSB approaches have been proposed and some of these approaches use concept of human vision to increase the quality of stego-image. A "pixel value differencing" steganography method is proposed by Wu and Tsai in 2003, that uses the difference value of two consecutive pixels to find how many secret bits should be embedded [14]. In 2005, Wu et al. proposed the pixel value differencing (PVD) and LSB replacement method [15]. In this method, the two pixel values are embedded by LSB replacement method and PVD methods, if their difference value falls into lower level and higher level respectively. If the difference value of the two pixel changes from lower level to higher level then readjustment of the two pixel values is required. Due to readjustment, the difference value comes back to lower level. In 2008, Yang et al. proposed an adaptive LSB steganographic method using pixel value differencing (PVD) for hiding data in gray images [16]. Their method exploits the difference value of two consecutive pixels to estimate how many secret bits will be embedded into two pixels. The pixel located in the edge areas are embedded by k-bit LSB substitution method with a larger value of k than the pixels located in smooth areas. The range of difference values is adaptively divided into lower, middle and higher level. The value of k is adaptive and decided by the level which the difference value belongs to. In order to increase the quality of stego-images, a readjustment of the pixels values is done when embedding results cause the difference values to fall into another range. In our paper, the analysis of non-adaptive and adaptive steganography methods is done by comparing these methods on the basis of mean square error (MSE) and peak signal to noise ratio (PSNR). The comparison of these methods has been done for gray-scale as well as color images. Besides this, the original image is recovered from the stego-image after the extraction of secret data.

2. Non-Adaptive Edge Based LSB Steganography Method

In this algorithm, cover image is partitioned into non-overlapping blocks of two consecutive pixels, states p_i and p_{i+1}. From each block we can obtain a different value d_i by subtracting p_i from p_{i+1}. All possible different values of d_i ranges from -255 to 255, then $|d_i|$ ranges from 0 to 255. Therefore, the pixel p_i and p_{i+1} is located within the smooth area when the value $|d_i|$ is smaller and will hide less secret data. Otherwise, it is located on the edged area and embeds more data. In smooth areas, the data is hidden into cover image using LSB method, whereas the Pixel Value Differencing (PVD) method is used in the edge areas. The division between the 'lower-level i.e. smooth areas' and 'higher-level i.e. edge areas' of the range table is controlled by the users. Anyone who has extracted the secret data from a stego-image must use the original division. A division is the key of the extracted secret data. In the lower–level of range table, each block of two continuous pixels will hide 6-bit secret data (i.e. each pixel hides 3-bit secret data), otherwise (such as the higher-level of the range table), the bit-number of hidden data depends on w_i. The data embedding algorithm is given as:

Data Embedding Procedure

First, one must assume a division *Div* of the 'lower-level' and 'higher-level'. For example, let *Div*=15, so one can set the 'lower-level' to be R_1 and R_2, 'higher-level' to be $R_{3,} R_4, R_5$ and R_6. The detailed secret data hiding steps are as follows:

Step 1) Calculate the difference value d_i for each block of two consecutive pixels p_i, p_{i+1} (for each intensity of RGB image), which is given in Eq. (1)

$$d_i = |p_i - p_{i+1}| \tag{1}$$

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

Step 2) Find the optimal R_i of the d_i such that $R_i = \min(u_i - k)$, where $u_i \geq k$ and $k = |d_i|, R_i \in [l_i, u_i]$ is the optimum R_i for all $1 \leq i \leq n$ [15].

Step 3) If R_i belongs to the lower-level, read six bits from secret data stream, and transf-orm the intensity value p_i, p_{i+1} into a binary value. Next, we hide 6-bit secret data into cover image by modifying p_i and p_{i+1} according to the following procedure. Make the 6-bit secret data S = $m_1, m_2 m_3 m_4, m_5, m_6$ [15].

(1) Convert p_i to be $p_i^{'}$ by substituting 3-LSB of p_i by $m_1, m_2 m_3$ (for each intensity of RGB image).

(2) Convert p_{i+1} to be $p_{i+1}^{'}$ by substituting 3-LSB of p_{i+1} by $m_4 m_5, m_6$ (for each intensity of RGB image).

(3) Calculate the new difference value $d_i^{'}$ as in Eq.(2):

$$d_i^{'} = \left| p_i^{'} - p_{i+1}^{'} \right| \tag{2}$$

(4) If $d_i^{'} >$ Div (i.e. $d_i^{'} \in$ higher-lower), then readjust $p_i^{'}$ and $p_{i+1}^{'}$ considering the Eq.(3):

$$\left(p_i^{'}, p_{i+1}^{'}\right) = \begin{cases} \left(p_i^{'} - 8, p_{i+1}^{'} + 8\right), & if \ \ p_i^{'} \geq p_{i+1}^{'} \\ \left(p_i^{'} + 8, p_{i+1}^{'} - 8\right), & if \ \ p_i^{'} < p_{i+1}^{'} \end{cases} \tag{3}$$

Step 4) If R_i belongs to higher-level [15]:

(1) Compute how many bits t of the secret data, which are hidden in each block of two consecutive pixels, depend on each w_i of the R_i is defined as $t = \lfloor \log_2 w_i \rfloor$, where w_i is the width of the R_i.

(2) Read t bits binary secret data one by one according to step (1), and then transform t into decimal value b.

(3) Calculate the new difference value $d^{'}$ which is given by $d_i^{'} = l_i + b$.

(4) Modify the p_i and p_{i+1} by the following formula using in Eq.(4):

$$\left(p_i^{'}, p_{i+1}^{'}\right) = \begin{cases} \left(p_i + \left\lceil \frac{m}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), & if \quad p_i \geq p_{i+1} \ \& \ d_i^{'} > d_i \\ \left(p_i - \left\lfloor \frac{m}{2} \right\rfloor, p_{i+1} + \left\lceil \frac{m}{2} \right\rceil\right), & if \quad p_i < p_{i+1} \ \& \ d_i^{'} > d_i \\ \left(p_i - \left\lceil \frac{m}{2} \right\rceil, p_{i+1} + \left\lfloor \frac{m}{2} \right\rfloor\right), & if \quad p_i \geq p_{i+1} \ \& \ d_i^{'} \leq d_i \\ \left(p_i + \left\lceil \frac{m}{2} \right\rceil, p_{i+1} - \left\lfloor \frac{m}{2} \right\rfloor\right), & if \quad p_i < p_{i+1} \ \& \ d_i^{'} \leq d_i \end{cases} \quad (4)$$

Where $m = \left|d_i^{'} - d_i\right|$.

After following the above steps the stego image is constructed.

Data Extraction Procedure

The following steps are executed to extract the original data.

Step 1) Partition the stego-image into blocks of consecutive pixels and the partition proc--edure is identical with embedding [15].

Step 2) Calculate the difference value $d_i^{'}$ for each block of two consecutive pixels $\left(p_i^{'}, p_{i+1}^{'}\right)$ of the stego-image (for each intensity of RGB image), which is given in Eq. (5)

$$d_i^{'} = \left|p_i^{'} - p_{i+1}^{'}\right| \quad (5)$$

Step 3) Find the optimal R_i of the $d_i^{'}$ according to the original range table and judge the level of optimal R_i denoted by the original set *Div* value [15].

Step 4) Extract the k -LSB of the $p_i^{'}$ and $p_{i+1}^{'}$ of the stego-image directly, because the k -LSB of the $p_i^{'}$ and $p_{i+1}^{'}$ is represented by the hidden secret data [15].

After following the above steps the secret data is extracted from stego image.

3. Adaptive Edge Based LSB Steganography Method

The embedding strategy of the adaptive LSB substitution approach is based on the concept that edge areas can tolerate a larger number of changes than smooth areas [16]. Similar to non-adaptive scheme, pixel-value differencing is used to distinguish between edge areas and smooth areas. The range [0, 255] of difference values is divided into different levels, for instance, lower level, middle level, and higher level. For any two consecutive pixels, both pixels are embedded by the k -bit LSB substitution, but the value k is decided by the level which their difference value belongs to. A higher level will use a larger value of k. In order to improve the quality of the stego-images, the well-known LSB substitution method, called the modified LSB substitution method is applied. The concept of the modified LSB substitution is to increase or decrease the most-significant-bit (MSB) part by 1 for reducing the square error between the original pixel and the embedded pixel. In order to extract data exactly, the difference values before and after embedding must belong to the same level. If the difference value changes into another level after embedding, a readjusting phase is used to readjust the pixel values. The embedding and extracting procedures of adaptive approach are described as follows:

Data Embedding Procedure

The difference value d is computed for every non-overlapping block with two consecutive pixels [16]. The way of partitioning the cover image into two-pixel blocks runs through all of the rows in a raster scan. Prior to the embedding procedure, the range [0, 255] must be divided into different levels. The first case has one dividing line $D_{12} = 15$, which divides the range [0, 255] into ranges $R_1 = [0,15], R_2 = [16,255]$ where the lower level contains R_1 and the higher level contains R_2 . The second case has two dividing lines $D_{12} = 15$; and $D_{23} = 31$, which divide range [0, 255] into ranges $R_1 = [0,15], R_2 = [16,31]$ and $R_3 = [32,255]$, where R_1, R_2 and R_3 belongs to the lower level, middle level, and higher lever, respectively. The width of range R is denoted as $|R|$. For example, $|R_1| = 16$, $|R_2| = 16$ and $|R_3| = 224$. The $l - m - h$ division means that

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

two-pixel blocks with difference values falling into the lower level, middle level, and higher level, will be embedded by the l-bit, m-bit and h-bit LSB substitution approaches, respectively. In addition, to succeed in the readjusting phase, we apply the restrictions $l \le \log_2|R_1|$ and $h \le \log_2|R_2|$ to the $l-h$ division, and restrictions $l \le \log_2|R_1|$, $m \le \log_2|R_2|$ and $h \le \log_2|R_3|$ to the $l-m-h$ division. The algorithm for the data embedding in adaptive edge based LSB steganography method is explained as below:

Step 1) Calculate the difference value d_i for each block with two consecutive pixels (for each intensity of RGB image), say p_i and p_{i+1}, using $d_i = |p_i - p_{i+1}|$.

Step 2) From the $l-m-h$ division, find out the level to which d_i belongs to. Let $k = l, m$, and h, if d_i belongs to the lower level, middle level, and higher level, respectively [16].

Step 3) By the k-bit LSB substitution method, embed k secret bits into p_i and k secret bits into p_{i+1}, respectively (for each intensity of RGB image) . Let $p_i^{'}$ and $p_{i+1}^{'}$ be the embedded results of p_i and p_{i+1} , respectively [16].

Step 4) Apply the modified LSB substitution method to $p_i^{'}$ and $p_{i+1}^{'}$ [16].

Step 5) Calculate the new difference value $d_i^{'}$ by $d_i^{'} = |p_i^{'} - p_{i+1}^{'}|$ [16].

Step 6) If d_i and $d_i^{'}$ belong to different levels, execute the readjusting phases as follows:

case 6.1 $d_i \in$ lower-level, $d_i^{'} \notin$ lower level. If $p_i^{'} \ge p_{i+1}^{'}$, readjust $(p_i^{'}, p_{i+1}^{'})$ to being the better choice between $(p_i^{'}, p_{i+1}^{'} + 2^k)$ and $(p_i^{'} - 2^k, p_{i+1}^{'})$; otherwise, readjust $(p_i^{'}, p_{i+1}^{'})$ to be the better choice between $(p_i^{'}, p_{i+1}^{'} - 2^k)$ and $(p_i^{'} + 2^k, p_{i+1}^{'})$.

case 6.2 $d_i \in$ middle level, $d_i^{'} \in$ lower level. If $p_i^{'} \ge p_{i+1}^{'}$, readjust $(p_i^{'}, p_{i+1}^{'})$ to be the better choice between $\left(p_i^{'}+2^k, p_{i+1}^{'}\right)$ and $\left(p_i^{'}, p_{i+1}^{'}-2^k\right)$; otherwise, readjust $\left(p_i^{'}, p_{i+1}^{'}\right)$ to be the better choice between $\left(p_i^{'}, p_{i+1}^{'}+2^k\right)$ and $\left(p_i^{'}-2^k, p_{i+1}^{'}\right)$.

case 6.3 $d_i \in$ middle level, $d_i^{'} \in$ higher level. If $p_i^{'} \geq p_{i+1}^{'}$, readjust $\left(p_i^{'}, p_{i+1}^{'}\right)$ to be the better choice between $\left(p_i^{'}, p_{i+1}^{'}+2^k\right)$ and $\left(p_i^{'}-2^k, p_{i+1}^{'}\right)$; otherwise, readjust $\left(p_i^{'}, p_{i+1}^{'}\right)$ to be the better choice between $\left(p_i^{'}, p_{i+1}^{'}-2^k\right)$ and $\left(p_i^{'}+2^k, p_{i+1}^{'}\right)$.

case 6.4 $d_i \in$ higher level, $d_i^{'} \notin$ higher level. If $p_i^{'} \geq p_{i+1}^{'}$, readjust $\left(p_i^{'}, p_{i+1}^{'}\right)$ to be the better choice between $\left(p_i^{'}, p_{i+1}^{'}-2^k\right)$ and $\left(p_i^{'}+2^k, p_{i+1}^{'}\right)$; otherwise, readjust $\left(p_i^{'}, p_{i+1}^{'}\right)$ to be the better choice between $\left(p_i^{'}, p_{i+1}^{'}+2^k\right)$ and $\left(p_i^{'}-2^k, p_{i+1}^{'}\right)$.

In Step 6), the better choice, say $\left(x_i, x_{i+1}\right)$, means that it satisfies the conditions that $\left|x_i - x_{i+1}\right|$ and d_i belong to the same level and $x_{i,} x_{i+1} \in [0,255]$, also the value of $\left(x_i - p_i\right)^2 + \left(x_{i+1} - p_{i+1}\right)^2$ is smaller.

After following the above steps the stego image is constructed.

Data Extraction Procedure

The stego-image is partitioned into non-overlapping blocks with two consecutive pixels, and the process of extracting the embedded message is the same as the embedding process with the same traversing order of blocks. Also, the same $l-m-h$ division, which is used in the embedding procedure, is used here. For each block, the detailed steps of data extracting are as follows:

Step 1) Calculate the difference value $d_i^{'}$ for each block with two consecutive pixels (for each intensity of RGB image), say $p_i^{'}$ and $p_{i+1}^{'}$, using $d_i^{'} = \left|p_i^{'} - p_{i+1}^{'}\right|$.

Step 2) From the $l-m-h$ division, find out the level to which $d_i^{'}$ belongs to Let $k=l,m$, and h if belongs to the lower level, middle level, and higher level, respectively.

Step 3) From the k-bit LSB of a pixel, extract k secret bits from $p_i^{'}$ and k secret bits from $p_{i+1}^{'}$ [16].

After following the above steps the secret data is extracted from stego image.

4. Procedure for Recovery of Original Image from Stego-image

The original image can be recovered from the stego-image by using recovery procedure. In this paper, we propose the technique to recover original image and hidden message from stego-image. This procedure is used for colored images. Before the embedding of the k-bits of the secret data, original k-bits of the pixel values are stored at different location. The following steps are used to obtain the original image from stego-image:

Step 1) Calculate the difference value d_i for each block with two consecutive pixels, say p_i and p_{i+1} (for each intensity of RGB image), using $d_i = |p_i - p_{i+1}|$.

Step 2) From the $l-m-h$ division, find out the level to which d_i belongs to. Let $k=l,m$, and h, if d_i belongs to the lower level, middle level, and higher level, respectively.

Step 3) By the k-bit LSB substitution method, embed k original bits into $p_i^{'}$ and k original bits into $p_{i+1}^{'}$, respectively. Let p_i and p_{i+1} be the embedded results of $p_i^{'}$ and $p_{i+1}^{'}$, respectively .

When all $p_i^{'}$ and $p_{i+1}^{'}$ pixel values are replaced by p_i and p_{i+1}, the original image is recovered from stego-image.

After following the above steps the cover image is reconstructed from the stego image.

5. Experimental Results

This work is implemented by using MATLAB 7.0. The objective of the work is to compare the performance of non-adaptive and adaptive methods of steganography. The

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

methods have been implemented on set of 7 gray scale images and 7 colored images given in Fig.1 and Fig.2 respectively. The performance of the methods have been evaluated and compared on the basis of two measures and the measures are: Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) and the equations of these two are:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m-1} \sum_{j=1}^{n-1} \left(I_{ij} - \hat{I}_{ij} \right)^2 \tag{6}$$

$$PSNR = 10 \log_{10} \left[\frac{(255)^2}{MSE} \right] \tag{7}$$

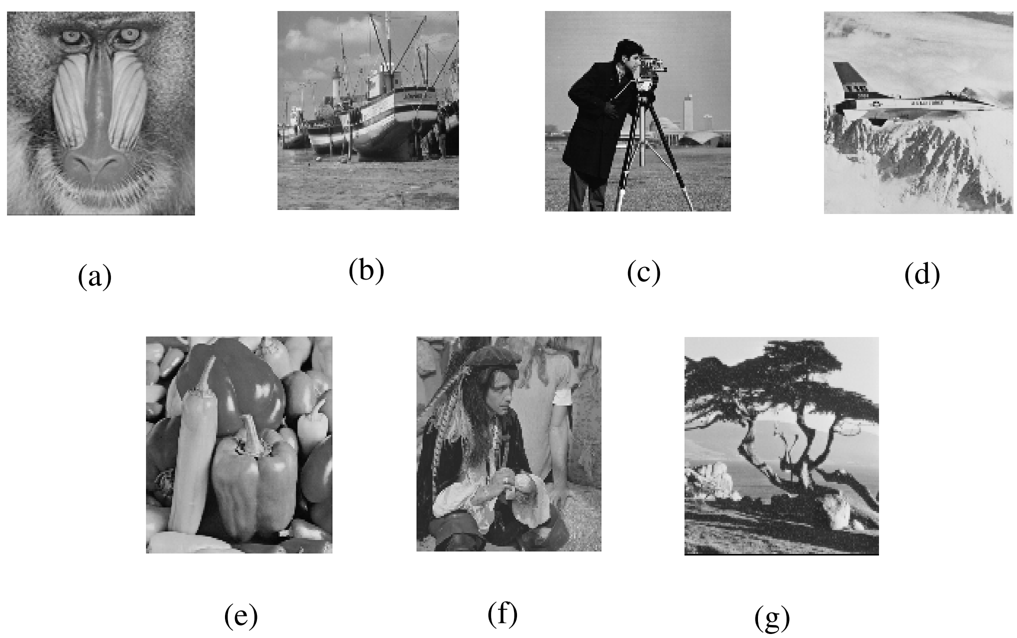

Fig.1 Gray-scale images. (a) Baboon (b) Boat (c) Cameraman (d) Jetplane (e) Peppers (f) Pirate (g) Tree

International Journal of Computing and Business Research (IJCBR)

ISSN (Online) : 2229-6166

Volume 2 Issue 1 2011

(a) (b) (c) (d)

(e) (f) (g)

Fig.2 Colored images. (a) Baboon (b) Boat (c) Goldhill (d) House (e) Lenna (f) Masuda (g) Peppers

These measures are calculated for gray-scale as well as colored images. The following equations are used to compute them: The table 1 shows the Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) of gray-scale images for both methods given as:

Table 1 MSE and PSNR for Non-Adaptive & Adaptive method for gray-scale images

S.No	Images (512 X 512 pixels)	Non-Adaptive (Gray-Scale)		Adaptive (Gray-Scale)	
		MSE	PSNR	MSE	PSNR
1	Baboon	4.75	41.39	4.72	41.42

2	Boat	4.77	41.37	4.73	41.41
3	Cameraman	4.72	41.42	4.70	41.44
4	Jetpalne	4.66	41.48	4.63	41.50
5	Peppers	4.67	41.47	4.66	41.48
6	Pirate	4.81	41.34	4.81	41.34
7	Tree	4.91	41.25	4.89	41.26
Average		4.76	41.38	4.73	41.41

The MSE and PSNR are calculated for more than one image that's why the average value of MSE and PSNR is also shown in the table 1. Table 2 shows the MSE and PSNR of colored images for both methods. The table of the MSE and PSNR for colored images is given as:

Table 2 MSE and PSNR for Non-Adaptive & Adaptive method for colored images

S.No	**Images (512 X 512 pixels)**	**Non-Adaptive (Colored)**		**Adaptive (Colored)**	
		MSE	**PSNR**	**MSE**	**PSNR**
1	Baboon	4.78	41.33	4.79	41.32
2	Boat	5.84	40.46	8.27	38.95
3	Goldhill	5.77	40.52	9.06	38.56
4	House	4.66	41.45	4.67	41.44
5	Lenna	4.71	41.39	4.75	41.36
6	Masuda	4.33	41.76	4.34	41.75
7	Peppers	4.61	41.49	4.64	41.46
Average		4.95	41.20	5.79	40.69

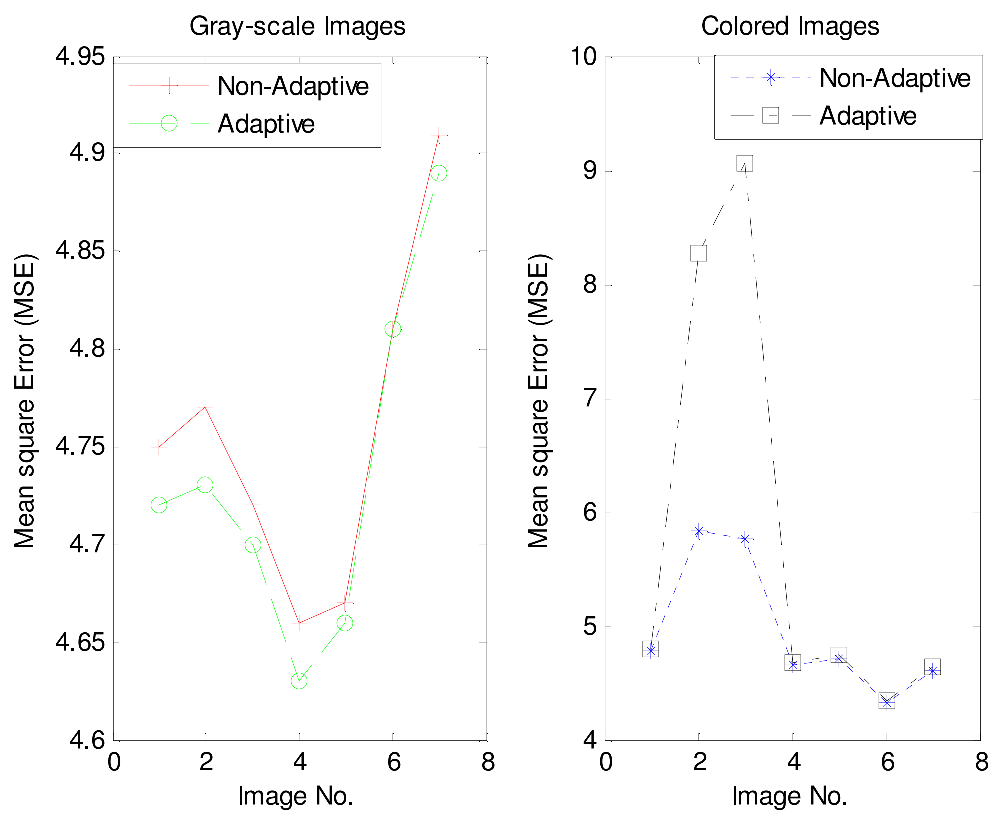

Fig. 3(a) Fig. 3(b)

Fig. 3(a) Comparison of MSE of non-adaptive and adaptive method (gray-scale),

Fig. 3(b) Comparison of MSE of non-adaptive and adaptive method (colored)

The comparisons of non-adaptive and adaptive steganography methods on the basis of MSE for gray-scale as well as colored images are shown in Fig.3 (a) and (b) and for PSNR comparisons are shown in Fig. 4 (a) and (b) respectively. The MSE in case of gray-scale image is more and the PSNR is less for non-adaptive steganography method than adaptive steganography method. The less MSE and more PSNR is the desirable condition for better performance. The adaptive steganography method satisfies this so, adaptive method is better choice for gray-scale images. For colored images the MSE is less and PSNR is more in non-adaptive steganography method than in adaptive steganography method. As compared to adaptive method, the performance of non-adaptive method is better for colored images.

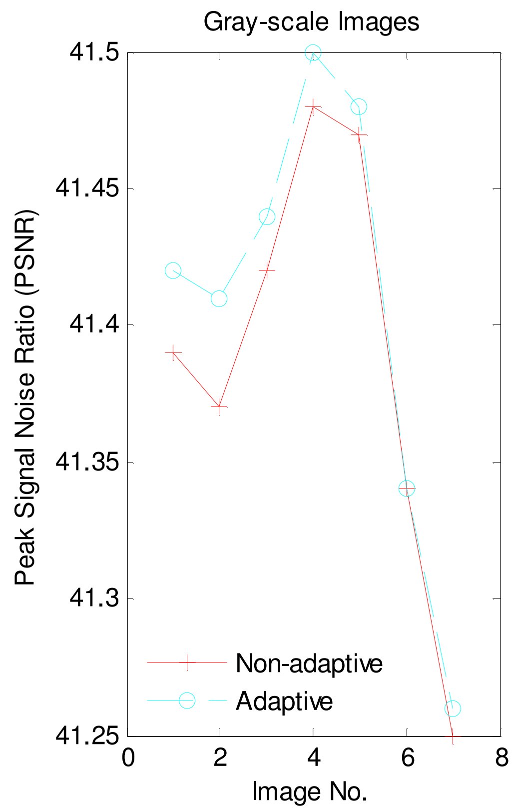

Fig. 4(a)

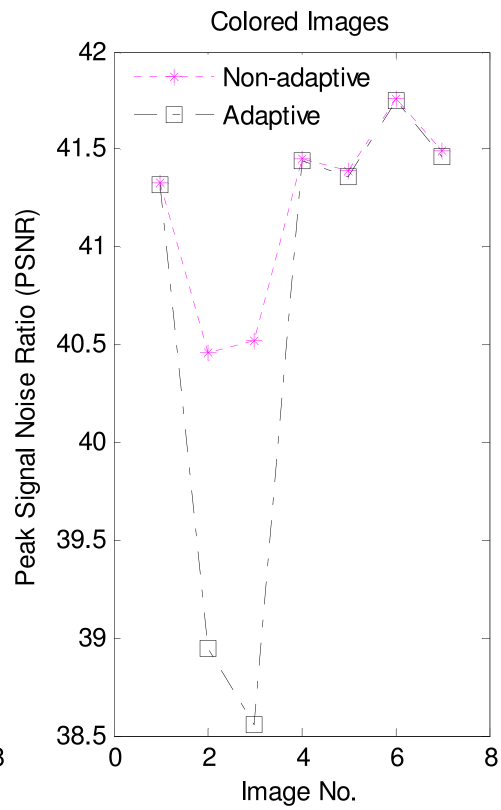

Fig. 4(b)

Fig. 4(a) Comparison of PSNR of non-adaptive and adaptive method (gray-scale),

Fig. 4(b) Comparison of PSNR of non-adaptive and adaptive method (colored)

5. Conclusions

In this paper, performance of adaptive and non-adaptive methods is analyzed for edge based LSB steganography. The image quality after data embedding is very important for better performance of steganography methods. The image quality is evaluated by Mean Square Error (MSE) and Peak Signal to Noise ratio (PSNR) for non-adaptive and adaptive methods for gray-scale as well as colored images. The following conclusions can be made from this analysis:-

1) For gray-scale images, a trend is observed that PSNR is higher and MSE is less in case of adaptive method, therefore adaptive method is better for gray-scale images.

2) For colored images, a trend is observed that PSNR is higher and MSE is less in case of non-adaptive method, therefore non-adaptive is better for colored images.

3) 100% recovery of original image is observed after extraction of secret data.

6. References

[1] D. Zou, C. W.Wu, G. Xuan, and Y. Q. Shi, "A Content-Based Authentication System with Lossless Data Hiding," in Proc. Multimedia Expo Int. Conf., vol. 2, pp. 6–9, 2003.

[2] T. Liu and Z. D. Qiu, "The Survey of Digital Watermarking-Based Image Authentication Techniques," in Signal Process., vol. 2, pp. 1556–1559, 2002.

[3] D. Artz, "Digital Steganographic: Hiding Data within Data," IEEE Internet Comput., vol. 5, no. 3, pp. 75–80, May/Jun. 2001.

[4] H. J. Highland, "Data Encryption: A Non-Mathematical Approach," Comput. Security, vol. 16, pp. 369–386, 1997.

[5] Y. H. Chu and S. Chang, "Dynamical Cryptography Based on Synchronized Chaotic Systems," Inst. Elect. Eng. Electron. Lett., vol. 35, no. 12, pp. 974–975, 1999.

[6] D. W. Bender, N. M. Gruhl, and A. Lu, "Techniques for Data Hiding," IBM Syst. J., vol. 35, pp. 313–316, 1996.

[7] R. R. Anderson and F. A. P. Peticolas, "On The Limits of Steganography," IEEE J. Sel. Areas Commun., vol. 16, no. 4, pp. 474–481, May 1998.

[8] Y. K. Lee and L. H. Chen, "High Capacity Image Steganography Model," Proc. Inst. Elect. Eng. Vis. Image, Signal Processing, vol. 147, no. 3, pp. 288–294, 2000.

[9] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image Hiding by Optimal LSB Substitution and Genetic Algorithm," Pattern Recognit., vol. 34, no. 3, pp. 671–683, 2000.

[10] C. C. Thien and J. C. Lin, "A Simple and High-Hiding Capacity Method for Hiding Digit-By-Digit Data in Images Based on Modulus Function," Pattern Recognit., vol. 36, no. 3, pp. 2875–2881, 2003.

[11] C. K. Chan and L. M. Chen, "Hiding Data in Images by Simple LSB Substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004.

[12] Walton, S., "Image Authentication for a Slippery New Age", Dr. Dobb's J., vol. 20, no. 4, pp. 18–26, 1995,.

[13] Wang, R.Z., Lin, C.F., and Lin, J.C., "Image Hiding by Optimal LSB Substitution and Genetic Algorithm", Pattern Recognit., vol. 34, no. 3, pp. 671–683, 2001.

[14] D. C. Wu and W. H. Tsai, "A Steganographic Method for Images by Pixel-Value Differencing," Pattern Recognit. Lett., vol. 24, no. 9–10, pp. 1613–1626, 2003.

[15] 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," Proc. Inst. Elect. Eng., Vis. Images Signal Process., vol. 152, no. 5, pp. 611–615, 2005.

[16] Cheng-Hsing Yang, Chi-Yao Weng, Shiuh-Jeng Wang, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems**."** IEEE Transactions on. Information Forensics and Security, Vol. 3, no. 3, September 2008.

[17] Rafel C. Gonzalez, Richard E. Woods, "Digital Image Processing" 2nd ed., 2002.