Research Journal of Applied Sciences, Engineering and Technology 8(3): 387-393, 2014
DOI:10.19026/rjaset.8.984
ISSN: 2040-7459; e-ISSN: 2040-7467
© 2014 Maxwell Scientific Publication Corp.
Submitted: March 19, 2014 Accepted: April 15, 2014 Published: July 15, 2014

Research Article

Double Hiding Information in Color Image File Based on Classical LSB Method

[1, 2]Aymen Mudheher Badr, [1]Xiao Di and [3]Husham T. Ibrahim
[1]College of Computer Science and Technology, Chongqing University, China
[2]Faculty of Engineering, Diyala University, Diyala, Iraq
[3]Faculty of Engineering, Basra University, Basra, Iraq

Abstract: This study presents a two principles, Cryptography and Steganography, each tow methods work separately from the other to ensure a secure content. We are developed an algorithm to increase the safety and reliability of the copyrights of the images or books (etc.) that published on the internet by providing a watermark image (as logo) hiding inside the original file that we want product it. Firstly reading image (the logo image), convert it to binary and encrypted it by using EX-OR with a secret key and embedding it inside a gray image in the LSB (in the 1st) and hiding first key in the 2nd bit and the second key in the 3rd bit, then we embedding them in the LSB of Original image in RGB to be protected. The two secret keys, first one as an encryption key and the second key using as signature (data) that have been taken from the cover image (original) to make sure the reliability of the image transmitted via the Internet.

Keywords: Cryptography, EX-OR, gray code, LSB, steganography, watermark

INTRODUCTION

The development in computer technology and communication to increase the need to provide protection and security for files and information stored in it from tampering with or changed by thieves and hackers (Unauthorized), Hence there is a need to provide a means of security data, including cryptography, which serves to provide protection for the storage of data by changing the shape of or the content of the information is not clear manner using a secret key.

Due to the increased use of the World Wide Web has become difficult to protect such information private and that in the formula sends to doubt the intruder as a result of the imposition of several restrictions to prevent the use of encryption across the network led to the emergence of another way in the development of security data which is aware of hiding information and the aim is hackers knowledge of hidden information, but to remove doubt originally the existence of this information and especially thing in hiding technique they keep pace with modern technology and can be used in all media of computer images and text and audio and video network packets.

The scientific data encryption and steganography that represented on hidden writing a watermark and ways to provide security and confidentiality of the data transmitted, where they work together to encode the message transmitted and hide the existence of a connection between the two parties.

The researcher (Ali, 2010) has the hidden text within a color image of the type (BMP) based on the least significant bit where it was hide in first-third of the image and the lowest and the least amount of distortion on the image data.

And researcher (Saurabh and Gaurav, 2010) the proposal watermark technology that distinguish characters used to ensure the integrity of the security hidden data in the files.

We can hide the information in different ways in the digital images have been in this study adoption of spatial domain by using Least Significant Bit (LSB) has been used type of image files (BMP, JPEG and TIFF) as a cover and the pictures represent watermark.

Robust digital image watermarking can also be classified into two major categories spatial domain and transform domain watermarking. There are three important issues in the watermark system.

First, the embedded watermark should not degrade the quality of the image and should be perceptually invisible to maintain its protective secrecy. Second, the watermark must be robust enough to resist common image processing attacks and not be easily removable, only the owner of the image ought to be able to extract the watermark.

Robust watermarking systems are expected to withstand different kind of attacks: image compression, introduction of noise, low pass filtering and image rescaling cropping, rotation JPEG compression are

Corresponding Author: Aymen Mudheher Badr, Computer Science and Technology, Chongqing University, China

This work is licensed under a Creative Commons Attribution 4.0 International License (URL: http://creativecommons.org/licenses/by/4.0/).

some, but a few of types of attacks that often are not addressed in most literatures. And lastly the viability of a watermarking may also be judged by how much data it can store into the host image.

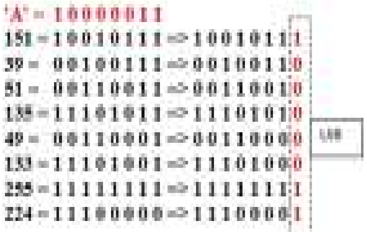
We can hide the information in different ways in the images have been in this search adoption of the spatial domain by using the Least Significant Bit (LSB) was used type of image files BMP, JPEG and TIFF as a cover and the image represent watermark (Lokeswara Reedy *et al*., 2011).

For example, to hide data in LSB For a gray scale image that represents each value of the 8-bit color is converted to a series of binary numbers to hide the character, for example to hiding ‘A’ in gray scale image must convert ‘A’ to binary (ASCII) and convert the gray scale image to binary array shown in Fig. 1 (Ronald, 2006; Hartung and Kutter, 1999).
In every color images color value which is 24-bit.

When we want to hide the character after the conversion character to binary and convert each value of color in the color image from decimal to binary and since each value of color is made up of three values are Red, Green and Blue (RGB), then the embedding was be easily and do not affect the data's original Fig. 2.
And now embedding “A” in LSB as shown in Fig. 3:

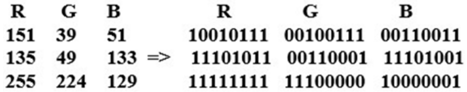
'A' = 1 0 0 0 0 0 1 1

Work included put up the structure of the proposed algorithm in the third paragraph and included an algorithm to hide the Watermark and retrieval In the fourth paragraph, the results have been obtained from the application of the algorithm on several types Of different resolution images; the fifth paragraph has been to review the conclusions and was finally put forward some proposals For future work in the sixth paragraph.



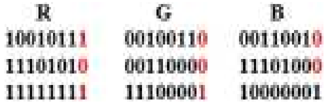
```
'A' = 10000011
151 = 10010111 => 1001011 1
39 =  00100111 => 0010011 0
51 =  00110011 => 0011001 0
135 = 11101011 => 1110101 0
49 =  00110001 => 0011000 0
133 = 11101001 => 1110100 0
255 = 11111111 => 1111111 1
224 = 11100000 => 1110000 1
```

Fig. 1: Covert letter to binary and how LSB



R	G	B		R	G	B
151	39	51		10010111	00100111	00110011
135	49	133	=>	11101011	00110001	11101001
255	224	129		11111111	11100000	10000001

Fig. 2: Convert RGB to binary



R	G	B
10010111	00100110	00110010
11101010	00110000	11101000
11111111	11100001	10000001

Fig. 3: Embedding “A” in the LSB

PROPOSED METHODS

In our scheme, a binary (logo) image is used as the original watermark W of size pixels 512*512, which is shown in Fig. 4a. In order to construct a good watermark for embedding, the original watermark is permuted to obtain a pseudo random sequence, which uncorrelated to the original watermark as shown in Fig. 4b. This is done by performing bitwise EX-OR operation between the original watermark bits and random bits, which generated using a secret key (k). Then we embedding that encrypted image (W″) and the first key (secret key) and the second key (as signature using to test the validity and reliability of the cover file) to the Second watermark (cover 1) gray scale image to obtain (W2′); finally we embedding cover 1 (W2′) to cover 2 color cover (c).

The fourth algorithm to check values of two keys if same, then extract the original watermark (message) from the two covers (gray and color images), if not same then send error message and end.

The algorithm has been applied on image types (BMP, JPG and TIFF) as watermark and color cover.

Algorithm I: Encrypted the message (W):
Input: Watermark (message) as image gray level and its size (512*512), secret key (k)

Output: Encrypted watermark (W″)
----

1. Reading the first image (message) as gray scale level and refer to it (w):

   $W = \{w (i, j), 1 \le i \le 512, 1 \le j \le 512, w (i, j) \epsilon (0, 1)\}$

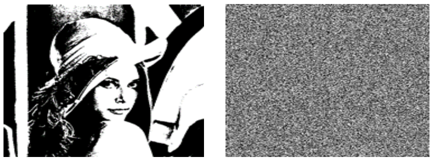
2. Resize of it to 512*512
3. Reading secret key (k) and generate the random array (K) binary sequence:

   $K1 = \{k (i, j), 1 \le i \le 512, 1 \le j \le 512, k (i, j) \epsilon (0, 1)\}$

4. Use XOR function to generate a secret watermark (W′):

   $W' = W \oplus K$ where $\oplus$ denotes XOR operation

5. The permuted watermark W″ is obtained by applying Gray code to W′, shown in Fig. 4



(a) (b)

Fig. 4: (a) Original watermark, (b) permuted watermark

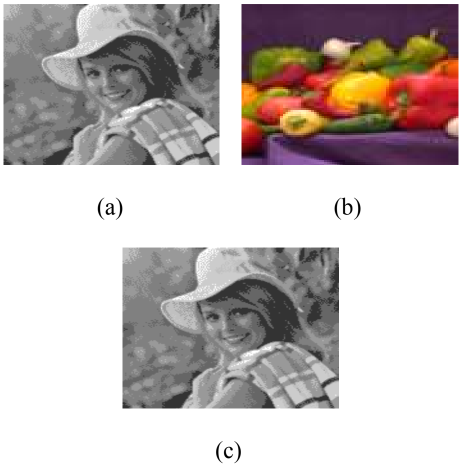


Fig. 5: (a) Second watermark w2, (b) color cover c, (c) watermark W2′ after embedded

Algorithm II: First embedding:
Input: Secret Watermark (W″), first key (K1), second key (K2), Color image (c)

Output: Second watermark (W2′)
----

1. Reading color image (c) to use it as a final cover
2. Reading the second image w2 (watermark 2) as gray scale
3. Embedding W″ (the secret message) in the left significant bit to (w2) by using LSB algorithm in the first bit
4. Embedding the first key (K1) in the second bit
5. By using the second key (K2), take some data from different location in color image and sort it as an array
6. Embedding the second key (K2) in the third bit of color cover (c)
7. W2′ the permuted watermark shown in Fig. 5

Algorithm III: Second embedding:
Input: Watermark (W2′), Color image (c)
Output: final image (C)
----

1. Start
2. Embedding (W2′) in left significant bit to color cover by using LSB algorithm for each color value (R, G and B) in that case we change 9-bit from each color value in image
3. Display the color image (cover file) and save it to send, shown in Fig. 6

Watermark extraction:

- Start
- Reading color image (c)
- Extract the gray image from the left significant bit from the first bit to (R, G and B) colors in the image (c) and save it as a gray image (W2′)
- Extract the encrypted message (W″) and the value of the first secret key (K1′) and the second key (K2′) from the gray image (W2′) from the second and third bit
- Convert (K2) from (K2′) and (K1) from (K1′) and (W′) from (W″) by using gray code algorithm
- Check the second key (K2) if same data in original color image, then the color cover is original, else send "error wrong cover image" and exit from the program

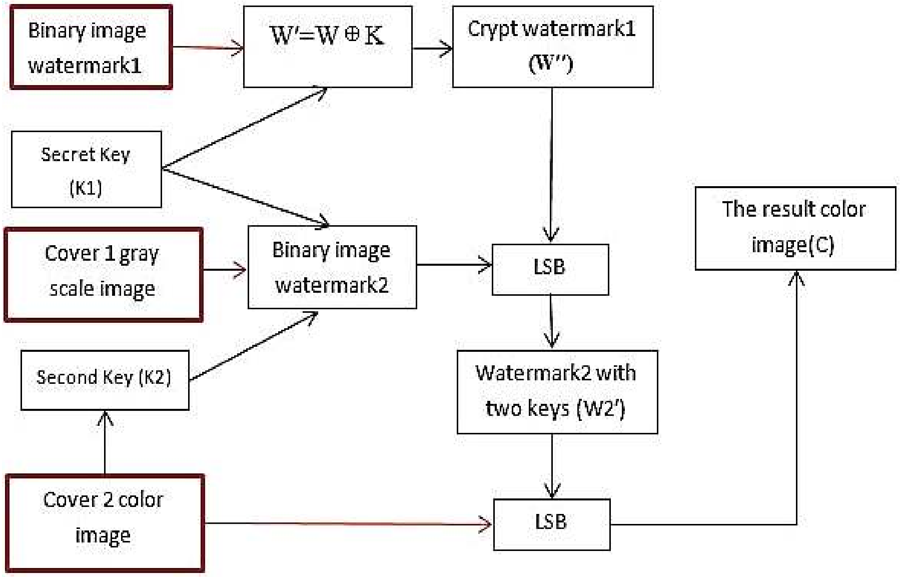


Fig. 6: The proposed watermark embedding scheme

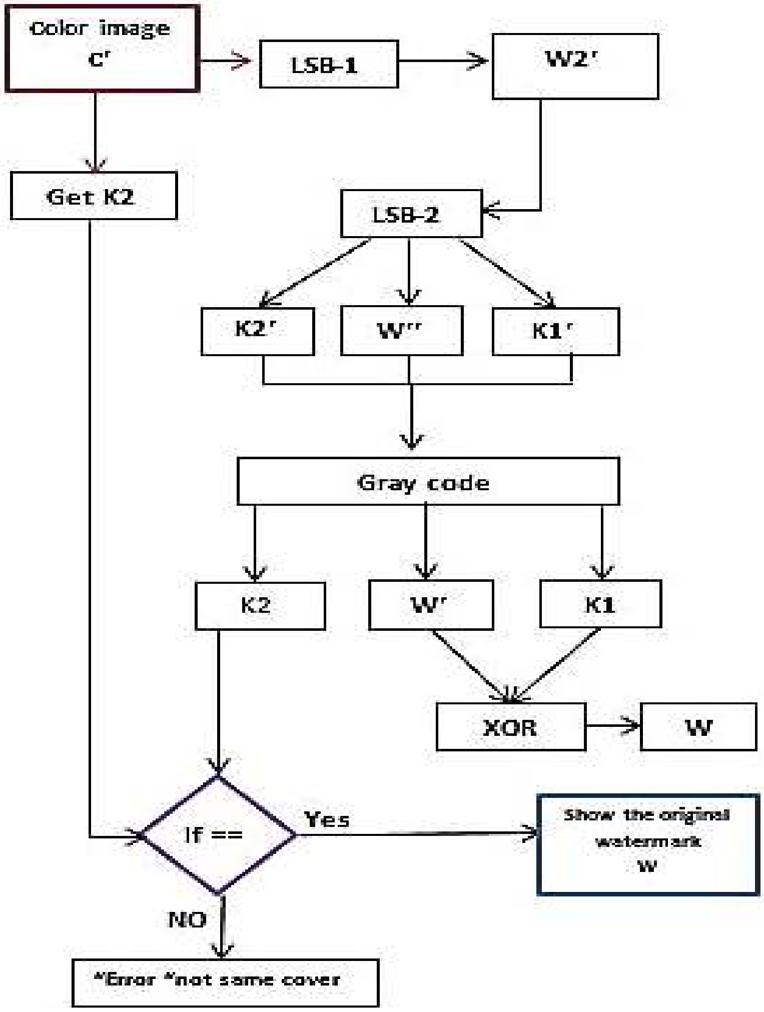


Fig. 7: The extraction watermark

- By using the (K1) to generate random array and input it with the cover1 (W′) to XE-OR operation to decryption and show the original message (W)
- Calculate the value of NC (Normalization Correlation), shown in Fig. 7

RESULTS AND DISCUSSION

Has been the adoption of a number of measures to turn a measuring image quality resulting from the application of an algorithm (Huajian, 2008; Teruya and Kentaro, 2010; Mamta *et al*., 2009):

- Normalization Correlation (NC):

$$NC = \Sigma_i \text{ sw } (i) * s \text{ } (i) / \Sigma_i (s \text{ } (i))^2 \qquad (1)$$

- Mean Squared Error (MSE):

$$MSE = 1/M*N \text{ } \Sigma_{ij} (\text{sw } (i, j) - s \text{ } (i, j))^2 \qquad (2)$$

- Peak Signal To Noise Ratio (PSNR):

$$PSNR=20*\log 10 \left(\frac{255}{\sqrt{\frac{1}{M*N}\Sigma_i \Sigma_j (sw(i,j)-s(i,j))^2}}\right) \qquad (3)$$

where,

SW : Represent the values of an array that contains the watermark
S : The original array values
M : Represents the number of rows
N : Represents the number of columns

For the purpose of measuring the quality of the image containing the resulting watermark the results were as shown in the Fig. 8 with Table 1 and 2 and Fig. 9 with Table 3 and 4 which describes the process of hiding and retrieving the watermark and Table 1 to 4 shows the values of (MSE, PSNR) of the previous forms, respectively (For all the image in that size the NC = 1).

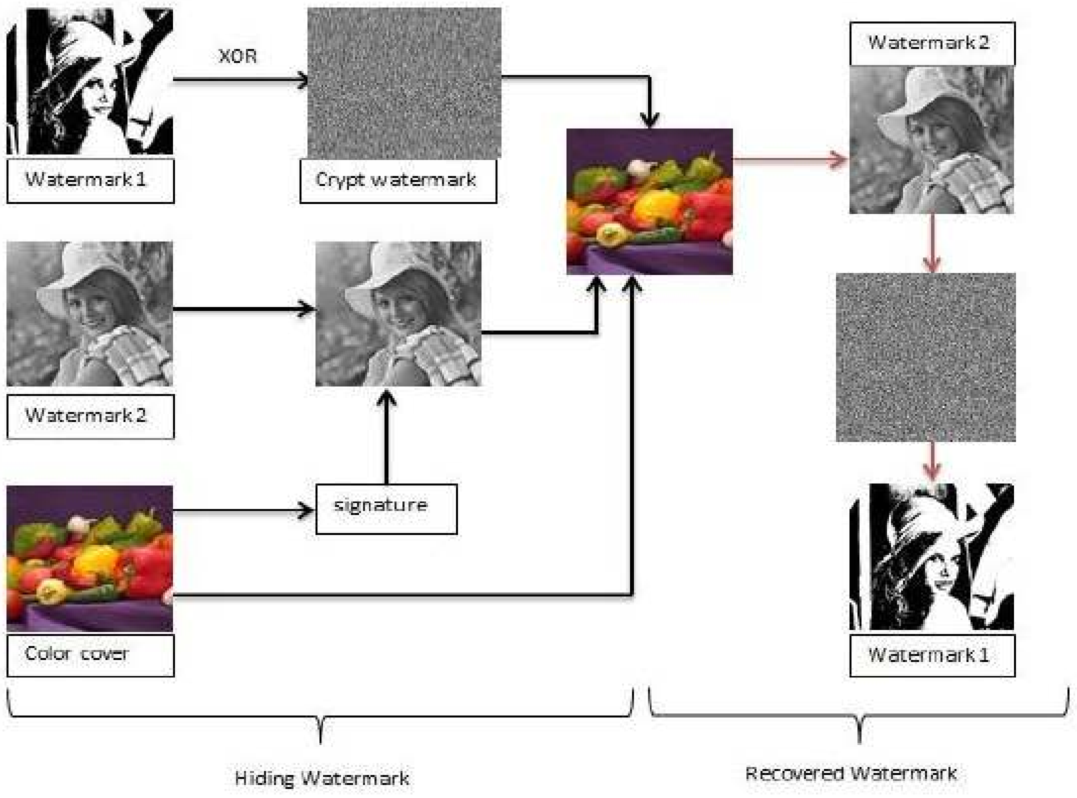


Fig. 8: Embedded and recover watermark

Table 1: The MSE and PSNR values to Fig. 8, image size (100×100)

Type of image			JPEG	BMP	TIFF
Image size 100×100	MSE	Gray image	6.3859	6.3276	6.4043
		Color (R)	4.8372	4.8429	4.8226
		Color (G)	5.2237	5.1280	5.1345
		Color (B)	4.8476	4.7746	4.8068
	PSNR	Gray image	40.0785	40.1184	40.0660
		Color (R)	41.2848	41.2797	41.2979
		Color (G)	40.9510	41.0313	41.0258
		Color (B)	41.2755	41.3414	41.3122

Table 2: The MSE and PSNR values to Fig. 8, image size (200×200)

Type of image			JPEG	BMP	TIFF
Image size 200×200	MSE	Gray image	6.2189	6.3041	6.2280
		Color (R)	4.8891	4.8642	4.8926
		Color (G)	5.1821	5.1324	5.1282
		Color (B)	4.8946	4.9548	4.9533
	PSNR	Gray image	40.1940	40.1345	40.1873
		Color (R)	41.2385	41.2606	41.2354
		Color (G)	40.9857	41.0275	41.0311
		Color (B)	41.2333	41.1805	41.1818

Table 3: The MSE and PSNR values to Fig. 9, image size (100×100)

Type of image			JPEG	BMP	TIFF
Image size 100×100	MSE	Gray image	4.3165	4.4722	4.3241
		Color (R)	2.5462	2.6796	2.5301
		Color (G)	2.6146	2.8363	2.5828
		Color (B)	2.6530	2.8408	2.6268
	PSNR	Gray image	41.7794	41.6258	41.7718
		Color (R)	44.0718	43.8501	44.0994
		Color (G)	43.9567	43.6032	44.0098
		Color (B)	43.8934	43.5963	43.9365

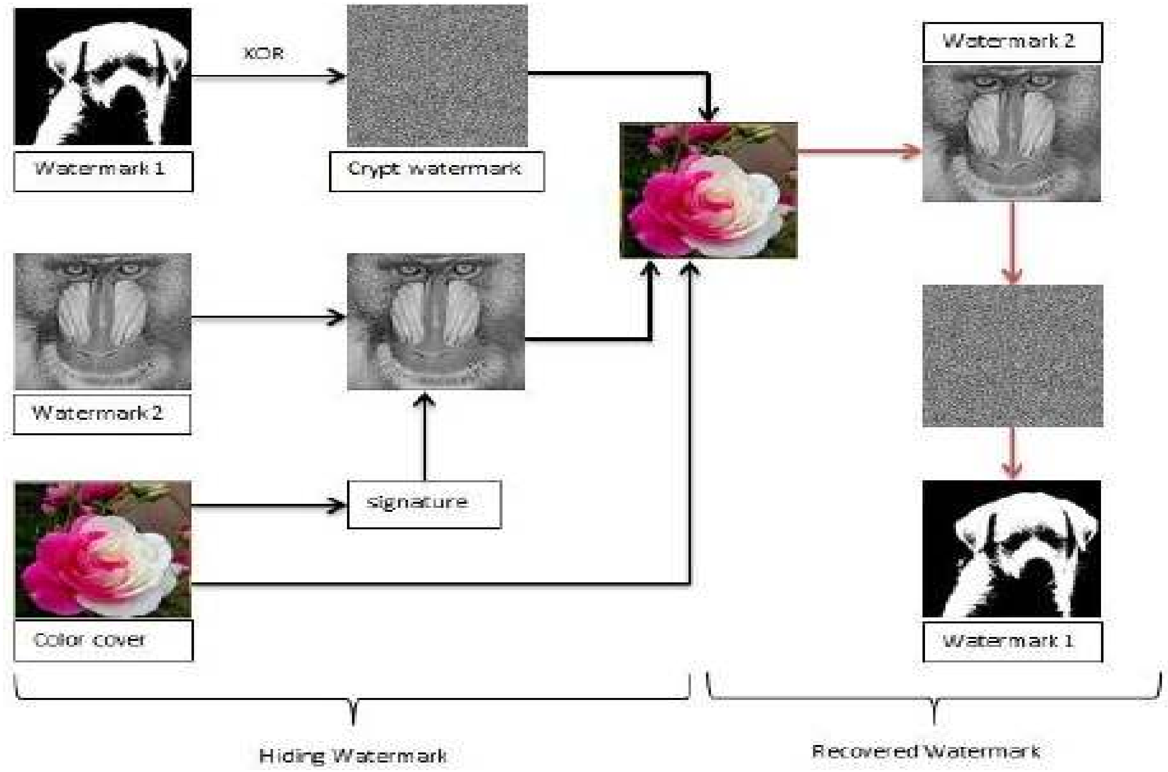


Fig. 9: Embedded and recover watermark

Table 4: The MSE and PSNR values to Fig. 9, image size (200×200)

Type of image			JPEG	BMP	TIFF
Image size 200×200	MSE	Gray image	4.7587	5.1238	4.7649
		Color (R)	2.6491	2.8520	2.6746
		Color (G)	2.6666	2.8189	2.6624
		Color (B)	2.5841	2.7673	2.5982
	PSNR	Gray image	41.3559	41.0348	41.3502
		Color (R)	43.8998	43.5793	43.8582
		Color (G)	43.8712	43.6300	43.8780
		Color (B)	44.0077	43.7102	43.9840

CONCLUSION

The LSB modification technique provides an easy way to embed information in images, but the data can be easily decoded. The proposed scheme used in this study encrypts the secret information before embedding it in the image. After the applicant of the proposed algorithm on more images and in different sizes and for more than one type that show the values of Normalization Correlation (NC) was equal to (1) and the distortion unconsciously suggesting that the recovered image and the rate of signature it exactly identical.

This shows the efficiency of the algorithm's performance to hide the watermark, particularly in the case (9-bit) from every color point value in color image 24-bit (3-bit of each color) and change the first 3-bits of each color point value in gray scale image 8-bit, where embedded the first watermark data and that data where take it from cover file (color image) with the two secret keys.

After calculate the values of performance metrics based on the Mean Squared Error (MSE) had varied within the range of simple suggesting that the margin of error is very small when you use any size of images and any extension and noted that changing the size of the images has nothing to increase or decrease the performance measure and because the algorithm pass on all points of the image sequence (i.e., be enforced in all points of the image without exception).

REFERENCES

Ali, A.N., 2010. An image steganography method with high hiding capacity based on RGB image. Int. J. Signal Image Process., 1(4): 238.

Hartung, F. and M. Kutter, 1999. Multimedia watermarking techniques. Proc. IEEE, 87(7): 1079-1107.

Huajian, L., 2008. Digital Watermarking for Image Content. Geboren, Shandong, China, pp: 47.

Lokeswara Reedy, V., A. Subramanyam and P. Chenna Reddy, 2011. Implementation of LSB steganography and its evaluation for various file formats. Int. J. Adv. Netw. Appl., 2(5): 868-872.

Mamta, J., S.P. Sandhu and W. Ekta, 2009. Application of LSB based steganographic technique for 8-bit color images. Proceedings of World Academy of Science: Engineering and Technology, 50: 427.

Ronald, E.B., 2006. Securing transaction image files using digital watermarking. M.A. Thesis, Department of Science in Information Systems, Athabasca, Alberta.

Saurabh, S. and A. Gaurav, 2010. Use of image to secure text message with the help of LSB replacement. Int. J. Appl. Eng. Res., 1(1): 201.

Teruya, M. and A. Kentaro, 2010. A blind digital image watermarking method using interval wavelet decomposition. Int. J. Signal Process. Image Process. Pattern Recogn., 3(2).