Journal of Engineering and Applied Sciences 14 (11): 3754-3760, 2019
ISSN: 1816-949X
© Medwell Journals, 2019

Adaptive Least-Significant-Bit Substitution Applied in Data Hiding Structure for RGB Image

[1]Hussain A. Younis, [2]Issa Ahmed Abed, [3]Isra'a M. Hayder and [4]Hameed Abdul-Kareem Younis
[1]College of Education for Women, University of Basrah, Basrah, Iraq
[2]Engineering Technical College, Southern Technical University, Basrah, Iraq
[3]Technical Institute, Southern Technical University, Quurna, Iraq
[4]College of Computer Science and Information Technology, University of Basrah, Basrah, Iraq

Abstract: In order to insert the data through the text, image or audio, the data hiding process can be used. Where the audio and text will be embedded into the color image. Third Least-Significant-Bit (LSB 3) will be used here, rather than utilizing Least-Significant-Bit (LSB 1) of the cover for embedding the information which help to improve the reliability. LSB 1 and LSB 2 might be adjusted by bits of data in order to limit the contrast between the cover and the stego cover. In this research, a stego-key is utilized to permute the characters of data before embedding them and this procedures gives more security. The results of the proposed technique proved that the Peak Signal to Noise Ratio (PSNR) is better than the classical strategies for the same topic. Hence, the suggested framework provides good simulation results.

Key words: LSB, data hiding, embedding algorithm, MSE, technique, embedding

INTRODUCTION

Overview: A new open doors for accomplishing the indistinctness and privacy of communication have been presented by the coming and the development of the Internet and calculation of power. In order to protect the information from any probable danger it is suggested steganography as a one solution. It is utilized in clandestine communication (El_Rahman, 2015; Chugh, 2013). To avoid the identification of the concealing information, this information is forbidden by using steganography. Subsequently, the message can't be obvious when use the steganography. The word 'steganos' means "covered or protected" and 'graphie' means "writing" (Petitcola *et al.*, 1999; El_Rahman, 2018). Different methods utilized in order to conceal the information. First is composing a hiding data on tables made from a wood previously camouflaging it with a phony composition over wax. Second, inking the information on the head of the slave at that point trusting that the hair develop for inclusion at that point removing it back when achieving the goal (Petitcola *et al.*, 1999). The sender embeds a secret message into digital media (e.g., image) where only receiver can extract this message (Yadav, 2011). Steganography is consequently, the workmanship and investigation of concealing the way that correspondence is not withstanding occurring as well as the specialty of data covering up (Orebaugh, 2013; Marvel *et al*., 1999). The two parts of information can turn into a solitary element by implanting one part within another. The covering medium consists of multi-media things of practical relevance, like as audio, video or image files which ought to be retrieved with minimal distortion and escape detection (Abduallah *et al*., 2014). Hence, the data of the patient can be included inside the medicinal symbolism which is considered as a one utilization of steganography. The goal of steganography is to avoid drawing suspicion to the transmission of the secret message. In order to make the unapproved person can't identify or even pay attention the nearness of communication it uses the image, audio, text, multimedia and video as a bearer for concealing special data. It takes into consideration verification, copyright insurance and implanting of data in the image or in conveyance of the image (Voyatzis *et al*., 1998). Figure 1 illustrates the steganographic encoder. The message is the data that the sender tries to stay confidential and may be images, video, text, audio or different information which is constructed by train of bits. The technique of the hiding the data is extremely relied upon the temple of the image which is considered as a cover. Therefore, no need similar form for the data and the cover. After that, the stego image is built by hiding the data confidentially in the image this is by using the encoder. The stego should match the input image with casual inspection and permission. Actually, the stego key is important in the

Corresponding Author: Hussain A. Younis, College of Education for Women, University of Basrah, Basrah, Iraq

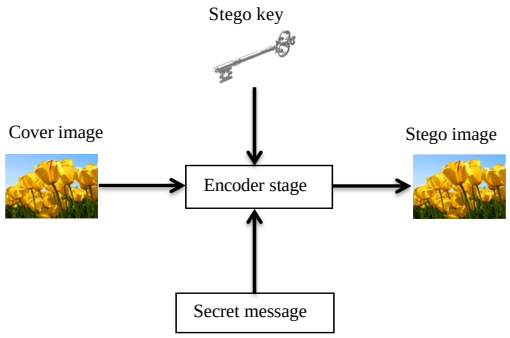

Fig. 1: The encoder of the steganography

encoder because it ensures the person who have the key of decoding is ambidextrous to extract the data from the output image. Retrieving the data from the output image need this image, in addition to the accompany key. The premier input image may or may not be needed; in part of applications it is eligible that the cover image not be needed to find the message.

MATERIALS AND METHODS

Steganography types

Text steganography: In each word of a text message, secrete the message which want to be hidden in each nth letter (Marvel, 2000). In order to conceal the information in the text files, many methods have been used. Text steganography utilizing digital files is not utilized many times where text files own a few amount of redundant data.

Image steganography: In digital steganography, the images are so, common cover source. The data can be secreted within a large amount of redundant bits in the pixels. Where the array of pixels construct the image.

Audio/video steganography: In audio steganography, the masking is considered as a method which take advantage of the ear of the individuals unnoticeably disappear the data. In the turn out of the high audible sound, the dim and audible voice classified as inaudible (Marvel, 2000). The greater size of meaningful audio files makes them less common to utilize than images.

Protocol steganography: The method of embedding messages in the data and system control convention utilized in system conveyance is called protocol steganography (Bender *et al.*, 1996, 2000). For instance of where data can be hidden is in the header of a TCP/IP packet in some fields that are either optional or are never utilized.

Steganography applications

Secret communication: Confidentially, association between two sides without anybody thinking about the communication this is done by steganography. Then cryptography, just encodes the data anyway its reality isn't imperceptibly and after that draws unfortunate intrigue, however, secretes the presence of message in some cover media is steganography. Then sending a cryptographic message draws undesirable attention. The law may be limited the use of cryptographic method. Actually, in the application of a secret communication, if the assailant finds a part of deformation which excites suspicion of the turnout of secret information in a stego image then the encoding of the steganography is failed, although, the assailant is not able to get the message. Preserving perceptual straightforwardness in hiding watermark for copyright protection is what's more of central because of the finishing of the fundamental employment ought to be settled (Wolfgang *et al*, 1999).

Copyright protection: A hidden data is incorporated in the image this will give the watermark and after that recognize it as a licensed innovation which identifies with an explicit proprietor. Hence, the data is the watermark in the screenplay of watermarking (Wolfgang *et al*, 1999; Swanson *et al*., 1998). A watermark help to find whether the image has been thus changed (Wolfgang and Delp, 1999).

Robustness: If the stego-image incurs transformations in this case the robustness means the capability of embedded information to stay unchanged. There are different examples of transformations like addition of random noise, transformation from D/A and after that transformation its again to discrete form, linear and non-linear filtering and scaling and rotations. Anti-watermarking software is found in the internet which presented ability in taking off some watermarks (Petitcolas *et al*., 1999).

Feature tagging: Time stamps, captions and annotations are elements incorporated within the image, like the name for the persons in a picture or position in a chart. Duplicating the stego picture will copy the whole incorporate merits and just the sections who owns the translating stego key capable of getting and finding all the merits.

Discrete watermarking: It inserts a digital watermark within the image. Also, this application can be utilized to prove the originality or on the other hand trustworthiness of the bearer signal or to offers the similarity of its

proprietors. In fact it is conspicuously utilized following copyright infringements and for banknote authentication.

The Substitution of Least Significant Bit (LSB): One of the easier steganography techniques this is utilized LSB. The process of embedding contains continue substitution of every LSB1 of the pixel of image for the bit message. Actually, this technique is able to gild a large amount of information (Karzenbeisser and Perircolas, 2000; Bender *et al*., 2000; Shih, 2017). This method is a totally mutt and it gives a peace fault. The important is a sequential reading of LSB, beginning from the first image pixel to get the hidden message. Unbalanced distribution of the variable pixels is produced by this technique, this is due to the message is incorporated in the top of the image.

Mean Square Error (MSE): This metric is very important in this research where it is the square error accumulative result from the input (cover image) and the output (stego image) (Singh and Kaur 2017) as in Eq. 1:

$$MSE = \frac{\sum_{X,Y}[image_1(x,y)-image_2(x,y)]^2}{xy} \quad (1)$$

Hence, the number of columns and rows in the cover image are x and y. While $image_1$ (x, y) is the input image and $image_2$ (x, y) is the stego-image (Abduallah *et al*., 2014).

Peak Signal to Noise Ratio (PSNR) calculations: It is a mathematical measurement in the processing of the image use to check the goodness of the suggested techniques (Yu *et al*., 2007). The unit of this quality is in decibel (dB). In addition, PSNR measures the contrast in terms of pixels between the original and reconstructed images. Equation 2 illustrates the PSNR:

$$PSNR = 10\times Log_{10}(255^2/MSE_{mean}) \quad (2)$$

$$MSE_{mean} = ((MSE_1+MSE_2+MSE_3)/3) \quad (3)$$

where, MSE_{mean}, MSE_2 and MSE_3 are the errors for the three channels.

The substitution of adaptive LSB: Here, the cover is RGB image with size 256*256. In this case, it can be hidden message of about 65536 bits. In order to defend the data from different effects like compression, noise and filter and improve the robustness, the data is incorporated within LSB3 of the cover image. The explanation is in the following steps.

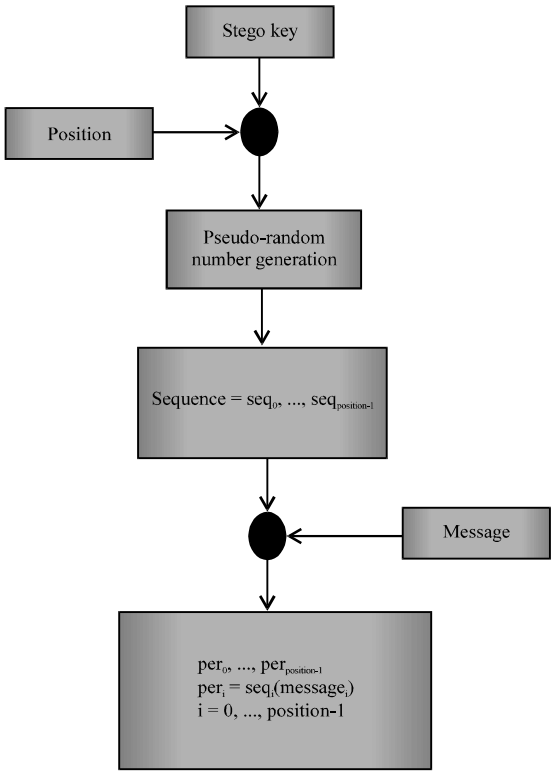

Fig. 2: Permutation

First; The data:

If the message = {$message_0$, $message_1$, ..., $message_{length-1}$}

Length of the message to be embedded is greater than and equal to 1, also it is less than and equal to g+1 where g = 65535. Also, values for message are taken in this research which are 0 and 1. However, k takes the values from 0 until length-1.

Second; Cover image: The image can be analyzed to the pixels as: {$point_0$, $point_1$, ..., $point_g$}. Then, for LSB3, it can denoted as: {cc_0, cc_1, ..., cc_g} with cc_j equal to 0 or 1 and j = 0, ..., g.

Third; Permutation procedures: In this step, different indexes are produce. Where it can use the Pseudo-Random Number Generator (PRNG) and the seed is stego key. Therefore, the stego image can be generated by changing of the group of LSB3 of cover image with permutated characters, hence, the stego image will result in new pixels as shown in Fig. 2.

Fourth; Algorithm: This step is the core of the work. By this algorithm the results are improved further compared to the others. Hence, the first and second bit plane are

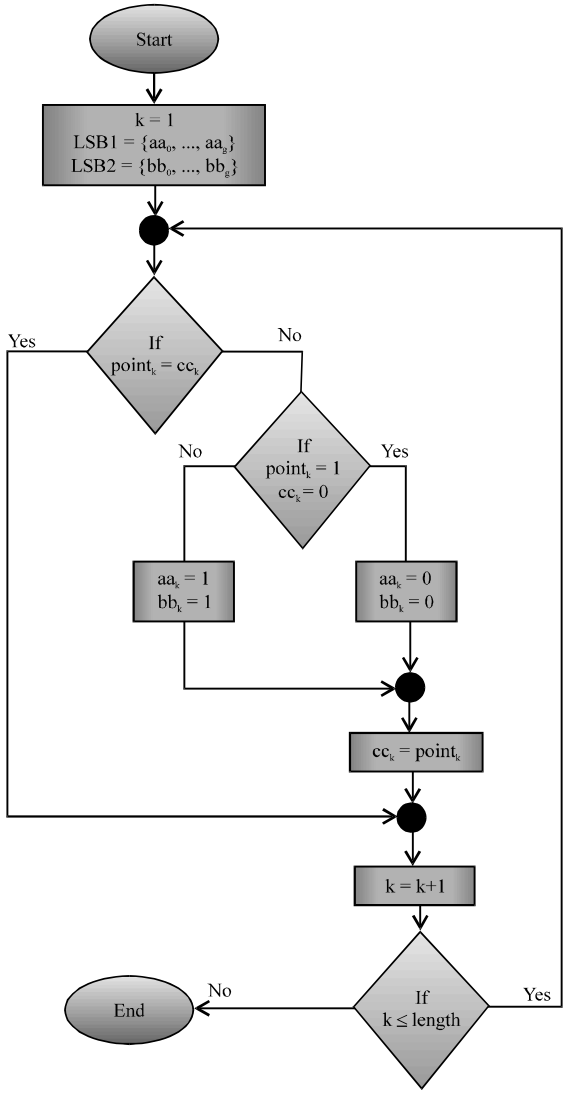

Fig. 3: The proposed method

extracted as $\{aa_0, aa_1, ..., aa_g\}$ and $\{bb_0, bb_1, ..., bb_g\}$, respectively. The complete procedures are presented in Fig. 3.

RESULTS AND DISCUSSION

Different images have been taken, here with RGB of 256*256 dimensions such as airplane, barbara, boatscolor, earth, kit, cmap and cbirds which represent the suggested cover images as in Fig. 4 in order to test the proposed method and check its ability. The research has been done with PC has the following properties:

- Windows 7 Ultimate
- 2 GB RAM
- Intel Atom N2600 CPU
- R2008a MATLAB Version

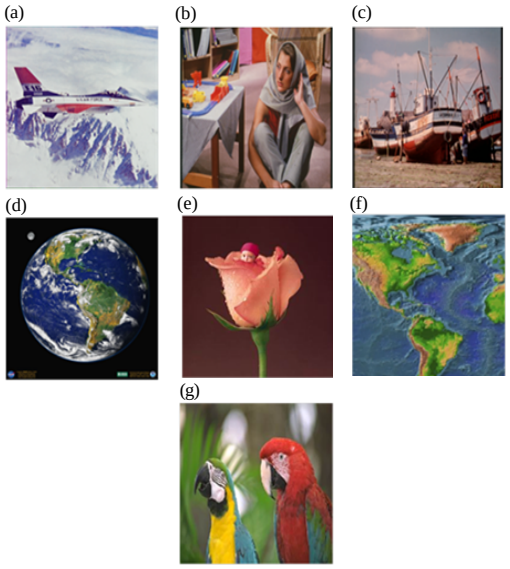

Fig. 4: Sample images: a) Airplane; b) Barbara; c) Boatscolor; d) Earth; e) Kit; f) Cmap and g) Cbirds

Table 1: The method of LSB3

Images	PSNR	MSE_{mean}	MSE_1	MSE_2	MSE_3
Airplane	50.69605	0.55395	0.84033	0.82153	0
Barbara	50.70308	0.55305	0.83081	0.82836	0
Boatscolor	50.64153	0.56095	0.84570	0.83715	0
Earth	50.41505	0.59098	0.89160	0.88134	0
Kit	50.73193	0.54939	0.86303	0.78515	0
Cmap	50.73772	0.54866	0.80761	0.83837	0
Cbirds	50.76162	0.54565	0.80639	0.83056	0

In addition, two types of messages are processed in this study.

Text messages: The size of the suggested text is 6800 bits with contents shown in Fig. 5. After that, the text will be permuted by utilizing stego key as presented in Fig. 6. Audio signal with length 6800 bits as shown in Fig. 7.

In the same procedures, this wave should be permuted with a key before hiding. Figure 8 shows the permuted signal.

Simulation results without algorithm: In this part, the test has been done on different images as shown in Table 1 where the message is embedded using LSB3. Simulation results with incorporating the proposed method. In this part, the LSB1 and LSB2 are modified, also the amount of bits are changed as shown in Table 2-5.

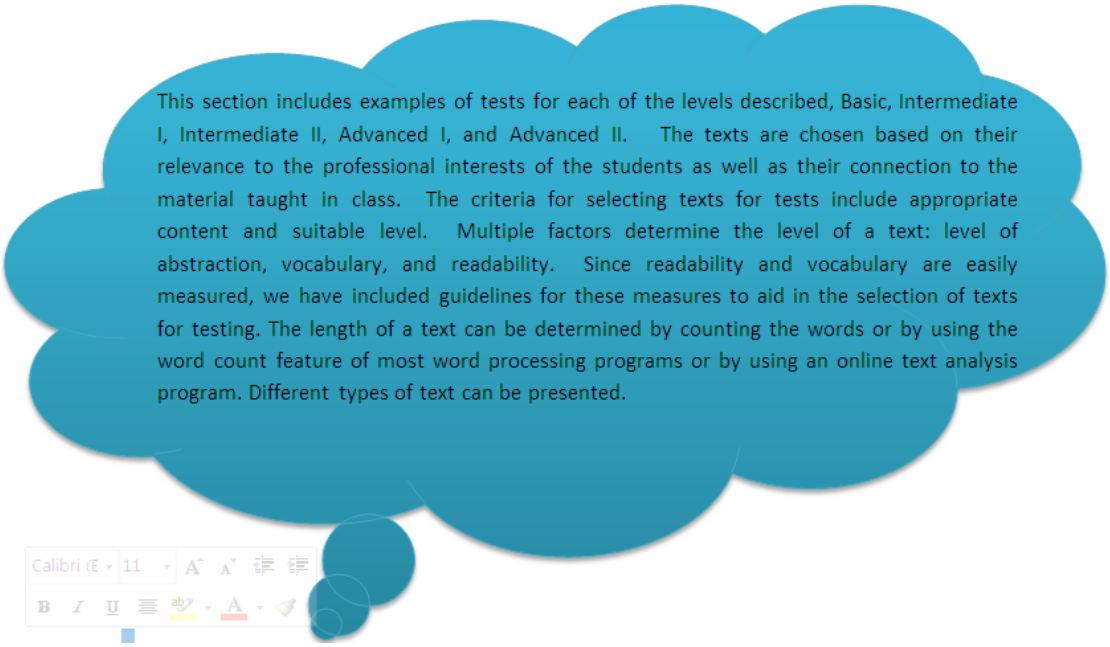

Fig. 5: The proposed text

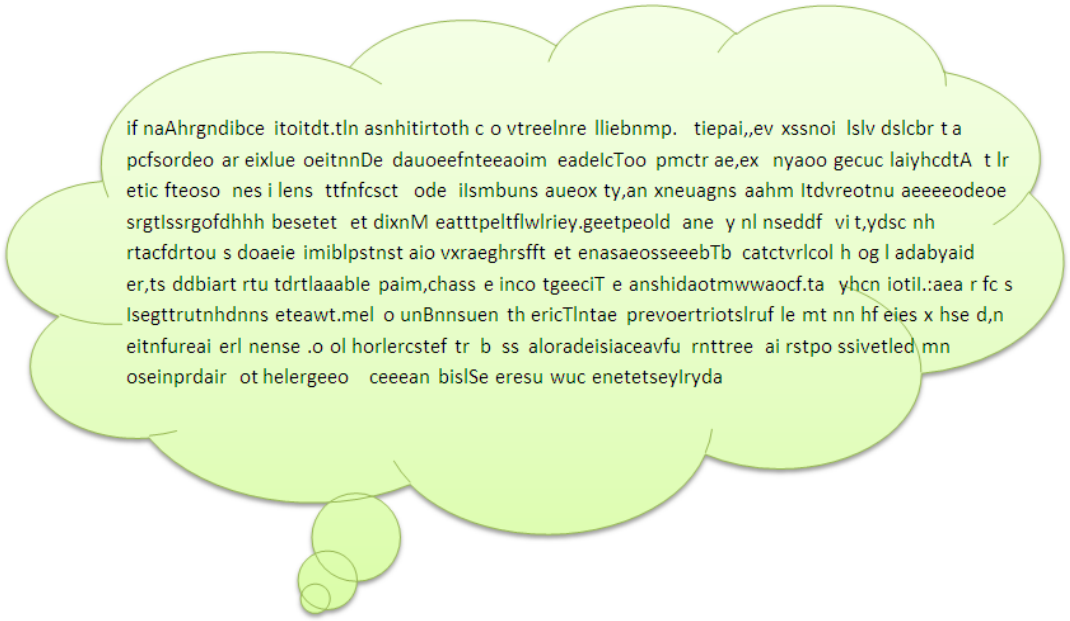

Fig. 6: The text after permutation

Table 2: Embedded bits of 6800 bits

	Images						
Test 1	Airplane	Barbara	Boatscolor	Earth	Kit	Cmap	Cbirds
PSNR	59.1939	59.159	59.3361	58.5685	59.1222	59.2736	59.1467

Table 3: Embedded bits of 5600 bits

	Images						
Test 2	Airplane	Barbara	Boatscolor	Earth	Kit	Cmap	Cbirds
PSNR	60.0507	60.0714	60.1649	59.3913	59.969	60.1565	60.0548

Table 4: Embedded bits of 1000 bits

	Images						
Test 2	Airplane	Barbara	Boatscolor	Earth	Kit	Cmap	Cbirds
PSNR	67.4269	67.3672	67.6663	66.2956	67.3598	67.7546	67.4045

Table 5: Embedded bits of 800 bits

	Images						
Test 3	Airplane	Barbara	Boatscolor	Earth	Kit	Cmap	Cbirds
PSNR	68.3345	68.6914	68.6713	67.2647	68.7623	68.8762	68.4852

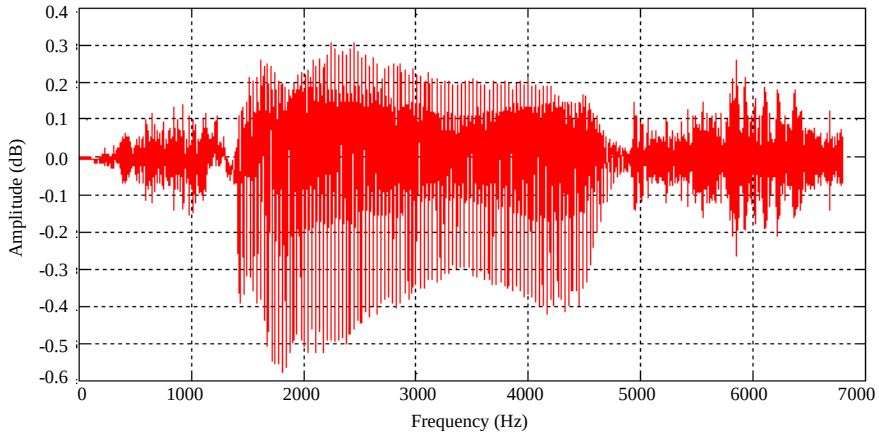

Fig. 7: The waveform of the given audio signal

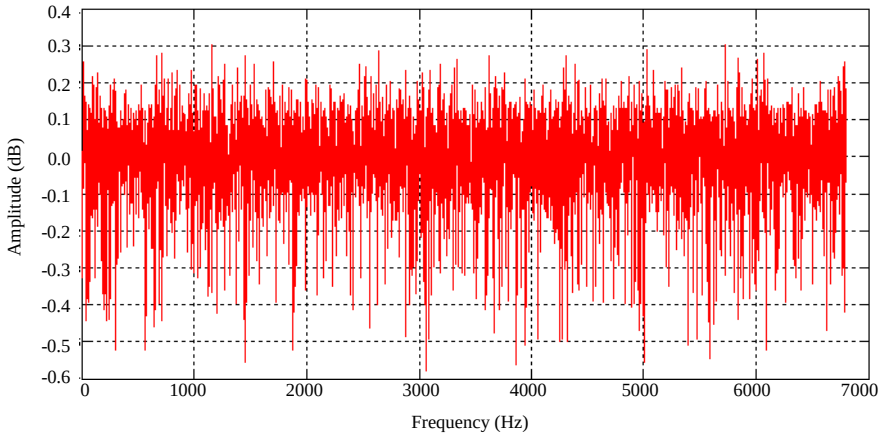

Fig. 8: Signal after permutation

CONCLUSION

Efficient model has been proposed in this study to hide the message within the cover images. The technique includes the modification of LSB1 and LSB2 of the RGB image. Hence, the difference between the input and the output image will be minimum. In that case will produce secret communication with high performance. This means the others can't recognize between the image before the hiding and after the hiding. Different values of bits data are taken to check the effect on the peak signal to noise ratio. All the simulations have been done on the MATLAB Software and the results demonstrate that the algorithm is simple and effective.

ACKNOWLEDGEMENT

I would like to thank all people who helped us in the Basrah University and Southern Technical University.

REFERENCES

Abduallah, W.M., A.M.S. Rahma and A.S.K. Pathan, 2014. Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach. Comput. Electr. Eng., 40: 1390-1404.

Bender, W., D. Gruhl, N. Morimoto and A. Lu, 1996. Techniques for data hiding. IBM. Syst. J., 35: 313-336.

Bender, W., W. Butera, D. Gruhl, R. Hwang, F.J. Paiz and S. Pogreb, 2000. Applications for data hiding. IBM Syst. J., 39: 547-568.

Chugh, G., 2013. Information hiding-steganography & watermarking: A comparitive study. Intl. J. Adv. Res. Comput. Sci., 4: 165-171.

El_Rahman, S.A., 2015. A comprehensive image steganography tool using LSB scheme. Intl. J. Image, Graphics Signal Process., 7: 10-8.

El_Rahman, S.A., 2018. A comparative analysis of image steganography based on DCT algorithm and steganography tool to hide nuclear reactors confidential information. Comput. Electr. Eng., 70: 380-399.

Karzenbeisser, S. and F.A.P. Perircolas, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, UK., ISBN: 9781580530354, Pages: 220.

Marvel, L.M., 2000. Image steganography for hidden communication. Master Thesis, United States Army Research Laboratory, Maryland, USA.

Marvel, L.M., C.G. Boncelet and C.T. Retter, 1999. Spread spectrum image steganography. IEEE Trans. Image Process., 8: 1075-1083.

Orebaugh, A.D., 2013. Steganalysis: A steganography intrusion detection system. J. Steganography, 1: 1-21.

Petitcolas, F.A.P., R.J. Anderson and M.G. Kuhn, 1999. Information hiding-a survey. Proc. IEEE, 87: 1062-1078.

Shih, F.Y., 2017. Digital Watermarking and Steganography: Fundamentals and Techniques. 2nd Edn., CRC Press, New York, USA., ISBN:9781498738774, Pages: 292.

Singh, G. and N. Kaur, 2017. Encryption of Medical Images with Steganography Method. Imperial J. Interdiscip. Res., 3: 1090-1094.

Swanson, M.D., M. Kobayashi and A.H. Tewfik, 1998. Multimedia data embedding and watermarking technologies. Proc. IEEE, 86: 1064-1087.

Voyatzis, G., N. Nikolaidis and I. Pitas, 1998. Digital watermarking: An overview. Proceedings of the 9th European Conference on Signal Processing Conference (EUSIPCO 1998), September 8-11, 1998, IEEE, Rhodes, Greece, ISBN:978-960-7620-06-4, pp: 1-4.

Wolfgang, R.B. and E.J. Delp, 1999. Fragile watermarking using the VW2D watermark. Proceedings of the SPIE Security and Watermarking of Multimedia Contents, Volume 3657, January 23, 1999, San Jose, CA., USA., pp: 204-213.

Wolfgang, R.B., C.I. Podilchuk and E.J. Delp, 1999. Perceptual watermarks for digital images and video. Proc. IEEE, 87: 1108-1126.

Yadav, R., 2011. Study of information hiding techniques and their counterattacks: A review article. Intl. J. Comput. Sci. Commun. Netw., 1: 142-164.

Yu, Y.H., C.C. Chang and I.C. Lin, 2007. A new steganographic method for color and grayscale image hiding. Comput. Vision Image Understanding, 107: 183-194.