Image and audio steganography based on indirect LSB

Article *in* Kuwait Journal of Science · August 2021

DOI: 10.48129/kjs.v48i4.8992

2 authors, including:

Ban N. Dhannoon
Al-Nahrain University
75 PUBLICATIONS **215** CITATIONS

SEE PROFILE

Kuwait J.Sci., Vol.48, No.(4),October.2021,pp(1-12)

Image and audio steganography based on indirect LSB

Zainab N. Sultani *, Ban N. Dhannoon
Dept. Computer Science, College of Science, Al-Nahrain University, Baghdad, Iraq
** Corresponding author: zna@sc.nahrainuniv.edu.iq*

Abstract

Hiding the presence of data during communication has become a pressing concern in this overly digitalized world as a consequence of illegitimate access. These concerns have led to cryptography and steganography techniques as methods for securing data. This paper presents a modified information hiding technique based on an indirect least significant bit. Instead of saving each bit of the secret message in the least significant bit (LSB) of the cover media, each bit of the secret message is compared to a mask bit in the cover media. The result is saved in the cover media's LSB. In this paper, two steganography schemas are designed in which the cover media are image and audio, while the secret message is a text file. A simple encryption technique is used to transform the secret message into an unreadable format before the hiding process begins. The experimental results indicate that the proposed algorithm achieves promising performance.

Keywords: Audio; image; LSB; steganography; multimedia eecurity

1. Introduction

In recent years, the capability of media data exchange over the Internet has become much easier and faster due to the fast progress in multimedia technologies and new trends in the field of communication (Bhardwaj & Sharma, 2016). As a result, issues related to security and vulnerability have become a vital concern. Digital texts in the form of text files or messages are used widely, such as in email, short message service (SMS), mobile banking, and news transmitted as plain, understandable, and readable text, exposing the content to attacks (Taleby Ahvanooey *et al*., 2019). Hackers attempt to exploit such communications by copying, modifying, or destroying confidential information, whether it is text, image, audio, or video, while it is being transmitted. There is a need to secure the message against ordinary listeners and unauthorized professional recipients (cryptanalysts). Security in terms of hours is needed for observers, while for the cryptanalyst, it may be in terms of years (Latef *et al*., 2011). Cryptography and steganography are two of the research fields in information security (Maniriho & Ahmad, 2019); while the objective of both techniques is to protect data, they have different concepts. Cryptography is a method that incorporates protecting communication by encrypting data before being transmitted without concealing the communication's existence. The encrypted message is prone to doubt if it falls into hackers' hands; thus, there is a need to use a hiding technique such as steganography to ensure security (Mahmood & Dhannoon, 2017). Steganography is the science of concealing information in cover media such as text, image, audio or video while preventing unwanted access from discovering the existence of secret data (Ali & George, 2016). The word "hiding" means to preserve secret information through unknown communication. The "secret" media is covertly placed inside another media (cover) such that it remains inconspicuous to unintentional receivers. The word "steganography" is obtained from

the Greek words steganos and graphein, meaning "covered" and "to write", respectively, and refers to the art/technique of enabling covert communication that uses creative methods to conceal information in plain sight (Arora, 2018). In image steganography, secret data are hidden in a cover image called a stego image, whereas, in audio steganography, the cover media is an audio file (Maniriho & Ahmad, 2019). In the stego image or audio, the statistical properties must be maintained after concealing the secret data (Swain, 2019).

In Section 2, related work in both image and audio steganography is summarized. Besides, the scope and contribution of the paper are presented. A brief discussion of LSB is presented in Section 3, and Section 4 describes the proposed method. Section 5 presents the evaluation metrics. In Section 6, results and discussion are detailed. Section 7 concludes the paper.

2. Related work

Many researchers have concentrated on designing and developing algorithms for hiding data in an image data or audio signal in the past few years.

2.1 Image

(Lin *et al*., 2001) developed a novel technique to hide important information in the cover image. The main idea of the proposed technique is using LSB substitution. To prohibit illegal access of data and at the same time enhance the system performance, randomized and optimal LSB substitution are designed. They developed a genetic algorithm to tackle the problem of hiding secret data in the rightmost k LSBs of the cover image, which could consume time to discover the optimal result when the k value is large. Using perceptual modeling concept, an enhanced concealing technique is designed, to achieve an improved embedding result. In (Parvez & Gutub, 2011), a color image steganography technique is designed where the number of secret data bits selected to be saved in the cover image is flexible. The proposed technique has two stages. It uses the capacity of the cover image file as much as possible by selecting a partition of the color values. Using the selected partition, the channel intensity values are used to specify the number of bits that a pixel can save. In (Dhannoon, 2013), an idea focused on indirectly concealing secret messages in the most significant bit (MSB) of the cover image while using the least significant bit to guide the hiding value is introduced. The method also uses an encrypted key to indicate which bits to be used to hide the secret image. Consequently, it becomes complicated to extract hidden information without knowing the retrieval method and the secret key. In (Jose, 2014), the researcher used a 3-bit LSB and RC4 for hiding an image in a cover image. To enhance the classic LSB method, in which the bits are embedded sequentially in the cover media, random pixels are selected from the cover image. Those pixel locations are generated using the RC4 algorithm, where the bits of the secret image are hidden in the respective order. In (Islam *et al*., 2014), an effective filtering approach for improving LSB image steganography is proposed. The LSB bit in the cover image is checked to determine whether it is suitable for the message bit hiding. Therefore, the cover image hides both the secret message and the bit status, which is saved in the MSB. In (Bhardwaj & Sharma, 2016), an image steganography technique in which the secret information is hidden using inverted LSB in random pixels generated through a pseudo number generator is proposed. A comparison of two different techniques is presented in (Abdel Wahab *et al*., 2019). The first technique uses LSB without using encryption or compression, while in the second technique, the secret information is encrypted, and then the LSB technique is applied. The payload bits are placed into the cover image LSBs, in the spatial domain, to create the steganography image, while the DCT algorithm is utilized such that the

payload bits are concealed into the cover image's frequency components. In (Swain, 2019), a steganography technique is presented using differencing and substitution techniques. The image is divided into 3×3 blocks with no overlap, and for every pixel of each block, the LSB method is applied to 2 LSBs, while quotient value differencing (QVD) is applied to the remaining 6 bits.

2.2 Audio

A new schema for audio steganography is presented in (Pathak *et al*., 2014); the schema is based on diffusing the secret message over host audio. The selected position for the secret bit from positions 0 through 7 LSB in the host sample depends on the decimal value of 3 MSBs. In (Tanwar *et al*., 2014), the authors divide the cover sound into samples to be concealed by distributing the bit representation of the secret image (grayscale) using the LSBs of the preprocessed audio samples. In the LSB technique, the bits from the secret information are saved in the LSB in the cover media. Using the discrete cosine transform (DCT) technique, the embedding of secret information in the media relies on the DCT coefficients. Any DCT coefficient value above a suitable threshold is a possible place for the secret information to be inserted. Authors (Hmood *et al*., 2012) suggested a new method for hiding an image in a cover audio file. First, the red, green, and blue (RGB) images are encrypted, and a discrete wavelet transform is applied to the audio signal to retrieve the high and low frequencies. Then, the encrypted image is concealed within the audio's high-frequency part, where the 2 bits LSB algorithm is used. In (Hosny *et al*., 2018), two novel approaches are proposed; the first approach is to randomize the specified frame used to conceal data using a "PN" sequence generator. The second approach is to hide secret information in the cover media's higher significant bits. The simulated annealing technique used for optimization can hide the secret message binary representation in "higher significant bits" of the cover audio samples and flip other bits values to minimize the error. In (Rajput *et al*., 2017), two algorithms are designed; in Algorithm-I, 2 bits of the secret message are hidden at LSB positions of the cover audio based on the 3 MSBs. Algorithm-II also uses 2 bits of the secret message, which are hidden in the LSB of the cover audio but at the compliment of 3 MSBs.

In this paper, image and audio steganography schemas are presented. The hiding technique is based on LSB, but with modification to what is being saved or hidden. Instead of hiding the binary representation of the secret message, a comparison result between the secret message bit and a mask bit from the cover media is saved into the LSB. Specifically, in image steganography, the mask bit is retrieved from the first cell for each channel (RGB) by extracting the location of bit "1" in the binary representation of the first cell. While in audio steganography, the mask bit location is specified using the location of bit "1" of the binary representation of the audio length.

This technique is proposed to enhance the hiding process, where the typical LSB technique is known, and the operation is static so that the secret message can be easily extracted from the cover media. On the contrary, in this paper, the operation is dynamic and random since, in audio steganography, the length of the cover audio is variable. In image steganography, 3 different locations are specified. Therefore the comparing is applied to different bit locations in the cover media.

3. The Proposed Steganography Schemas

A new method to conceal secret information by incorporating both cryptography and steganography techniques is proposed. In this paper, audio and image steganography schemas are designed.

3.1 Audio steganography schema

The procedure of the proposed audio steganography schema is illustrated in Figure 1. The cover media is an audio wave file, while the secret message is an English alphabetic text. The audio and the secret message are read, and their lengths are extracted; if the length of the text message multiplied by eight is greater than the audio length, then steganography cannot be performed. Before hiding the secret message, encryption is applied to ensure 2-layer security. The XOR operation is applied to the bit message with the mode of different predefined prime numbers to randomize the encrypted output. Then, the encrypted message is transformed into a bit representation, ready to be concealed in the audio file; see Figures 2 and 3.

To enhance the LSB algorithm, the indirect LSB method is suggested. In this method, each bit in the encrypted secret message is compared to a mask bit in the audio sample, and the result of the comparison is saved in the LSB audio sample.

Those mask bit locations are retrieved using the bit representation of the audio length. Suppose that the length of an audio file equals 73113 samples. Then, its bit representation is 10001110110011001, so the L vector that holds the locations of bit 1 is

L= [1, 4, 5, 8, 9, 11, 12, 13, 17]

The first location (1) is ignored since it is reserved for the LSB insertion. Locations greater than 16 are neglected because the audio sample used in this paper is 16-bit; therefore, location (17) is also ignored.

Using the indirect LSB technique, each encrypted message bit is compared to a bit from the audio cover, where its location is retrieved from the L vector; see Figure 4a. For example, in the first sample, the bit at location 4 is used for the comparison, and so on for the next value of the L vector. If the encrypted bit value is equal to the bit value in the sample audio, then the audio sample

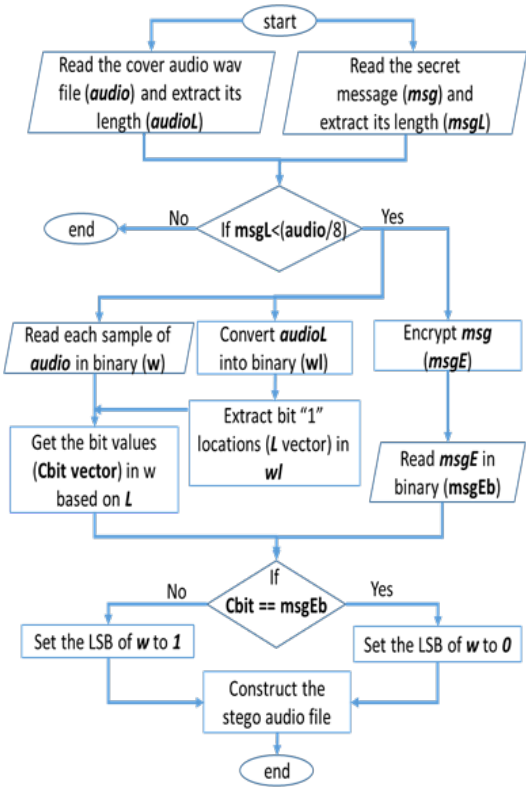

Fig. 1. Proposed Audio Steganography Flowchart

Text Encryption Algorithm

Input: secret message: **msg (1×msgL)**, prime_vector: **pr**
Output: encrypted message: **msgE (1×msgL)**

```
Function encrypt (msg,pr):
    msg_ascii = char_to_ascii(msg)
    j=1;
    for k=1:length(msg_ascii)
        ascii_byte = BINARY(msg_ascii(k));
        msgE(k) = XOR(ascii_byte, MOD(k, binary(pr(j))) ;
        j=j+1;
        if j> length(pr)
            j=1;
        end if
    end for
return msgE
```

Fig. 2. Secret Message Encryption Algorithm

Secret Message

V	i	d	e	o	

ASCII Representation

86	105	100	101	111	32

Encrypted Secret Message (repeatedly, XOR with mode prime 5, 13, 23)

W	k	g	a	j	&

Encrypted Secret Message 8-bit representation (msgEb)

01010111	01101011	01100111	01100001	01101010	00100110

Fig. 3. Secret Message Encryption Example

LSB is set to zero otherwise; otherwise, it is set to 1, as shown in Figure 4b. Finally, when the message bit length is reached, the steganography process is finished, and the audio-stego file is finalized.

3.2 Image steganography schema

In the proposed image steganography schema, the same stages are applied but with some modifications in selecting the location in each image channel to compare with a secret message; see Figure 5. In the first step, the length of the text message is multiplied by eight and divided by three, where it should be less than or equal to the image size to carry out the steganography. Here, the message is divided by three, since an image has three channels (matrices) that can be utilized for concealing the information.

To select the locations for the sake of comparing with the text binary representation, the first cell is transformed into the binary representation, and the location of bit "1" is saved in the P vector, where p1, p2, and p3 are the bit locations of the red, green and blue channel matrices, respectively. Each value of the P vector should differ from the other values. However, if the first cell's value is zero, then the location is set to the most significant bit location. Then, using the LSB technique, each encrypted message bit is compared to the bit located at P, and the result of that comparison is saved in the LSB of each matrix cell channel. For example, the first pixel values for the RGB matrices are 164, 150, and 71, respectively. Then, the values of p1, p2, and p3 are calculated using the binary representation of each matrix value.

The value of the first cell in the red channel is 164, which converted into binary is 10100100, so the location of the first bit that holds "1" is 3. The value of the first cell in the green channel is 150, which converted into binary is 10010110, so the location of the first bit that holds "1" and is not equal to p1 is 2. The value of the first cell in the blue channel is 71, which converted to binary is

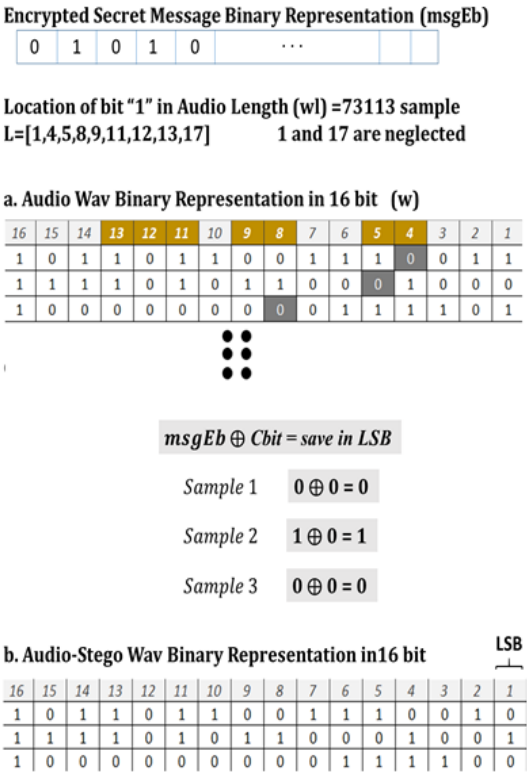

Fig. 4. Audio Steganography illustrated example for the first 3 samples

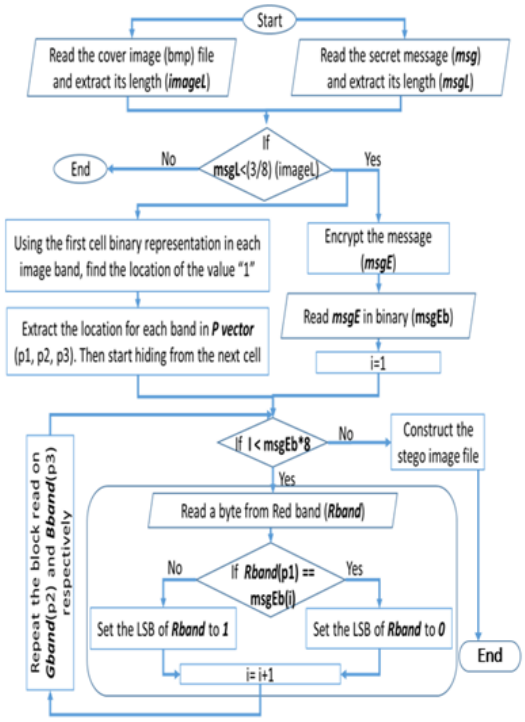

Fig. 5. Proposed Image Steganography Flowchart

1000111, so the location of the first bit that holds "1" and is not equal to p1 or p2 is 7. Location 1 is neglected since it is preserved in the LSB concealing process. After locating the P vector values, the hiding process begins from the next cell for each matrix. Each image pixel hides 3 bits from the secret message, one bit for each pixel channel. The comparison procedure is visualized in Figure 6.

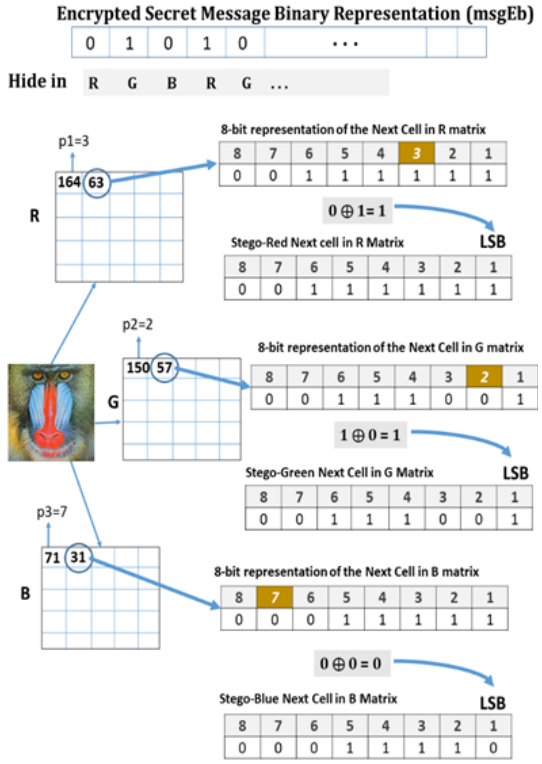

Fig. 6. Image Steganography illustrated example

4. Evaluation methods

In this section, the performance of the suggested schema is evaluated using the following objective quality measurements: the peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), mean square error (MSE), and structural similarity index metric (SSIM).

PSNR is used to calculate the quality of the steganography media (Shen *et al*., 2018). PSNR is a metric to evaluate the distortion (deformation) in steganography media, and it is measured in decibels (dB). If the PSNR value is greater than 30, then the hidden information inside the cover media is invisible to the human eye or ear (Jung & Yoo, 2009). Equation 1 is used to calculate the value:

$$PSNR = 10\log_{10}\frac{MAX^2}{MSE}, \quad (1)$$

where max is the maximum value of pixels in the media.

SNR for the wave signal is stated as the ratio of the signal power to the noise power, usually expressed in decibels (dB) (Zhou, 2004), and it is calculated using Equation 2:

$$SNR = 10\log_{10}\frac{\sum X^2}{\sum(X-Y)^2}, \quad (2)$$

Where, X represents the original audio samples, while Y represents the audio samples after applying the LSBs modifications

Log to different bases will have the same behavior since Log functions are monotonic. But using log_10 will produce more insights; the difference in the magnitude for different inputs can be noticed more easily. While a scale of 10 is being applied to bound the output to a certain range.

MSE is used to quantify the average mean square error between pixels of the cover media and steganography media; its value is computed by utilizing Equation 3 (Younus and Younus, 2019):

$$MSE = \sum_{i=1}^{M\times N}\frac{(p_i - p_i')^2}{M\times N}, \quad (3)$$

steganography media, and M*N denotes the size of the media (matrix or vector). Lower values of MSE indicate better quality of the stego-media.

SSIM is utilized to evaluate the similarity between the cover media and the steganography media (Zhou, 2004). The range of SSIM values is between 0 and 1. If the SSIM value is close to 1, it shows that the steganography media is like the cover media and holds high quality (Sultani *et al*., 2016); see Equation 4:

$$SSIM = \frac{(2\mu_X\mu_Y + C_1)\times(2\sigma_{XY}+C_2)}{(\mu_X^2+\mu_Y^2+C_1)\times(\sigma_X^2+\sigma_Y^2+C_2)}, \quad (4)$$

Where, μ_X and μ_Y are mean intensity values of the cover media (X) and steganography media (Y), σ_X and σ_Y are the media variance (standard deviation) values of the cover media and steganography media, and σ_XY is the covariance of X and Y. C1 and C2 are constants to stabilize the division.

5. Results and discussion

This paper's primary goal is to hide secret message file in image and audio cover files such that the quality is preserved and there is no evidence of data hiding. The proposed techniques are implemented using MATLAB R2019a. Starting with the proposed audio steganography technique, audio wave files are downloaded from the available MATLAB sample audio files (Mathworks, 2019). In Table 1, properties such as the duration and sampling rate of each audio file are presented. To address the effect on the quality metric values, different payloads are used. Table 2 reports the values of PSNR, SNR, MSE, and SSIM for each payload hidden in the two different audio files. As mentioned in Section 4.a, in each audio sample, only one bit is hidden. Therefore, as reported in Table 2, the maximum number of bytes that can be hidden in the Hallelujah chorus wave audio is 9139, since 73113 samples divided by 8 equals 9139.125 bytes, while the male voice wave audio file contains 913.512 samples and thus can hold up to 114144 bytes. Both audio files are one channel only (mono). The proposed schema exhibits very good performance, as shown in Table 2, MSE is very close to 0, and SSIM equals 1, also Figure 7 shows the PSNR and SNR values are greater than 30, even for higher payloads. Table 3 reports the SNR values for (Hosny *et al*., 2018) specifically (3rd LSB); those authors used 2 audio files with two channels (stereo), and the number of samples for each file were 42672 and 48558. In stereo, the number of bits is multiplied by two in the case of hiding one bit per sample. It is clearly shown that the results obtained with the proposed schema are superior to those of (Hosny *et al*., 2018).

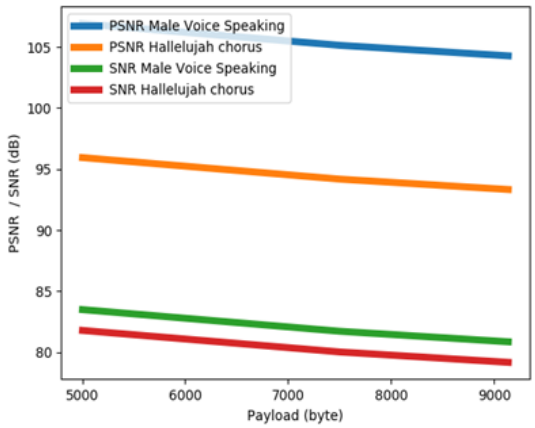

Fig. 7. Audio Samples PSNR and SNR Values

For the proposed image steganography, six images are used, as shown in Figure 8, which displays the original RGB color images used as cover media in the image steganography. These images were obtained from the SIPI image database.

Different payloads of text messages are concealed in these images and the respective qualities of the stego images' are reported in Table 4. As shown in Figure 9, these stego images are not corrupted, so they will not derive any attention. The maximum payload size that an image can hide is 98303 because 512*512*3= 786432 divided by 8 equals 98304 bytes, but since the first cell in each matrix is not used for hiding, the maximum payload is reduced to 98303 bytes.

In Figure 10, it can be noticed that the PSNR values are greater than 30 with every payload; thus, the proposed method is good at concealing the secret information inside the stego image. Moreover, the value of SSIM is close to 1, and in some cases, it is equal to 1; this result indicates that the stego image is similar to the original image and has very good quality.

Subsequently, the proposed scheme is compared with the schema presented in (Swain, 2019) using the same six images, as reported in Table 5. In (Swain, 2019), the PSNR values are less than 50, since in their approach, instead of saving one bit per byte,

Table 1. Audio wav files properties

Audio File	Sampling Rate (Hz)	Duration (s)	Bits Per Sample	# of samples
Male Voice Speaking	8000	114.1440	16	913152
Hallelujah chorus	44100	8.9249	16	73113

Table 2. The proposed Audio Steganography quality results

Audio	Measurements	Payload (byte)				
		5000	7500	9139	50000	114144
Male Voice Speaking	PSNR	106.9013	105.1278	104.2647	96.8923	93.3132
	SNR	83.4988	81.7252	80.8622	73.4898	69.9106
	MSE	$2.041\ e^{-11}$	$3.070\ e^{-11}$	$3.745\ e^{-11}$	$2.045\ e^{-10}$	$4.553\ e^{-10}$
	SSIM	1	1	1	1	1
Hallelujah chorus	PSNR	95.9391	94.1764	93.3260	-	-
	SNR	81.7942	80.0316	79.1812	-	-
	MSE	$2.547\ e^{-10}$	$3.822\ e^{-10}$	$4.649\ e^{-10}$	-	-
	SSIM	1	1	1	-	-

Table 3. SNR and Payload values (Hosny *et al*., 2018)

Audio File	# of samples	Payload (byte)	SNR (dB)
A	42672	10666 bytes	62
B	48588	12137 bytes	63.17

(a) (b) (c)

(d) (e) (f)

Fig. 8. Original images. a House , b Baboon, c Airplane, d Splash, e Sailboat, f Peppers

Table 4. The proposed Image Steganography Quality Results

Images	Measurements	Payload (byte)				
		98303	**65536**	**32768**	**16384**	**10240**
House	MSE	0.4975	0.3319	0.1661	0.0831	0.0519
	PSNR	51.1630	52.9204	55.9276	58.937	60.979
	SSIM	0.99	0.99	0.99	0.99	0.99
Baboon	MSE	0.4976	0.3313	0.1656	0.0828	0.0517
	PSNR	51.1622	52.9283	55.9412	58.9513	60.994
	SSIM	0.99	0.99	0.99	1	1
Airplane	MSE	0.497	0.3324	0.1663	0.083	0.0519
	PSNR	51.1608	52.9142	55.9226	58.9407	60.9753
	SSIM	0.99	0.99	0.99	0.99	0.99
Splash	MSE	0.496	0.331	0.1654	0.0824	0.0516
	PSNR	51.173	52.9315	55.9458	58.9695	61.001
	SSIM	0.99	0.99	0.99	0.99	0.99
Sailboat	MSE	0.496	0.3310	0.165	0.0825	0.0516
	PSNR	51.1746	52.9326	55.945	58.963	61.005
	SSIM	0.99	0.99	0.99	0.99	1
Pepper	MSE	0.4962	0.3310	0.1654	0.0825	0.0516
	PSNR	51.174	52.932	55.9454	58.9638	61.005
	SSIM	0.99	0.99	0.99	1	1

(a) (b) (c)

(d) (e) (f)

Fig. 9. Stego-images with payload of 10240 bytes.

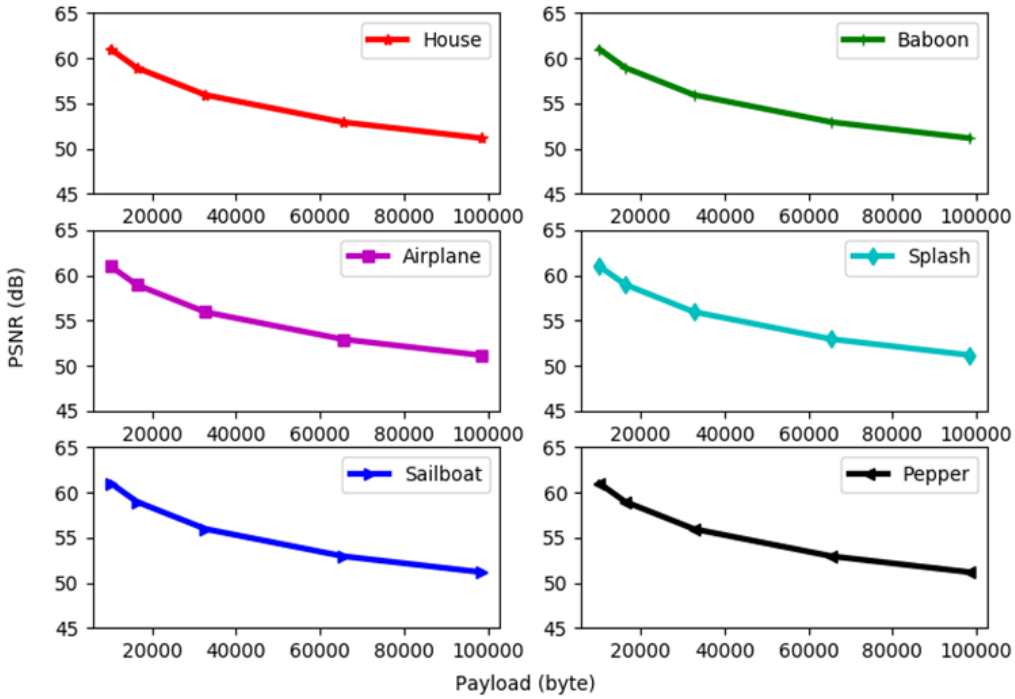

Fig. 10. Proposed Image Steganography's PSNR Values for different Payloads.

Table 5. PSNR Quality results with payload of 87,500 bytes (QVD+LSB) Swain (2019)

Images 512×512×3	PSNR (dB)
House	32.94
Baboon	32.41
Airplane	32.74
Splash	33.13
Boat	33.14
Peppers	33.21

they use approximately 4 bits per byte. This approach decreases the quality, but it is still greater than 30 dB. From these two tables, it can be concluded that the quality and performance of the proposed schema are much better than those of the schema presented in (Swain, 2019).

6. Conclusions

In this paper, a modification of the LSB technique is proposed by saving the comparison result in the cover media LSB. The comparison is made between each bit of the secret binary message and a mask bit retrieved using the proposed selective method. The proposed method is considered an efficient method for hiding the data since the extraction differs from that in the traditional LSB method. The designed steganography schema can embed secret message bits in both cover images and audio files. The objective test showed that the stego-cover generated from the proposed schemas cannot be distinguished from the original cover file. Some of the limitations are that the quality of the stego-cover depends on the sizes of both the cover media and the secret message. The other limitation is that the proposed schema is designed such that each byte of the cover media hides only a single bit of the text message. Those limitations can be addressed using compression and transformation. The secret message size can be reduced before the embedding process, and using some additional information through transformation. The embedding can be increased by hiding more than one bit per audio sample and 3 bits per image pixel.

References

AbdelWahab, O. F., Hussein, A. I., Hamed, H. F., Kelash, H. M., Khalaf, A. A. & Ali, H. M. (2019). Hiding data in images using steganography techniques with compression algorithms. *Telkomnika*, **17**: 1168-1175.

Ali, A. H. & George, L. (2016). A review on audio steganography techniques. *Research Journal of Applied Sciences, Engineering and Technology,* **12**: 154-162.

Arora, S. K. (2018). *Audio Steganography: The art of hiding secrets within earshot (part 1 of 2)* [Online]. https://medium.com. Available: https://medium.com/@sumit.arora/audio-steganography-the-art-of-hiding-secrets-within-earshot-part-1-of-2-6a3bbd706e15 [Accessed 2019].

Bhardwaj, R. & Sharma, V. (2016). Image steganography based on complemented message and inverted bit LSB substitution. *Procedia Computer Science,* **93**:832-838.

Dhannoon, B. N. (2013). An Indirect MSB Data Hiding Technique. *Life Science Journal, 10.*

Hmood, D. N., Khudhiar, K. A. & Altaei, M. S. (2012). A new steganographic method for embedded image in audio file. *International Journal of Computer Science and Security (IJCSS)*, **6**: 135-141.

Hosny, A. A., Murtada, W. A. & Youssef, M. I (2018). Improving LSB Audio Steganography Using Simulated Annealing for Satellite Telemetry. (2018). International Computer Engineering Conference (ICENCO), IEEE: 11-16.

Islam, M. R., Siddiqa, A., Uddin, M. P., Mandal, A. K. & Hossain, M. D. (2014). An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography. International Conference on Informatics, Electronics & Vision (ICIEV), IEEE: 1-6.

Jose, M. (2014). Hiding image in image using LSB insertion method with improved security and quality. *International Journal of Science and Research,* **3**: 2281-2284.

Jung, K.-H. & Yoo, K.-Y. (2009). Improved exploiting modification direction method by modulus operation. *International Journal of Signal processing, Image processing and pattern,* **2**: 79-87.

Latef, S., Hassan, N. A. & Dhannoon, B. N. (2011). Color image encryption using random password seed and linear feed back shift register. *Al-Nahrain Journal of Science,* **14**: 186-192.

Lin, C.F., Wang, R.Z., & Lin, J.C. (2001) Image hiding by optimal lsb substitution and genetic algorithm. *Pattern Recognition* **34**: 671–683.

Mahmood, M. B. & Dhannoon, B. N. (2017). Information hiding by using Developed M8PAM. *International Journal of Advanced Research in Computer and Communication Engineering*, **6**:7-11.

Maniriho, P. & Ahmad, T. (2019). Information hiding scheme for digital images using difference expansion and modulus function. *Journal of King Saud University-Computer and Information Sciences,* **31**:335-347.

Mathworks. (2019). *Sample Audio Files - Matlab & Simulink* [Online]. Mathworks. Available: https://www.mathworks.com/help/audio/ug/sample-audio-files.html.

Pathak, P., Chattopadhyay, A. K. & Nag, A. (2014). A new audio steganography scheme based on location selection with enhanced security. First International Conference on Automation, Control, Energy and Systems (ACES), 2014. IEEE: 1-4.

Parvez, M. T. & Gutub, A. (2011). Vibrant Color Image Steganography using channel differences and secret data distribution. *Kuwait Journal of Science and Engineering.* **38**: 127-142.

Rajput, S. P., Adhiya, K. P. & Patnaik, G. K. (2017). An Efficient Audio Steganography Technique to Hide Text in Audio. International Conference on Computing, Communication, Control and Automation (ICCUBEA), 2017. IEEE: 1-6.

Shen, S.-Y., Huang, L.-H. & Yu, S.-S. (2018). A novel adaptive data hiding based on improved EMD and interpolation. *Multimedia Tools and Applications,* **77**: 12563-12579.

SIPI Image Database [Online]. Available: http://sipi.usc.edu/

Sultani, Z., Al-Tuma, R. F. & Wefel, S. (2016). Color Reduction in an Authenticate Live 3D Point Cloud Video Streaming System. *Computers*, 5 :17.

Swain, G. (2019). Very High Capacity Image Steganography Technique Using Quotient Value Differencing and LSB Substitution. *Arabian Journal for Science and Engineering,* **44**:2995-3004.

Taleby Ahvanooey, M., LI, Q., Hou, J., Rajput, A. R. & Chen, Y. (2019). Modern text hiding, text steganalysis, and applications: a comparative analysis. *Entropy*, 21: 355.

Tanwar, R., Sharma, B. & Malhotra, S. (2014). A robust substitution technique to implement audio steganography. International Conference on Reliability Optimization and Information Technology (ICROIT), IEEE: 290-293.

Younus, Z. S. & Younus, G. T. (2019). Video Steganography Using Knight Tour Algorithm and LSB Method for Encrypted Data. *Journal of Intelligent Systems*. 29(**1**): 1216–1225

Zhou, W.(2004). Image quality assessment: from error measurement to structural similarity. *IEEE transactions on image processing,* **13**: 600-613.

Submitted: 09/01/2020
Revised: 17/10/2020
Accepted: 02/12/2020
DOI: 10.48129/kjs.v48i4.8992