A Technique for Increasing Payload Capacity of RGB Images Steganography based on Mod Factor and Segmentation

Mahmoud S. Abdelbar
Department of Mathematics Faculty of Science
South Valley University
Qena, Egypt

Abdelmgeid A. Ali
Faculty of Computers and Information, Minia University Al Minia, Egypt

M. Hasabala
Department of Mathematics Faculty of Science
South Valley University
Qena, Egypt

ABSTRACT
With the evolution of computer technologies and the internet, the security of information has become the most crucial challenges in communication to protect information, Steganography is one of the data hiding techniques which embed secret information in a media such as images, sounds, videos, and etc. in a way that it is not detectable by others. Focusing on the image, there are many methods which apply image steganography, with the increasing rate of unauthorized access and attacks, security of confidential data has an utmost importance. Steganography hides the confidential data in some cover image such that the existences of the data, which do not arouse suspicion regarding the communication taking place between two parties. In this paper, we proposed a technique to hide the secret message inside the cover image based on segmented the blue layer from the cover image, using initial threshold value, and we can change the value of the threshold according to the size of the secret message. Finally convert the secret message and embedding it in the segmented area. The results showed that the proposed technique gives better results of higher PSNR lower MSE.

General Terms
Data Hiding, Image Steganography

Keywords
Steganography, least-significant-bit, modulus factor, segmentation

1. INTRODUCTION
Nowadays, the internet has become the foremost popular communication media for message transmission in several places of the planet [1]. Two schemes are needed to protect secret messages from being captured during transmission. One is encryption where the key information is encoded in another form by employing a secret key before sending, which may only be decoded with secret keys. Another way is steganography which may be a technique of hiding secret information into a canopy media or carrier.

If the cover media may be a digital image, it's called cover image and therefore the cover image with hidden data is named stego-image. Stenographic technique are often utilized in military, commercial, anti-criminal then on. There are various stenographic techniques available where a digital image is employed as a carrier. The foremost common and simplest method is least-significant-bit (LSB) substitution, where the LSB position of every pixel of the cover image is replaced by a little bit of secret data. We can say that today's digital technology [2], digital content is often shared quickly and simply on internet networks. With the increasingly faster and easier digital content spreads, copy and digital content distribution can cause illegal acts in internet publics. The copyright holders of digital content are basically concerned with the copyright protection technology. Some experts have provided data hiding techniques to insert secrets, copyright information, or trademark into digital content to guard or secure the copyright, and only slightly modify the first content. Broadly speaking, there are two methods of securing data: they're cryptography and steganography. The difference between cryptography and steganography is that in cryptography, the media with inserted information will change, while in steganography, the media with inserted information won't have any changes. In cryptography [3], suspicion from the third party will arise because the media that are inserted are going to be very different from the first, although the third party isn't actually conscious of the inserted information. Meanwhile, in steganography, with naked eyes the media that has and has not inserted with information will look an equivalent, so it'll not arise suspicions from the third party or it'll be very difficult to differentiate them. The concept of steganography has been around since Roman era, usually administered by military to send secret messages. Messages sent by tattooing it on the slave's scalp that previously shaved, after the hair grows, the slaves were then sent to allies. To read the messages, the allies shaved the slave's head.

Steganography may be a technique which want to transmit a secret message under the cover of digital media like images [4]. It first pays far more attention on embedding payload instead of robustness against intentional attacks compared with watermark which is employed to guard the copyright. Moreover, imperceptibility, which is that the second requirement, is carefully considered within the Steganography algorithms. Thus, an efficient Steganography scheme shouldn't cause any perceptible distortion and need to achieve high capacity.

Today, the media carried steganography include (image, video, audio, and text) commonly used media such as image or also called as Cover-Image. Cover Image inserted with secret messages is named Stego-Image. Chung et al. [5] Steganography and cryptography are often combined into one which within the insertion process before the message is inserted into the media the cryptography process is performed first. Next, the encrypted messages are going to be inserted using steganography. The steganography and cryptography process are performed to reopen the messages.

According to Bohme [6], the steganography techniques within

the image media are often divided into four sections:

(a) Spatial Domain techniques manipulate or alter the image by manipulating the pixels within the image. In simple spatial domain, we are directly facing the image matrix, while the matching images is that the lossless type.

(b) Transform / Domain Frequency with the domain transform method, first turn the image into a distribution. The signal changing from time domain to the frequency domain is employing a mathematical operator called transformation. A number of the transformations are Fourier series, Fourier transformation, Laplace transform and z transform.

(c) Spread Spectrum Steganography the essential concept of Spread Spectrum Steganography is hiding the knowledge within the noise added to the digital images. Noise is attached to the image acquisition process and if saved within the low level are going to be difficult to be recognized by human eye and also not susceptible to attack without access to the first image.

(d) Model Based Steganography Steganographic algorithm supported the statistical characters of the cover is Model Based Steganography, which inserts the knowledge without changing the contents of the property.

These carriers might be images, audio files, video files, or text files, but digital images are the foremost common because of these reasons: [7]. Natural image data are often modified slightly without resulting in visible artifacts (If the color of a couple of pixels is shifted slightly in one direction or another, it's likely to travel unnoticed). These sorts of files on the web are inherently of anonymous nature, and It contains a big amount of knowledge [8], enabling high secret communication rates.

The objectives of Steganography [9] are :

Capacity: mention the quantity of data which will be hidden within the cover medium.

Security: associate with the eavesdropper's inability to detect hidden information.

Robustness: be that of the amount of modification the stego medium can withstand before an adversary can destroy the hidden information.

Imperceptibility: mention the perceptual difference between the cover and original signal.

Steganographic System Evaluation

In order to make a decision of which steganography technique is better than others, an evaluation scheme for steganographic systems is needed. The amount of hidden information and the difficulty of detection the stego files are the two most important aspects of any steganographic system [10]. So, the measures of steganographic capacity and undetectability are needed in order to evaluate the efficiency of steganographic systems [11].

(a) Evaluation of Steganographic Capacity (Payload)

Evaluating the capacity of the system means what proportion information of the steganography technique is often embedded. It's important to work out what percentage bits a steganographic system are often embedded as compared to the opposite methods. So, the utmost number of bits which will be hidden must be determined.

(b) Evaluation of Imperceptibility

The methods which will be needed to evaluate the imperceptibility of steganographic systems are different from one system to a different counting on the sort of canopy file used for information hiding.

Two sorts of perceptibility are often distinguished and evaluated in signal processing systems, namely "fidelity and quality". Fidelity means the perceptual similarity between signals before and after processing. However, quality is an absolute measure of the goodness of a sign [11]. There are some parameters which are required to evaluate the steganography technique, which are: the height signal-to-noise (PSNR) and therefore the Mean Square Error (MSE). PSNR is one of the metrics to work out the degradation within the embedded image with reference to the host image. It wants to measure the stego image quality in dB, values over 36 dB in PSNR are acceptable in terms of degradation, which suggests no significant degradation is observed by human eye [12].

MSE measures the difference between the cover image and therefore the stego image [6]. High PSNR value indicates high security because it indicates minimum difference between the first and stego values. So, nobody can suspect the hidden information [13]. PSNR and MSE are defined as shown in equation 1 and 2 [14]:

$$\mathrm{MSE} = \left(\frac{1}{\mathrm{MN}}\right)\sum_{i=1}^{M}\ \sum_{j=1}^{N}\left(X_{ij} - X'_{ij}\right)^2 \quad (1)$$

$$\mathrm{PSNR} = 10\log_{10}\frac{I^2}{\mathrm{MSE}} \quad (2)$$

Where X is the i^{th} row and the j^{th} column pixel in the original (cover) image, X_{ij} is the i^{th} row and the j^{th} column pixel in the reconstructed (stego) image, M and N are the height and the width of the image, I is the dynamic range of pixel values, or the maximum value that a pixel can be taken, for 8-bit images; I=255. Thus, the best image quality can be found when the MSE value is very small or going to be zero since the difference between the original and reconstructed image is negligible.

2. RELATED WORK

A computer image is an array of square pixels (picture elements) arranged in columns and rows. Today digital images are most generally used for hiding of secret messages. The sector that uses image to cover a message is called the image steganography. Payload capacity with good image quality of stego image is extremely important aspect. There are many attempts to cover the message within the images . Some of them are mentioned below:

In [15] a picture steganography the technique has been presented. This system used the logical AND operation on both selected pixel intensity and selected pixel position. Firstly, both pixel intensity and pixel position are converted into binary equivalents. Then, four least significant bits of every binary equivalent are removed and logical AND operation is performed on them. To insert 0, results of logical AND must be 0, if not then the pixel intensity is modified such results of logical AND becomes 0. Similarly, to insert 1, results of logical AND must be greater than 0, if not then the

pixel intensity is modified such results of logical AND becomes greater than 0. At the receiver side, after calculating logical AND of pixel intensity and pixel position, if the result is 0 then 0 is that the message bit else 1 is that the message bit. The advantage of this method is that it makes Steg-analysis harder because it distributes the message uniformly on all the bits of pixel value.

In [16], have proposed a novel method of Pixel Value Modification (PVM) by modulus function which works as follows; Convert the secret information into base 3 values of (0, 1, 2). These secret values are embedded using all layers of the pixel (Red, Green and Blue) on condition the pixel value should fall in the range of $0 \leq gi \leq 250$. After that applying this equation on each pixel:

$$"f = f(g_1, g_2, g_3, \ldots\ldots, g_n) = \sum_i^n 1gri \bmod 3" \quad (3)$$

It has been found that the function f has three values (0, 1, 2). then modified pixel value with secret data in RGB planes and combined these RGB planes to give stego image. The proposed method gives better visual nature of stego picture. In addition, proposed strategy extricates the concealed mystery message proficiently without utilizing the range table.

In [17], this process, Zero Order Keep Zooming (ZOH) is used to change the hidden message of the previously proposed image steganography method by using the LSBraille image steganography method to increase MHC. By using the LSBraille image steganography method that can represent the secret message characters by 6 bits only not 8 bits as binary representation, To change the secret message embedded in the cover not the technique of embedding the previously proposed image steganography method, it's vital to use Zero Order Hold zooming (ZOH) This proposed approach offers more MHC and PSNR than the previous proposal method ZOH.

Steganography is the only account secure and secret communication. Existing methods in image steganography specialize in increasing embedding capacity of secret data which are consistent with existing methods, the experimental results indicating that two pixels are required for one secret digit embedding. In direction of improving the embedding size of secret data, a completely unique method of Pixel Value Modification (PVM) by modulus function is proposed. The PVM method can embed one secret digit on one pixel of canopy image. Thus, the PVM method gives good quality of stego image. The experimental outputs validate that good beholding of stego image with more secret data embedding capacity of stego image are often achieved by the proposed technique.

3. THE PROPOSED TECHNIQUE

In this section, the proposed technique will be presented. This technique will concern the spatial domain of the cover image, which works as follow: at first: convert the cover image into three layers (Red-Green-Blue), after that segment the blue layer using initial threshold, which the value of the threshold can be changed to according to the size of the secret message. (the initial threshold in proposed method is 0.2) then convert each pixel of the segmented area (white area) into decimal value, by using Modulus 4 Function take decimal value from the white area and find the values after applying this operation "F= gbi mod 4", So the values may be (0, 1, 2,3). Then take the decimal values of the secret message and converted it into base 4, so the values are 0 or 1 or 2 or 3. Finally, the secret message is embedded using LSB method but in that state, we didn't deal with (0, 1) only. The last significant bit may be (0, 1, 2, 3).

3.1 Embedding Procedure

The embedding process begins with reading the cover image and the secret message, the initial threshold which used in proposed method is (0.2). The flow diagram of embedding process is illustrated in Figure 1, and the embedding procedure can be discussed in the following steps.

Step 1. Read the cover image and the secret message as an input.

Step 2. Separate the cover image into three component color matrices (Red, Green and Blue) and the blue layer is used only to embed the secret message. According to Hecht (researcher) the blue colour is very less sensitive to the human eyes so blue channel is selected to hide the secret data, which is very effective to the visual perception.

Step 3. An initial threshold is selected to segment the blue layer (0.2), which the threshold value can be changed into according to the message length.

Step 4. Let (d) is secret message and convert it into base 4, values of (0, 1, 2, and 3).

Step 5. Take each pixel value from the white area of segmented region and applying Modulus 4function according to equation 1, where the decimal value of the blue pixel can be represented by gbi

$$F = gbi \bmod 4 \quad (4)$$

Step 6. After embedding the secret message in the last significant bit, function f has five cases:

Case 1: If f = d, then, Modification is not needed, directly gbi takes the same pixel value.

Case 2: If f≠d and f< d, by one then, increase the value of gbi by 1, gbi= (gbi +1) then new modified pixel value is obtained.

Case 3: If f≠d and f > d, by one then the value of gbi is decreased by 1, gbi= (gbi -1) then new modified pixel value is obtained.

Case 4: If f≠d and f< d, by two then, increase the value of gbi by 2, gbi= (gbi +2) then new modified pixel value is obtained.

Case 5: If f≠d and f > d, by two then, the value of gbi is decreased by 2, gbi= (gbi -2) then new modified pixel value is obtained.

Step 7: After modification of pixel value with secret data in blue layer, combine these RGB planes helps give the stego image, the resultant stego image.

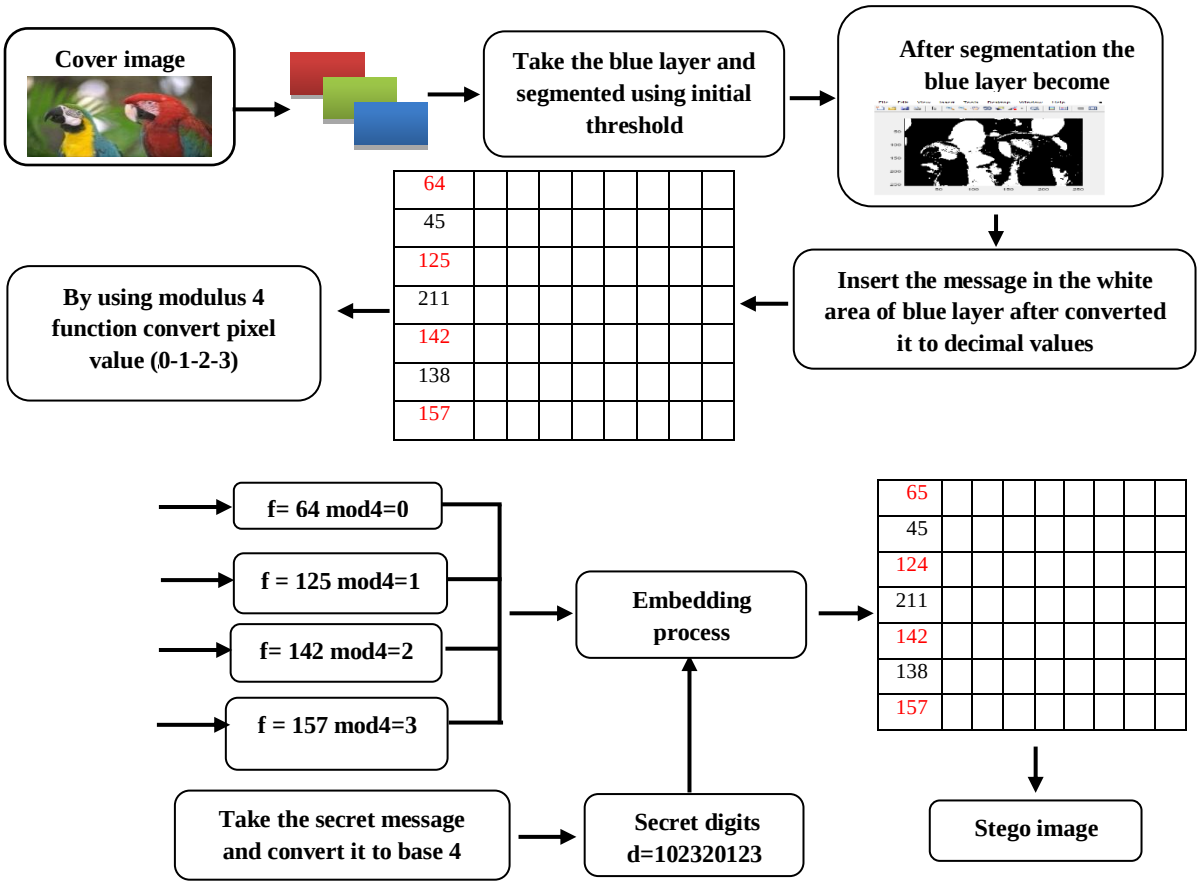

Fig. 1 Embedding process

3.2 Extracting Procedure

The data extraction process begins with reading the stego-image, and using the same threshold which has been used in the embedding process (0.2). The flow diagram of extraction process is illustrated in Figure2.and the following steps are discussed.

Step 1: Read the stego image as input and separate it into three component planes Red, Green and Blue.

Step 2: Take Blue layer and segment it by using the same threshold (0.2)

Step 3: In the segmented area (whit region) apply this equation on each pixel value.

$$F=gbi \bmod 4 \quad (5)$$

Step 4: The result of the mod value is the secret message of the base 4.

Step 5: By using the function char convert the decimal values to character and extract the secret message.

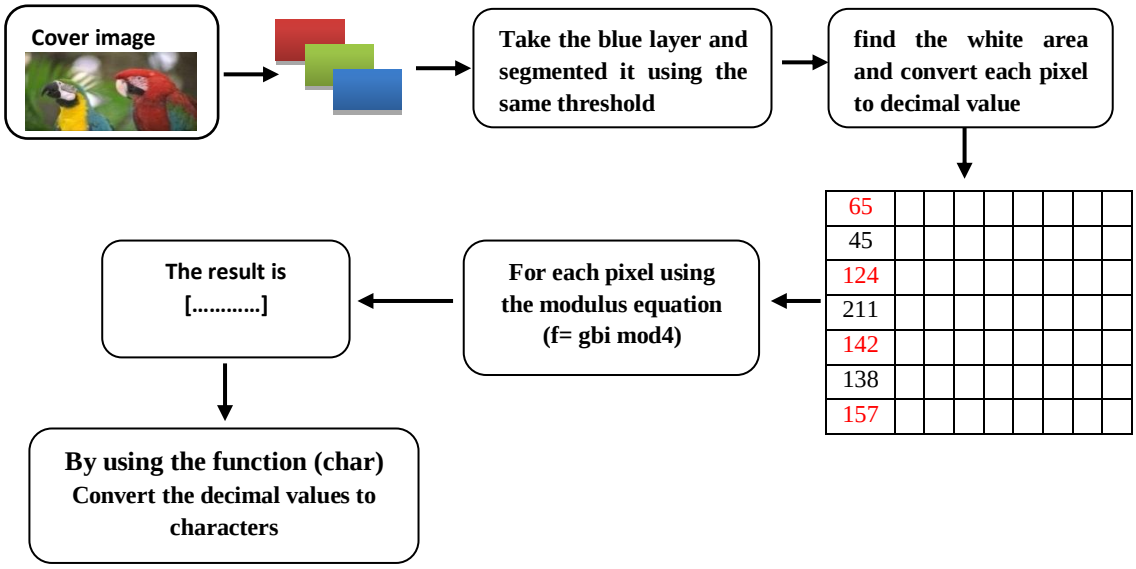

Fig.2 Extraction process

4. EXPERIMENTAL RESULTS

The proposed technique has been implemented using MATLAB environment. This technique has been tested using different messages with different lengths to hide them in cover image. The performance of this proposed technique has been studded using different kinds of measures like (PSNR, MSE). To evaluate the performance of proposed technique, several simulations have been performed in order to compare its performance with other existing schemes.as shown in Tables 1,2, 3, 4, and 5.

Table 1. Comparison between (LSB-3), (ZOH) techniques and proposed technique

Cover Images	Message Capacity	PSNR		
		LSB– 3 [16]	ZOH [17]	Proposed technique
Boat	8,160	39.1132	49.9386	52.5334
Bird	8,160	39.0955	49.9167	51.2065
Flinstone	8,160	39.1188	49.9513	52.4849

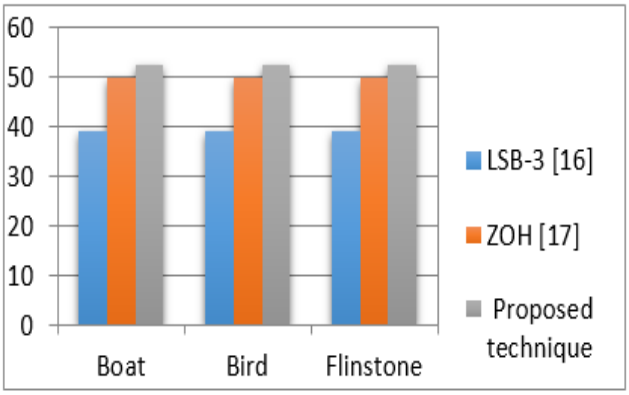

Fig. 3 PSNR Comparison between (LSB-3[16]), (ZOH [17]) techniques and the proposed technique

According to the comparative results in Table 1, and Figure 3, it is found that the PSNR of the proposed technique is better than that the LSB-3, and ZOH techniques. In addition, the stego image quality of proposed method is very high relative to the LSB-3, and ZOH techniques.

Table 2. Comparison Between Dagar [18], Maurya et al. [19] techniques and Proposed technique

Cover Images	Message Capacity	PSNR		
		Dagar [18]	Maurya et al [19]	Proposed technique
Boat	2881	49.2668	53.7618	57.0775
Bird	2881	48.8766	53.7558	57.0380
Flinstone	2881	47.9887	53.7869	57.0933

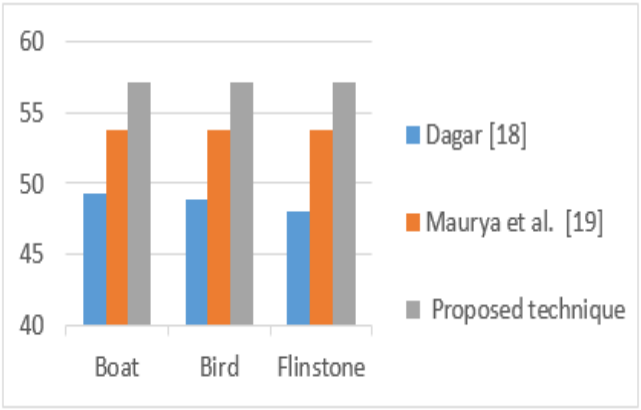

Fig. 4 Comparison between Dagar [18], Maurya et al. [19] techniques and the proposed technique

Table 2, and Figure 4 also represent the comparative results of the proposed technique with technique [18] and technique [19] by using (2881) byte (secret message character) and 256 x 256 cover image (Boat, Bird, and Flinstone). And it is found that the PSNR of the proposed technique is better than that the other techniques.

Table 3. Comparison between Singh et al. [20], Singla et al. [21] Techniques and Proposed technique.

Cover Images	Message Capacity	PSNR		
		Singh et al.[20]	Singla et al.[21]	Proposed technique
Lena	4287	38.5342	39.6310	55.3440
Pepper	4287	35.7352	38.6527	55.3324
Baboon	4287	35.1693	41.5895	55.3028

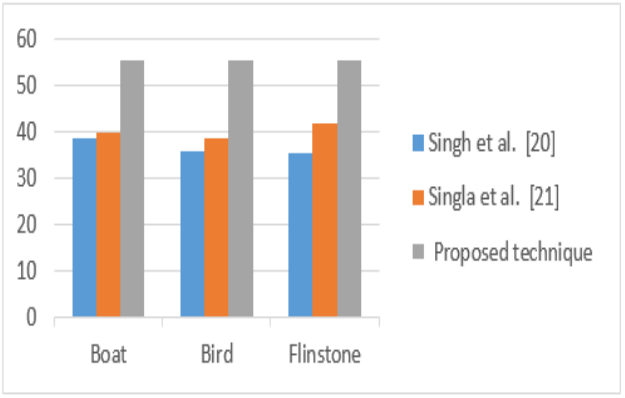

Fig. 5 PSNR Comparison between Singh et al. [20], Singla et al. [21] techniques and the proposed technique

Furthermore, as shown in Table 3, after the comparisons have been done among the proposed technique and technique [20] and technique in [21] by using secret message consists of 4287 bits and 3 different 256 x 256 cover images (Lena, Baboon and Peppers) it has been found that the proposed technique has the highest PSNR values among these methods which also means that the stego image quality of the proposed method will be higher.

Table 4. Comparison between Nandani et al. [22] technique and proposed technique

Cover Images	Message Capacity	PSNR	
		Nandani et al. [22]	Proposed technique
Lena	2547	40.0692	57.5129
Baboon	2547	38.4049	57.4179
Pepper	2547	37.2010	57.4301

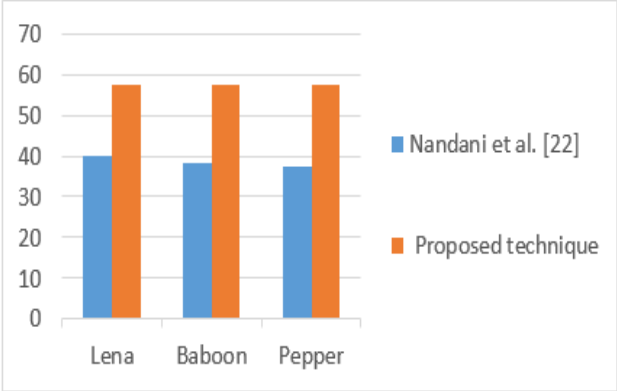

Fig. 6 PSNR Comparison between Nandani et al. [22] and the proposed technique

Table 4 and Figure 6 show the comparison between the proposed technique with technique [22] by using 2547 characters (bytes) secret message and 256 x 256 cover images (Lena, baboon, pepper), and it was founded that the proposed technique has more PSNR values than other technique which means the stego image quality of the proposed technique will be higher than the other techniques.

Table 5. Comparison Between MSLDIP-MPK technique and Proposed technique

Cover Images	Message Capacity	PSNR	
		MSLDIP-MPK[23]	Proposed technique
Boat	8,192	49.36969	52.5686
Bird	8,192	49.54604	52.5498
Pepper	8,192	49.25001	52.4864

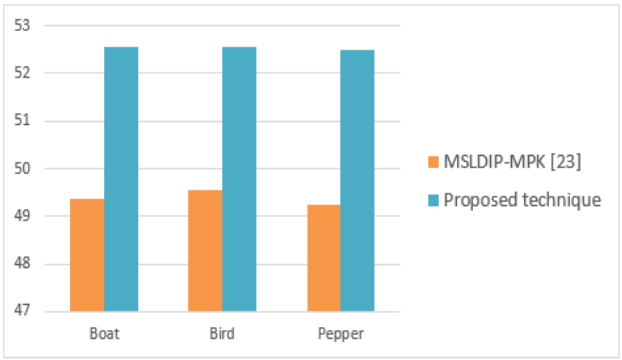

Fig. 7 PSNR Comparison between MSLDIP-MPK technique [23] and the proposed technique

Also, In Table 5, a secret message with length 8,192 bytes has been hidden in the cover images (Boat, Bird and Pepper) with sizes (256 x 256), using the MLDIP-MPK and proposed technique, it has been noticed that, the proposed technique has higher PSNR values too, as we shown in Figure 7.

The proposed technique was compared with a lot of techniques as shown from Table 1 to Table 5 or from Figures 3 to 7; it has been found that the proposed technique has higher PSNR values than other techniques which means that the stego image quality of the proposed technique will be higher than the image quality of other techniques. This means that this enhancement has been succeeded to improve the security. While keeping the PSNR values higher than other techniques.

5. CONCLUSION

In this paper, a new way of hiding information in an image with less variation in image bits have been created, based on modulus function and segmentation which makes our technique secure and more efficient. The new approach is based on calculating modulus of pixel value in the blue layer with the Mod Factor 4, which in the first segmented the blue layer depends on the initial threshold and embedded the secret message in the white area, after converting the secret message into base 4. A comparative study has been done and the experimental results founded that the proposed technique is considered an effective technique which achieved high level of capacity, higher PSNR for security. In the future work, It is hoped to apply the proposed techniques on other carrier files such as audio files and video files, and check the validity of the proposed techniques on these carriers. Try to develop some new techniques which improve the various parameters of image steganography and give us better results. Try to develop new techniques that are successfully to resist statistical attacks like RS analysis, histogram analysis, and chi-square analysis.

6. REFERENCES

[1] Hassaballah, M., Digital Media Steganography: Principles, Algorithms, and Advances, Elsevier, 2020, ISBN: 9780128194386.

[2] Alqadi, Z., Zahran, B., Jaber, Q., Ayyoub, B., & Al-Azzeh, J. (2019). Enhancing the Capacity of LSB Method by Introducing LSB2Z Method. International Journal of Computer Science and Mobile Computing, 8(3), 76-90.

[3] Khan, S.; Khan, K.; Arif, A.; Hassaballah, M.; Ali, J.; Ta, Q.T.H.; Yu, L. (2020). A Modulo Function-Based Robust Asymmetric Variable Data Hiding Using DCT. Symmetry, 12, 1659.

[4] Hassaballah, M., Hameed, M. A., Awad, A. I., & Muhammad, K. (2021). A Novel Image Steganography Method for Industrial Internet of Things Security. IEEE Transactions on Industrial Informatics.

[5] Chung-Ming Wang, Nan-I-Wu, Chwei-Shyong Tsai, Min-Shiang Hwang (2008). A High Quality Steganographic Method with pixel value differencing and modulus function, The Jurnal of System and Software, 81(1), 150-158.

[6] Bohme. Rainer (2010), Advaced Statistical Steganalysis. Springer.

A. A. Radwan, A. Swilem, and A.-H. Seddik, "A High Capacity SLDIP (Substitute Last Digit in Pixel) ", Fifth

International Conference on Intelligent Computing and Information Systems, 30 June - 3 July, 2011, Cairo, Egypt.

[7] Hassaballah, M., Hameed, M. A., Aly, S., & AbdelRady, A. S. (2020). A color image steganography method based on ADPVD and HOG techniques. In Digital Media Steganography (pp. 17-40). Academic Press.

[8] Altaay, A. A. J., Sahib, S. B., & Zamani, M., "An Introduction to Image Steganography Techniques", (2012) International Conference on Advanced Computer ScienceApplications and Technologies.

[9] Vaidya, K., Kargathara, A., & Kumbharana, C. K. (2021). Classification of Image Steganography in Substitution Technique. In Rising Threats in Expert Applications and Solutions (pp. 253-261). Springer, Singapore

[10] Almohammad, A. (2010). " Steganography-Based Secret and Reliable Communications: Improving Steganographic Capacity and Imperceptibility. PhD thesis, Brunel University.

[11] Hamid, N.; Yahya, A.; Ahmad, R. B.; Najim, D. and Kanaan, L. (2013). "Steganography in Image Files: A survey". Australian Journal of Basic and Applied Sciences, 7(1), pp. 35-55.

[12] Hemalatha, S., Acharya, D. U., Renuka, A., & Kamath, P. R. (2013). "A Secure and high capacity Image Stenography Technique". Signal & Image Processing: An International Journal (SIPIJ), 4(1), pp 83-89.

[13] Cheddad, A. (2009). "Steganoflage: A New Image Steganography Algorithm", Doctor of Philosophy Thesis, School of Computing & Intelligent Systems, Faculty of Computing & Engineering, University of Ulster.

[14] Saini, R., &Yadav, R. (2012). "A New Data Hiding Method Using Pixel Position and Logical and Operation". International Journal of Computer and Electronics Research, 1(1), pp. 12-18.

[15] Nagaraj, V., Vijayalakshmi, V., &Zayaraz, G. (2013)." Color image steganography based on pixel value modification method using modulus Function". IERI Procedia, 4, pp.17-24.

[16] Abdelmged, A., et al. (2016). "Improving ZOH Image Steganography Method by using Braille Method." International Journal of Computer Applications 975: 8887.

[17] Dagar, S. (2014). "Highly Randomized Image Steganography Using Secret Keys". In Recent Advances and Innovations in Engineering, IEEE, 2014 pp. 1-5.

[18] Maurya, S., & Shrivastava, V. (2014). "An Improved Novel Steganographic Technique for RGB and YCbCr Colorspace". IOSR Journal of Computer Engineering, 16(2), pp.155-157.

[19] Singh, S., & Datar, A. (2015). "Improved hash based approach for secure color image steganography using canny edge detection method". International Journal of Computer Science and Network Security, 15(7), pp.82-89.

[20] Singla, K., & Kaur, S. (2012). "A Hash Based Approach for Secure Image Stegnograpgy Using Canny Edge Detection Method". International journal of computer science and communication, 3(1), pp. 156-157.

[21] Nandani, D., & Yadav, R. (2015). "Assessment of Steganography using Image Edges for Enhancement in Security". International Journal of Modern Engineering Research, 5(8), pp. 36-46.

[22] Ali, A. A., & Saad, H. S. (2012). New Technique for Encoding the Secret Message to Enhance the Performance of MSLDIP Image Steganography Method (MPK Encoding). International Journal of Computer Applications, 59(15).