IPS Journal of Physical Sciences
IPS J Phys Sci, 1(1): 1-5 (2022)
DOI: https://doi.org/10.54117/ijps.v1i1.1

A Modified Least Significant Bit Replacement: Steganography Method for Handling Random Noise Effect

Mohammed Usman[1] and Badamasi Yusuf[2*]

[1]Department of Computer Science, Modibbo Adama University (MAU), Yola.
[2]Department of Science and Technology, Ministry of Education, Science and Technology, Dutse, Jigawa State.

*Corresponding author: yusufbadamasi@hotmail.com; Phone: +234(0)8032489331

Abstract

Steganography is one of the security measures employed at file level to cover information in a carrier. The goal of steganography is to send a confidential message over a network in a way that intruders will not notice it. In steganography, the message is wrapped in an innocent carrier such as image, audio or video file. There are always bits tempering in the process and this changes the looks and appearance of the carrier. The more secret message is embedded in any cover file, the more random noise occurs. Secret message bits when embedded drastically modify the Red Green and Blue (RGB) components' bits of the carrier, hence, the statistical properties and physical appearance of the carrier change and this draws the attention of intruders to suspect that confidential data is hidden there. This research introduced an improved method of least significant bit replacement to cover secret data using 24 bits bitmap image to handle random noise efficiently so that the Human Visual System (HVS) of intruders will not notice the secret communication. The research reviewed some previous related researches that aimed to reduce the effect of random noise and research gap is identified. The research implemented the new Modified Least Significant Bit Replacement (M-LSBR) method to fill the identified research gap. Five (5) experiments were conducted with 5 (five) varying dimension RGB images and the result gathered that the PSNR value, image quality and message capacity of the new method is better than those achieved by the previous methods, hence, the research gap is filled. Finally, conclusion was drawn and recommendation for future research was suggested.

Keywords: *Steganography, Cover, Stego, M-LSBR, PSNR, LSB, MSB*

Article History
Received: 18 Jan 2022
Accepted: 21 Feb 2022
Published: 22 Feb 2022

How to cite this paper: Usman, M. and Yusuf, B. (2022). A Modified Least Significant Bit Replacement: Steganography Method for Handling Random Noise Effect. *IPS Journal of Physical Sciences*, 1(1), 1–5. https://doi.org/10.54117/ijps.v1i1.1.

1. Introduction

Unauthorized access to data is the common threats in a networked system that may cause loss of confidentiality, integrity, and availability of the information technology assets (Kaur, Inderjeet & Duhan, 2017). Steganography is one of the techniques used to safeguard data/information against unauthorized access. Steganography is a method of hiding confidential information in a cover file (Alam, 2016). The cover file may be text file, digital image, audio file or video file. The message wrapped cover, also known as stego is securely sent to a destination over the internet with low chance of intruder noticing it. Steganography is a step further to cryptography which only scrambles the information into incomprehensible form to unauthorized person (Laskar & Hemachandran, 2019). Steganography on the other hand hides the entire existence of the message and therefore it is considered more secure approach (Mortazavian, Jahangiri & Fatemizadeh, 2016). The problem that raised concern in image steganography method is the effect of random noise which is added in the cover during the hiding process and this cause the stego image to degrade in quality (Juneja & Sandhu, 2013). This research is aimed at achieving a detection free technique that efficiently reduces the effect of random noise in stego image. In order to achieve this aim, the conventional Least Significant Bit Replacement method is improved and a 24 bit bitmap image format used as cover. The research is intended to fill the research gaps identified in previous relevant literatures.

2. Reviewed Literatures

Salluri (2020) proposed a method that slightly modified the technique of data embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage (Fig. 1). The research uses newer modules instead of older ones and provides a better Graphical User Interface for easy understanding and user-friendly experience.

Ansari *et al*. (2020) presents an algorithm called GSA that works for cover images of multiple formats that is designed to apply uniform security policies across all image formats as shown in figure 2. This method can adaptively select the most suitable cover image based on data length, network bandwidth and allowable distortions on the abstract concept of image components that can be adapted for JPEG, Bitmap, TIFF and PNG cover images.

The Conventional Least Significant Bit (LSB) replacement method of steganography proposed by Champakamala, Padmini and Radhika (2009) is a common and simple approach to embed information in an image file. The method used 640 X 525 sized RGB image as cover to replace the Least Significant Bits (LSBs) of the cover image (C) with the bits of secret message (M) aimed at reducing noise in the stego-image. Every pixel in 24-bit bitmap image consists of Red, Green and Blue (RGB) colour components and each colour component consists of eight (8) bits. This method is easiest to implement but it is characterized by Low PSNR of 19.9987 dB and low quality

image that draw intruder's attention to easily sense a secret message is hidden in the stego image. The method also accommodates only 15 bytes or less of message.

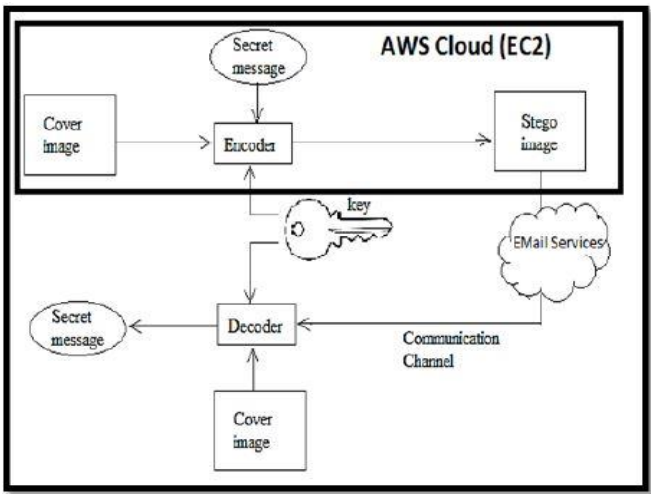


Figure 1: AWS Cloud Steganography Architecture (Salluri, 2020).

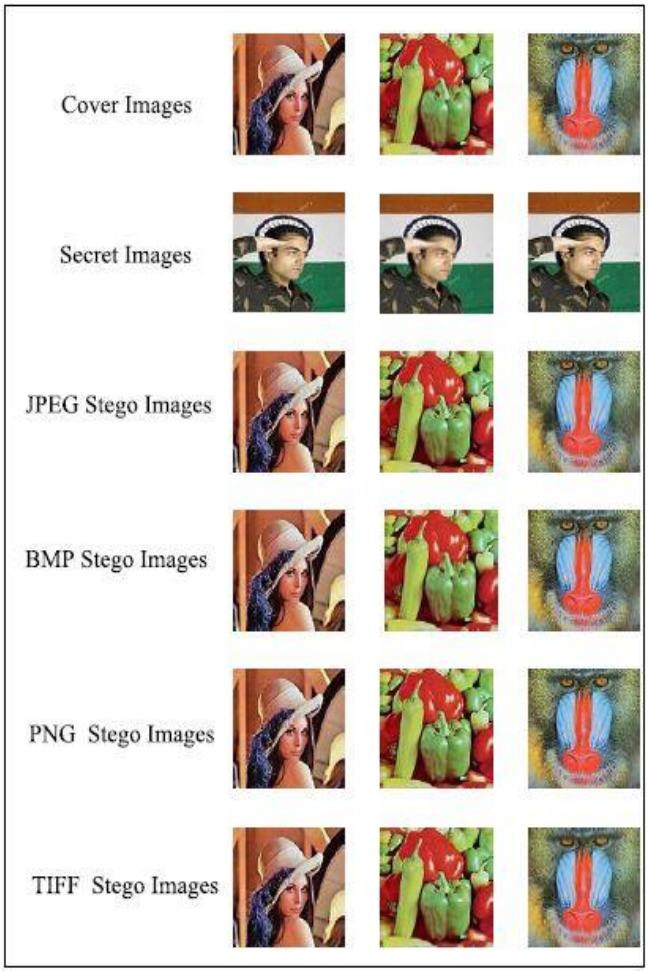


Figure 2: Varying Image Format (Ansari *et al.*, 2020).

Korothan, Kishor and Butey (2016) proposed a technique that involves hiding secret in an RGB image. In this technique, embedding is done through replacing the noisy bit of the image with bits of the secret message. From Human Visual System angle, the stego image looks a bit distorted thereby drawing intruder's attention. The PSNR value achieved by this method is 41.131 dB and the method capacity depends on the amount of noisy bits found in the cover to be replaced with message.

Emam, Ali and Omara (2016) proposed a random pixel replacement method to hide bits of the secret message. This method pays attention to hiding a message only in blue and green components of the cover image pixels, neglecting red colour component. This method achieved a high PSNR of 40.434 dB however; the appearance of the stego-image after embedding considerably changes. The method also has a good message hiding capacity as it can wrap up to 50 bytes of message length.

Ali and Saad (2019) proposed Secret Message Matching (SMM) method if the embedded bit does not match the LSB of the cover image, then the pixel value of the corresponding pixel is randomly added by ±1. The original image and the stego image looks identical to the Human Visual System and this help reduces suspicion of secret communication. The method achieved 40.1132 dB PSNR but designed to hide only 20 bytes long message.

Abdul-Sada (2017) method is based on LSB-3. The paper exploits the third Least Significant Bit instead of first or second Least Significant Bit and it has achieved great capacity of hiding up to 45 bytes of message and 30.087 dB of PSNR. The original and stego looks a bit different as noise is slightly noticeable to the human eye.

Manikandan et al (2021) came up with a combined framework of both encryption and steganography where only the authorized person can send the secret image to the receiver. In the first stage, an image steganography system is processed using confidential medical X-ray images which are hidden under the cover images. On the receiver side, the same process of decryption happens, followed by the two-level verification using email authentication and OTP generation using Pega. This ensures that only the authorized receiver can receive and view the secret image sent by the sender. Figure 3 has richly demonstrated this approach.

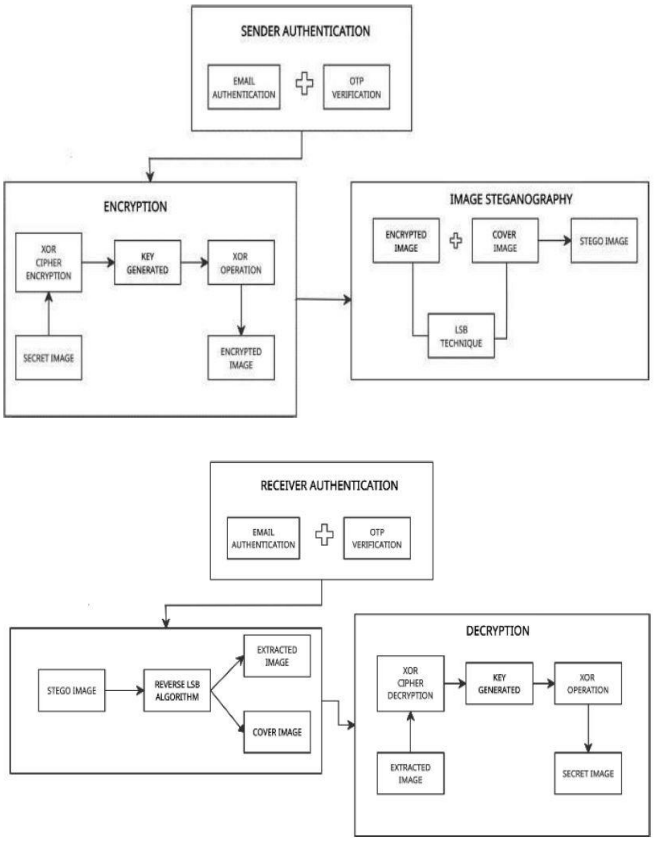


Figure 3: Combined Approach (Manikandan *et al.*, 2021).

Identified Research Gap

Some of the visited literatures achieved low image quality after hiding message, low Peak Signal to Noise Ratio value or low message holding capacity. This research has come to fill these gaps found in these previous researches.

3. Materials and Methods

Materials

1. Five varying dimension 24 bit bitmap images
2. Matlab software
3. Microsoft Visual studio v.2010
4. ASCII converter

Method

Modified Least Significant Bit Replacement (M-LSBR) method takes the following stages:

1. Determine the size of the secret message with that of the cover image such that size of the secret message should be less than the size of cover image.
2. Convert the pixels of the 24-bits bitmap image (cover) into binary bytes using bit and divide it into RGB parts. Each byte represents one of the three components (R,G,B)
3. Encode the secret message into binary using ASCII converter.
4. Embed first two MSBs of the secret message (M) into the last two bits of R component of the pixel, followed by second two bits in the G component then third two bits of the secret message in B component.
5. The operation on M continues from left to right MSBs for the remaining M's bits by inserting them in the subsequent pixels in a loop fashion until all the M's bits are fully embedded.

Practical of M-LSBR

The method converts the message characters into ASCII binary representations. Table 1 indicates how a secret message 'HELLO' was encoded and hidden in sixteen (16) pixels of a 24 bit bitmap image.

Table 1: Bits Hiding in Pixels

Pixel No	R	G	B	
1	10010001	10010010	10010010	1st character embedded
2	11100111	11100100	11100111	
3	10001100	10001100	10001110	
4	11001100	11001100	11001100	
5	11110011	11110001	11110011	2nd character embedded
6	10011010	10011010	10011000	
7	10000101	10000111	10000111	
8	10011000	10011001	10011000	
9	10000000	10000000	10000001	3rd character embedded
10	10101000	10101010	10101010	
11	11001100	11001111	11001100	
12	10001000	10001000	10001000	
13	10000001	10000011	10000011	4th character embedded
14	11001100	11001100	11001100	
15	11110000	11110000	11110011	
16	11001000	11001010	11001010	

Novelty of the Proposed Method

This research is an innovation of modifying the commonly known Least Significant Bit Replacement (LSBR) steganography method.

The method replaces the least bits of only one component out of the three components (Red, Green and Blue) of every pixel in a 24 bits bitmap image as shown in figure 4, achieving better image quality instead of following the conventional style (adopted by most of the previous methods) that replaces the least bits of all the three components in every pixel as shown in figure 5 which result in less image quality.

Figure 4: Modifying LSBR (Proposed Method).

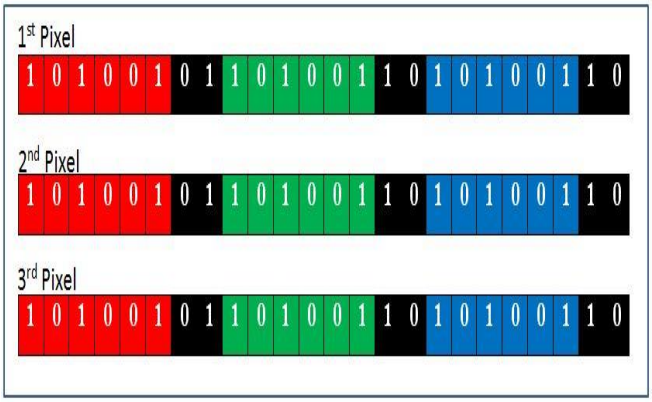


Figure 5: Conventional LSBR Method.

Experimentations

Experiments were carried out using Matlab software and observation of the image quality using Human Visual System (HVS) were the tools used in the experimentations. The factors considered in assessing the effectiveness and efficiency of the proposed method during the experiments were:

1. Image Quality
2. Peak Signal to Noise Ratio (PSNR) value and
3. Message Capacity

Peak Signal to Noise Ratio (PSNR): is a visual quality estimator for stego images. It is used to measure the perceptible quality of the modified Steganography image in decibels (dB). A high value for PSNR indicates higher quality of an image.

The PSNR is calculated as:

$PSNR = 20 \log (max_i) - 10 \log (MSE)$

Mean Square Error (MSE): is an estimate for error between the original cover image and the output stego (reconstructed) images.

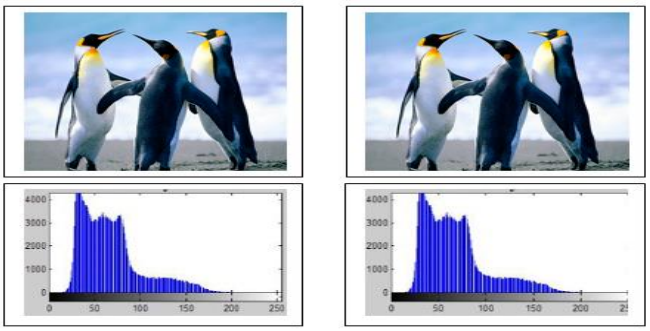
4. Results and Discussion

This research tries to compare the results for of some of the existing works and that of the proposed method (M-LBSR) in order to understand whether the proposed method filled the identified gap found in the previous works or otherwise.

The Conventional Least Significant Bit (LSB) replacement method used by Champakamala, Padmini and Radhika (2009) as seen in the literature review section is characterized with low PSNR value (9.9987 dB only) and low image quality image as shown in figure 6. The method could accommodate only 15 bytes or less of message.

In comparison, the method proposed by this research shows an image hiding a secret message of 52 bytes size in its first experiment with no difference in the appearance of the two images (before and after hiding) as depicted in figure 7 and achieved higher PSNR value (51.8283 dB) when analysed in a Matlab.

Figure 6: Cover image and stego image (Champakamala, Padmini & Radhika, 2009).



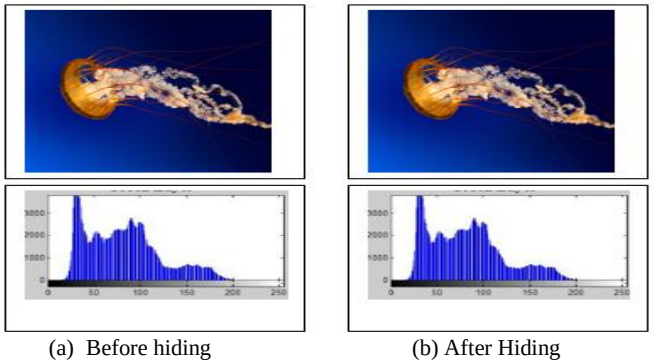
(a) Before hiding (b) After Hiding

Figure 7: Experiment 1 (Proposed Method).

The noisy bit replacement technique brought by Korothan, Kishor and Butey (2016) rendered the stego image distorted thereby drawing intruder's attention. The result of this method shows PSNR of 41.131 dB and message capacity of 43 bytes. Figure 8 displayed how the image is distorted when secret information is hidden in it.

When the 2nd experiment was done with the proposed method, the image hides a message of 53 bytes and there is no difference in the appearance of both the cover image and the stego image as shown in figure 9 and the PSNR achieved was 53.0805 dB.

Figure 8: Cover image and stego image (Korothan, Kishor & Butey, 2016)



(a) Before hiding (b) After Hiding

Figure 9: Experiment 2 (Proposed Method).

The random pixel replacement method by Emam, Ali and Omara (2016) hides bits of secret message in blue and green components of the cover image pixels. The method achieved high PSNR of 40.434 dB however; the appearance of the stego-image after embedding considerably changes as shown in figure 10. The method also has good message hiding capacity as it can wrap up to 50 bytes of message length.

The 3rd experimental result of the proposed method is compared with the Emam, Ali and Omara (2016) method discussed in the literature review section. The proposed method shows no difference in appearance of both original and after hiding image as shown in figure 11. The method is capable of holding 51 bytes message size and achieved 54.8254 dB PSNR value, hence it is more effective.

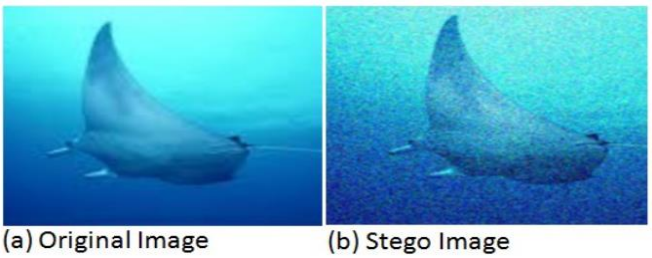
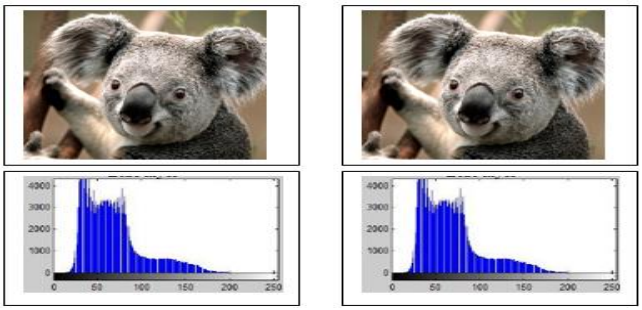


Figure 10: Cover image and stego image (Emam Ali & Omara, 2016).



(a) Before hiding (b) After Hiding

Figure 11: Experiment 3 (Proposed Method).

The Secret Message Matching (SMM) method by Ali and Saad (2019) achieved 40.1132 dB PSNR and is limited to hide only 20 bytes long message with relatively higher image quality that one may not notice any difference between the original and stego image as shown in figure 12. The result of the 4th experiment carried out by the method proposed by this research is compared with the Ali and Saad (2019) method which yielded almost the same outcome when it comes to image quality as shown in figure 13. However, the message capacity of the Modified Least Bit Replacement method of this research is higher than that of Ali and Saad (2019) method.

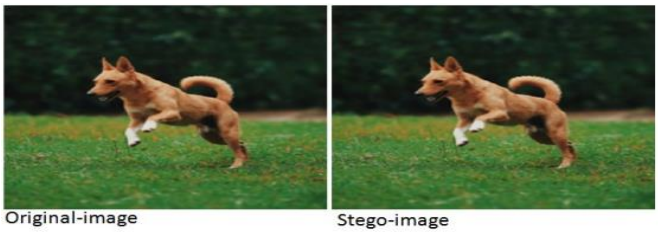
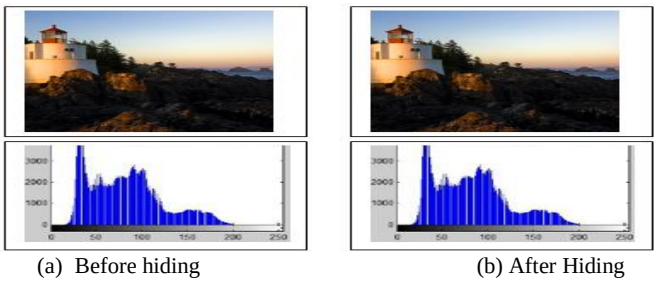


Figure 12: Cover image and stego image (Ali & Saad, 2019).



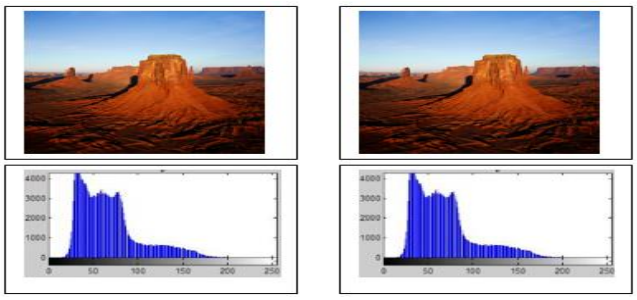
(a) Before hiding (b) After Hiding

Figure 13: Experiment 4 (Proposed Method).

Third Least Significant Bit Replacement method by Abdul-Sada (2017) achieved great capacity of hiding up to 45 bytes of message and 30.087 dB of PSNR. The original and stego looks a bit different as noise is noticeable (Fig. 14). The 5th experiment carried out with the Modified Least Significant Bit Replacement proposed by this research indicates that image containing the message remain the same in appearance and the PSNR value achieved is 51.8436 dB (Fig. 15).

(a) Original Image (b) Stego-Image

Figure 14: Original and Stego image (Abdul-Sada, 2017).



(a) Before hiding (b) After Hiding

Figure 15: Experiment 5 (Proposed method).

The fifth experiment indicates how the cover image Figure 10(a) was used to embed a secret message of 53 bytes size. Figure 10(b) indicates the stego image containing the secret message but no difference in the appearance and statistical property of the both the cover image and the stego image. The Human Visual System (HVS) couldn't distinguish between the stego image and original image. The histograms of both original and modified image remain the same. Tables 2 and 3 are summaries of results from previous studies and proposed methods.

Table 2: Summary of Results (Previous Researches)

S/N	Literature	Technique Used	PSNR (in dB)	Image quality	Message capacity (bytes)
1.	Champakamala *et al* (2009)	Conventional LSB	19.9987	Low	15
2.	Korothan *et al* (2016)	Noisy bit substitution	41.131	Low	43
3.	Emam *et al* (2016)	Random substitution	41.48	Low	51
4.	Ali and Saad (2019)	Matching method	40.1132	High	20
5.	Abdul-Sada (2017)	LSB -1,2 replacement	39.087	Low	45

Table 3: Summary of Results of the Proposed Method (M-LSB)

S/N	Cover image	Capacity(bytes)	PSNR (in dB)	Image quality
1.	**Jellyfish**	53	51.8283	High
2.	**Penguins**	52	53.0805	High
3.	**Koala**	51	54.8254	High
4.	**Lighthouse**	52	51.8436	High
5.	**Desert**	53	51.8283	High

5. Conclusion

The proposed method was compared with the LSB benchmarking method for hiding the secret message which hide the secret message directly in the least two significant bits of the image pixels. The proposed and the LSB hiding methods were implemented to hide varying size secret message in five (5) different Bmp images.

The results of the proposed and LSB hiding methods were discussed and analyzed based on the Peak Signal to noise ratio metric. It is concluded that the proposed method is more efficient, simple, appropriate and accurate than the reviewed methods because it embed uniformly, no over exploitation of one particular component neglecting the other. Thus, each component gives equal contribution of intensity when hiding data; hence the change in the image resolution is quite low and this makes the secret message more secure.

6. Recommendations and Future Work

1. Steganography should be seen as a complement to cryptography and not its replacement. Exploring how to use the combined techniques in future research will be a welcomed idea. Implementation of Crypto-Stego method using M-LSBR model is expected to guarantee better and effective information security. Therefore research should try exploring more than steganography alone.
2. The M-LSBR method can also be implemented in the future research using other forms of cover file other than image. The use of audio file, video file or text file as cover media can also be employed.
3. Enhancing the proposed method to make the capacity higher while keeping the same or higher PSNR value means more quality against intrusion.

References

Abdul-Sada, A.I. (2017). Information hiding using third Least Significant Bit (LSB-3). *J. Basrah Researches (Sciences)*, 33(4), 81-88.

Alam, I.F. (2016). An investigation into encrypted message hiding through images using SB. *International Journal of EST*, 6(33), 34-40.

Ali, A.A., &, Saad, A.S. (2019). New image steganography method by matching secret Message with pixels of cover image (SMM). *International Journal of Computer Science Engineering and Information Technology Research*, 3(2), 1-10.

Ansari, A.S., Mohammadi, M.S., & Parvez, M.T. (2020). A Multiple-format steganography algorithm for color images. *IEEE Access*, 8(3): 83926-83939.

Champakamala, B.S, Padmini, K., & Radhika, D. K. (2009). Least Significant Bit algorithm for image steganography. *International Journal of Advanced Computer Technology*, 3(4), 34-38.

Emam, M.M., Ali, A.A., & Omara, F.A. (2016). An Improved Image Steganography Method Based on LSB Technique with Random Pixel Selection. *International Journal of Advanced Computer Science and Applications*, 7(3), 361-366.

Juneja, M., & Sandhu, P.S. (2013). A New Approach for Information security using an Improved Steganography Technique. *Journal of Info. Pro. Systems*, 9(3), 405-424.

Kaur, J., Inderjeet, A., & Duhan, M. (2017). An analysis of steganographic techniques. *International Journal of Information Technology and Knowledge Mngt*., 2 (1),191-194.

Korothan, J., Kishor, S. & Butey, P. (2016). De-Noise Steganography by Enhancing the Cover Image: A Multi-Level Security Approach. The *International Arab Journal of Information Technology*, 13(6), 851-857.

Laskar, S.A., & Hemachandran, K. (2019). Steganography based on random pixel selection for efficient data hiding. *International Journal of Computer Engineering and Technology*, 4(2), 31-44.

Manikandan, T., Muruganandham, A., Babuji, R., Nandalal, V. & Iqbal, M. (2021). Secure E-Health using Images Steganography. *Journal of Physics: Conference Series*, 21(1), 1-7.

Mortazavian, P., Jahangiri, M., & Fatemizadeh, E. (2016). Low degradation steganography model for data hiding in medical image. International *Journal of Computer Science and Information Technology*, 4(2), 234-240.

Salluri, S.C. (2020). Image steganography and sending private data through email using cloud computing. *International Journal of Progressive Research in Science and Engineering*, 1(8), 92-94.

• *Thank you for publishing with us.*