Engineering and Technology Journal
Journal homepage: engtechjournal.org

An Improved Method for Combine (LSB and MSB) Based on Color Image RGB

Sally A. Mahdi [a*], **Maisa'a A. Khodher** [b]

[a] Department of Computer Sciences, University of Technology, Bagdad, Iraq, cs.19.68@grad.uotechnology.edu.iq
[b] Department of Computer Sciences, University of Technology, Bagdad-Iraq, 110044@uotechnology.edu.iq

*Corresponding author.

Submitted: 21/01/2020 Accepted: 19/04/2020 Published: 25/03/2021

K E Y W O R D S
Information Hiding, Steganography, LSB, MSB, Secret key.

A B S T R A C T

Image steganography is the art of hiding data into an image by using the secret key. This paper presents two techniques that combine the most significant bit (MSB) as well as the least significant bit (LSB) based on a color image (24bit for RGB). The presented study proposes a novel method to combine (LSB and MSB) bits based on check MSB values and replace bits from LSB with a secret message. The result of this proposed method that made not affect quality stego -image based on the resulting histogram that shows a match between the cover image and stego- image and more secure because not hidden in all image. The factors were used Mean Square Error (MSE), Compute Payload, in addition to Peak Signal to Noise Ratio (PSNR). The PSNR's rate is high and MSE is less. The result of this paper when applying on the different image gives high PSNR of 87.141 and less MSE of 0.00012 when inserting message 80 bits and reduction value PSNR of 72.023 and MSE of 0.0040 when inserting message 1200 bits and measure entropy is the same value for cover image and stego –image then this method is more security for the attacker.

How to cite this article: S. A. Mahdi and M. A. Khodher "An improved method for combine (LSB and MSB) Based on color image RGB" Engineering and Technology Journal, Vol. 39, Part B, No. 01, pp. 231-242, 2021.
DOI: https://doi.org/10.30684/etj.v39i1B.1574
This is an open access article under the CC BY 4.0 license http://creativecommons.org/licenses/by/4.0

1. INTRODUCTION

The internet is providing a lot of advantages to humans, particularly to exchange or get information, working, learning, and so on. Privacy of data and security are the problems of the internet. A lot of approaches were utilized to provide security including digital signatures, steganography, cryptography, and watermarking [1]. Steganography comes from the Greek words and indicates hidden writing, as "stegano" refers to "covered", and while "graphy" refers to "writing" [2]. The security of information is required to transmit confidential data. Cryptography and steganography are applied to secure the secrecy and confidentiality of information. With regard to the former, the secret text will be converted to ciphertext, whereas in the latter, the secret text won't be changed, yet it will be embedded in other data formats. Now, with the existence of significant systems of communication, there is a high difficulty to protect secret information from hackers. The fields of steganography hide the presence of information as well as protecting the secret information

from unauthorized access. The systems of steganography include 3 components, which are: plain-text, Cover file, in addition to the Stego file. Also, the secret information that should be protected has been referred to as plaintext. Furthermore, the cover files might be videos, audio, images, texts, where data have been embedded. The Stego file is defined as output regarding the steganographic system which consists of hidden information. There are 3 significant properties related to steganographic systems which are robustness, payload capacity, and security [3]. There have been many multimedia into images like JPEGs, GIFs, BMPs, TIFFs, and PNGs [4]. The main process of image steganography that contains two processes (embedded in the sender and extracting in the receiver) and hiding messages in the cover image is called embedded message, there are three types of steganography to embed a secret message in the cover image and these types are (pure, secret key, public key) [5]. The basic model of processes image steganography may be represented as shown in Figure 1, [6]:-

Cover image(c) + secret message (m) + Stego_ Key (k) = stego_image (c, m, k), [7].

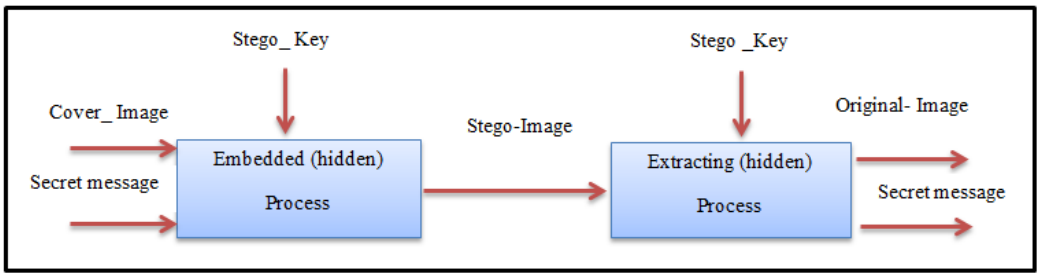

Figure 1: Basic Steganography System, [5]

In the image, steganography contains a spatial domain that includes the most popular technique is LSB that means takes the least value from the binary number when converting pixel value into binary, information is hidden inside the LSB bits of the embedded image which is not detectable when observed by the human eye [8], since changing the LSB values throughout embedding is going to have minimum impact on stego image quality so hackers cannot predict that some data is hidden behind that image [9]. The higher value is the bit location in binary number that called a Most significant bit(MSB) and also called (high order bit)[8].

This paper proposes a new approach by using combine LSB and MSB based on a color Image consist of 24 bit for 3 channel (Red, Green, Blue), As the data is hidden in dark areas more than light areas, and as a result, no change in the stego image appears based on the same secret key for embedding and extracting which is using point curve sin than the agreement between sender and receiver.

2. LITERATURE REVIEW

Below some of the research which is related to the proposed method. in this part, some of the previous works will be illustrated from 2015 to 2019, which are related to image steganography spatial domain, specifically, the proposed method Least significant bit (LSB).

In 2016, R. Tavoli, et al. have suggested a new method for image steganography using LSB، Where the proposal first includes compressing text data before hiding the data in the image and is encoded by using a 4 * 4 mask called snake scan order, after implemented compressed and snake scan order then loaded text in the image for embedding and extracting the used key and without key when the length of the key is dynamic, Then the researcher suggested making XOR the key and text after converting them into binary and the output is coding, then the result code applies XOR with the key and decode is produced. The result of the proposed method is illustrated measurements PSNR and MSE in each (RGB) channel which is the result of peak-signal-to-noise Ratio between (51.78-58.81) and the result of Mean Square Error between (0.1087-0.4363) when using Lena image and another image [10].

In 2017, C. G. Tappe, et al.have proposed a new method for image steganography in the spatial domain by using LSB and MSB, which is presented a new method in two steps embedding and extracting, the first step is read cover image and read bits No.5 and No.6 and compute difference between them if the information bit is not equal to difference will be transversal bit chosen No.5.The second step is extracting secret information bit from stego_image which is apply new suggested by

reading stego_image and every pixel in stego_image compute the difference between location bit No.5 and No.6 that must be equal, the result of this proposed is given high security and high capacity, the result peak-signal-to-noise Ratio of the proposed method was (47.50) and payload (786432)when using different image [11].

In 2018, G. Maji, et al. have proposed a new model for image steganography in the spatial domain by using technique LSB. This method has been included two images (cover image and Reference image) and a secret embed key (stego key). The reference image is partitioned into blocks with allocated block codes. In the embed, the key is stored in the absolute amount of blocks and other inserting parameters (beginning block, block crossing route, and so on), where the secure message is altered into binary which is included pair of bits, pair of bits in the reference image are encoded that using various blocks of the reference image and updating sometimes in LSB bits. As a discretionary limit improvement module for content, just secure messages lexicon word ordering based encoding is applied. At last, in cover, _image is inserted encoded bitstream utilizing any traditional LSB with its very own benefits and negative marks by using the public key of the recipient is encrypted embedding key. It is not possible to know the hidden message even if someone gets the encrypted message. This proposed can be used any LSB replacement to embed an encrypted message in the cover_ image by using the various lexicon word indexing designs each time this becomes safer depending on a random secure key which is added in the embed key. The result of the peak-signal-to-noise Ratio between (62.3249_ 71.5974) and Mean Square Error between (0.0381_ 0.0049) when using Mandi image [12].

In 2019, U. Ali, et al. have proposed a new method for image steganography using technique LSB. Where the information is embedded in the random bit location of the pixel. The researcher used color images represented by red،green and blue colors, and each color represents 8 bits, where the random location of the three binary colors is used to embed secret message bit, for each (R, G, B) values of the cover image is represented (7 bit) most significant bit (MSB) and generate random bit location by using pseudo-Random Number Generator. The operation XOR is performed between the first location of the secret message bit and the random bit location of the red value, as a result, it is replaced with Least significant bit and performs between the second location of the secret message bit and the random bit location of the green value in next the third location of the secret message bit and the random bit location of the blue value and so on. The result of the peak-signal-to-noise Ratio between (56.1544- 85.0479) and Mean Square Error between (0.02022934- 0.00004196) when using (Lena, peppers, Baboon) images [5].

In 2020, M. A. Al Mamun, et al. have proposed a new method for image steganography using technique LSB, the researcher encrypted data before hidden and determine pixels randomized way by using Stren-Brocot Sequence. Multiplied LSBs of the color image (RGB) are applied while injecting the encrypted message into the randomly chosen pixels. The result of this proposed is to change the cover image quality when inserting different size of the secret message, but not changing the stego image quality after applying the proposed method that appears successfully extracted secret message from the stego image [13].

3. TYPE OF STEGANOGRAPHY

I. Pure steganography

This kind of steganography does no need precognition of the code such as stego key to begin the communication system. The safety is totally trusted the secrecy, the benefit of this kind does not needs stego key to participate between sender and receiver. If the third party is Knowledge of the encryption algorithm then does not provide any security because the sender and receiver rely on that not Know the third party any information about the algorithm. The pure steganography is representing (C, M, D, EX) [14].

II. Secret Key Steganography

Secret key steganography is comparable to a symmetric cipher. This type represents the same key for the sender and receiver when the sender embeds a secret message in to cover image by using a secret key and the receiver can extract a secret message by reversing the process and using the same secret key. The secret key steganography is representing (C, M, K, EM, EX) [14].

III. Public Key steganography:-

This kind of steganography contains two keys (public key and private key). The public key used for the sender when embedding a secret message in to cover image and from the other side at the receiver will be used private key to extract the secret message from the cover image that was sent by the sender. In a public database is stored public key [15].

4. . STEGANOGRAPHY IN IMAGE

Steganography in an image consists of two domains: - spatial domain technique and transform domain technique, spatial domain (image-domain) works with the bits in the cover image and embeds the secret message in this image as it does not affect the image and noise is processed. The transform domain (frequency domain) works on transforms the image and manipulates the algorithm [1].

I. Image Domain (Spatial Domain Technique):-

In the spatial domain contain various techniques. These techniques work on replacing some bits in image pixel value without altering or affecting the image to hide the information such as Least significant bits is one of the not complex techniques but given good result and not effect on the image and modifications of the LSB in the value will be invisible for human eyes. This technique including resists uniform affine transformations inclusive of rotation, scaling, and cropping. Image domain strategies are broadly categorized into

1) Least significant bits (LSB).
2) Pixel value differencing (PVD).
3) Random pixel embedding method (RPE).
4) Labeling or connectivity method.
5) Pixel intensity-based method.
6) Texture based method.
7) Histogram shifting methods to be specific.

In this paper, we will discuss one technique is the Least significant bit and it's modified.

Least significant bit (LSB): The LSB is the most popular and simplest technique for hiding information. in an original image. In LSB one bit or all bytes of the image are changed in which the secret message is embedded When color images are used that consist of three colors (Red, Green, Blue), pixels composed of 24 bits, and each color consists of 8 bits for that it will be saved 3 bit per pixel, maybe store a total amount of 1,440,000 bits or 180,000 bytes of sending information for the image that you report 800 × 600 pixels, as an instance for 24-bit pixel, can be represented as follow:-

10010101 00001100 11001001 10010110 00001111 11001011 10011111 00010000

Which can be a binary description are **11001000** for the number 200 that is embedded in the cover image. In the section dedicated to LSB. These 8 bits are distributed over the eight bytes shown above the first bit is changed from each byte.

10010101 00001101 11001000 10010110 00001111 11001010 10011110 00010000

It is easy to hide information when the image is high quality and accurate as 24-bit images are the best for hiding information because of its size can be used in image format BMP or GIF. The best type to hide information inside the image is BMP [16]. When the message is embedded in the cover image by the LSB method, the result will be Stego Image [9].

5. FACTORS OF EFFECTIVE STENOGRAPHIC METHODS

Measuring image quality requires a comparison of cover image results and stego image and common measurements that are used (Peak Signal-to-Noise Ratio, Mean Square Error, payload).

1) Mean Square Error (MSE):- It is a measure between cover image and stego image C(x, y) and S(x, y) is calculated by using the following equation:

$$MSE = \frac{\sum_k [C(x,y) - S(x,y)]^2}{x * y} \quad (1)$$

Where x is represented the number of rows and y is the number of columns inside the cover image.

2) Peak Signal-to-Noise Ratio (PSNR):-The PSNR of the cover image and stego image is calculated by using the following equation:

$$PSNR = 10log_{10}\left(\frac{R2}{MSE}\right) \quad (2)$$

The maximum image pixel value is 'R', that the R=2b-1, b is represented bit bottom of the cover image, MSE is represented Mean square Error. PSNR measurement is done in decibels (db). To compare the results of the same restored image, PSNR is used as a good measure.

3) Capacity (Payload):- It is the scale of the information in the original image that may be changed. However, the integrity of the cover image is not affected. Payload depends on the full no. of bits according to pixel and the range of bits embedded in every pixel. Where the payload is in bits per pixel (BPP) and the maximum capacity (MHC) is to hide in percentage.

$$payload = no.of\ secret\ message\ bits\ /size\ of\ \text{the}\ cover\ image \quad (3)$$

4) Histogram: - The histogram evaluates the number of events of a definite density pixel value in the entire image. The number of pixels varies with a change in the density value due to a change in the lSB pixels, better to be the differences in histogram less between the cover image and the Stego image because these changes can be used to reveal the secret message in stego analysis [12].

5) Information entropy: - Measure security of steganography system by using entropy. Let e_1, e_2,e_3,... e_n be n possible element with probabilities $p(e_1), p(e_2), p(e_3)$. The entropy is given as:

$$H(e) = \sum_{i=1}^{n-1} p(e_i)\, log_2\, p(e_i) \quad (4)$$

This comparison produces an evaluation of the average minimum no. of bits that are needed to encode a sequence of bits based on the frequency of the symbol [17].

6. PROPOSED METHOD

In this proposed method will be used a color image which contains three colors (Red, Green, Blue) of 24 bit for each color (RGB) contain 8 bit and the value of each of these colors is represented using a number from 0 to 255, we know that the number 255 is (11111111) in a binary system, we will represent the pixel using 3 Bytes, which is the number that determines the intensity of the color, by way of representing decimal numbers using binary. One byte, meaning we only need one byte to represent the color using Least significant bit (LSB), Most significant bit(MSB) to hide the secret message so that no one can see the message in the image. This method includes three stages (embedding and extracting), and using the secret key for both two steps to increase security,

1) The first stage input the cover image and use the following extensions (".JPG", ".JPE", ".BMP", ".GIF", ".PNG"), which each extension can give a certain percentage in the hiding measures and no affect the image. In this step using the secret key) for the embedding and extracting stage, the secret key proposed has been implemented using point curve sin in the cover image. To extract locations key points (maximum point, minimum point, and the intercepts) so must apply these function y=sin(x) and the curve points that are extracted from the width of the cover_ image (X) and height using the function (y=sin(x)) which result point (x: width, y: height) to hide secret messages at these points. Figure 2 illustrates the general work of the proposed image steganography

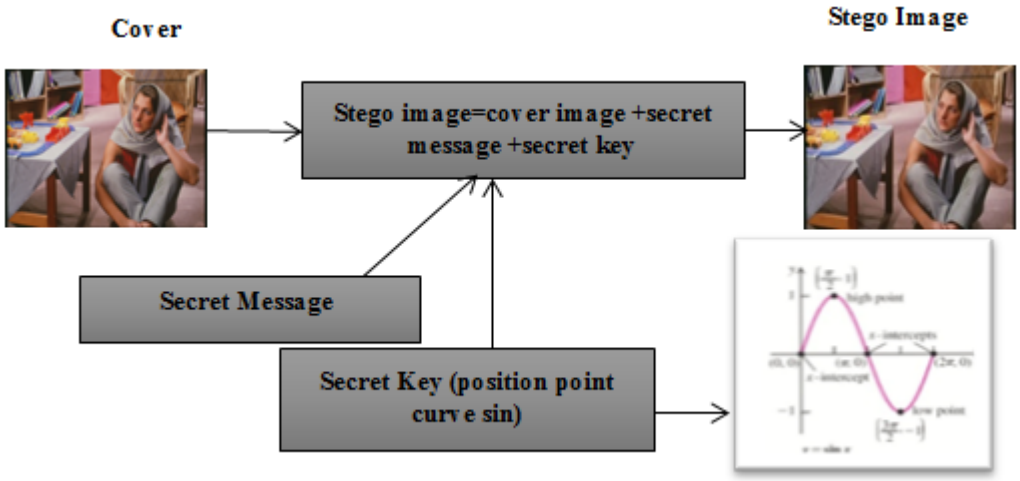

Figure 2: The general work of the proposed image steganography.

2)The second stage process LSB of embedding is converting secret message and cover image into binary and compare size of the secret message with the size of an image (width, function curve sin (height)) and then take last 3 bit from the most significant bit and apply condition if MSB contains last 3 bit is (000) will be replaced first 2 bit from LSB with the secret message but if contain MSB one in the last 3bit such as (001,100,101,010,111) so will be replacement 1 bit from first LSB with a secret message and embedded message based on the size of the cover image (using different size not determine).

3)The third stage process LSB of extracting secret message by using the same secret key (locations curve sin), which must be select pixels and converted to binary and extract secret message by using the same proposed method about LSB and MSB where check MSB if contains last 3 bit "000" then extract first 2 bit from LSB but if MSB contains '1' last 3 bit for example (111,011,010,101,110,100)then extract 1 bit from first LSB bits when the secret message is completely extracted from the binary bit, it will be converted to ASCII code and then converted to character. In Figure 3 below, the steps are illustrated for the proposed method.

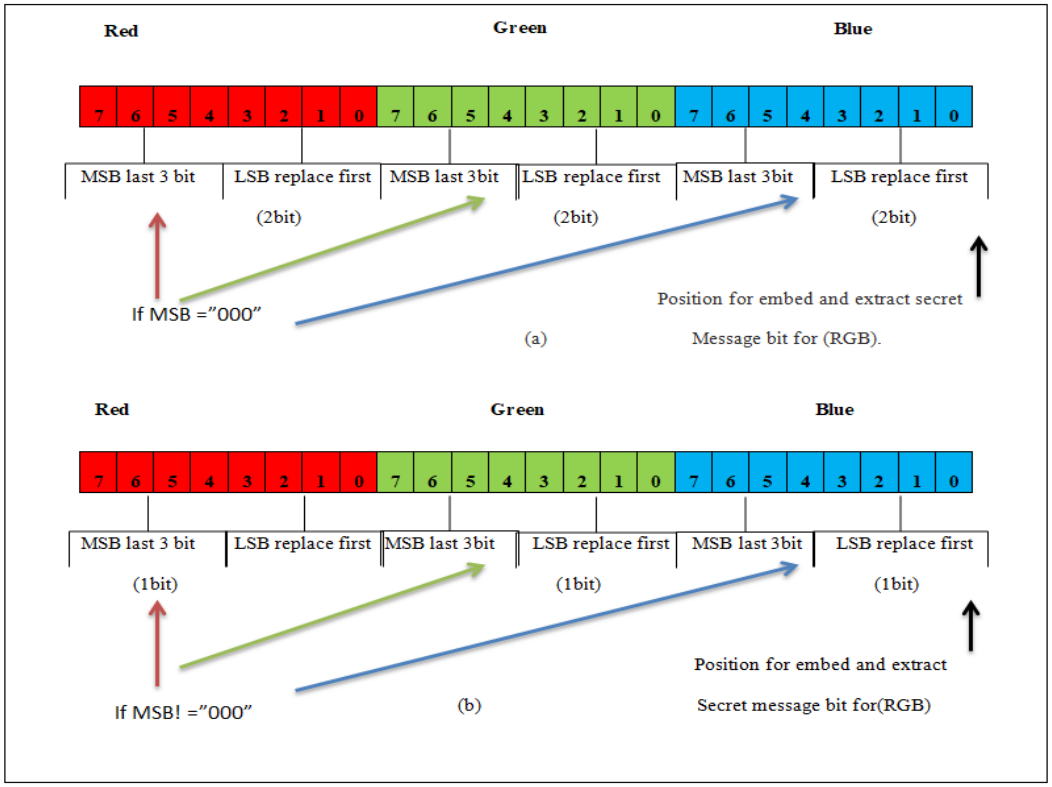

Figure 3: (a, b): LSB and MSB for embedding and extracting algorithm for 3 colors.

Algorithm (1): Embedding algorithm

Input

CovImg() *'Cover Image*
w, h *'Image width, height*
Seckey() *'secret key(point curve sin)*
Lmsg *'length secret message*

Output

StegoImg() *'stego image*

Steps

Define Tmp(w,h)
Set Tmp ← CovImg
Set lenth← (*Lmsg*8)+10*
Set *d*←0
For i Do{0 ≤ i ≤ lenth }
Set j←Sin(i* 2.0 * Pi / w+ 1.0) * (h - 1) / 2.0)
For all x, y **Do** {0 ≤ x≤ w, 0 ≤ y ≤ h}
If d < lenth **Then** *pedge* ← CovImg*(x, y)*
r ← *pedge.R* *g* ← *pedge.G* *b* ← *pedge.B*
If *r* = "000" **OR** *g* == "000" **OR** *b* == "000" **Then** **Set v**← Seckey(d)
d++
Set temp ← Remove(6, 1).Insert(6, v)
Else If d < lenth **Then Set v**← Seckey(d)
d++
Set temp temp← Remove(7, 1).Insert(7, v)
EndIf
EndIf
EndIf
Set Tmp(x,y) ← temp
End For
End For
End For

Algorithm (2): Extracting algorithm

Input

StegoImg() *'stego image*
w, h *'Image width, height*
Seckey() *'secret key(point curve sin)*

Output

Secmes() *'secret message*

Steps

```
Define Tmp(w,h)
Set Tmp ← CovImg
Set d←0
For i Do{0 ≤ i ≤ lenth  }
Set j←Sin(i* 2.0 * Pi / w+ 1.0) * (h - 1) / 2.0)
   For all x, y Do {0 ≤ x≤ w, 0 ≤ y ≤ h}
        If d < lenth Then  pedge ← StegoImg(x, y)
         r ← pedge.R     g ← pedge.G    b ← pedge.B
            If r = "000" OR g == "000" OR b == "000"  Then  Set v← Seckey(d)
              d++
                Set temp ← Remove(6, 1).Insert(6, v)
                 Else  If  d < lenth Then Set v← Seckey(d)
                  d++
                  Set temp temp← Remove(7, 1).Insert(7, v)
                EndIf
             EndIf
        EndIf
        Set Secmes(d)  ← ASCII( temp)
          End For
        End For
  End For
```

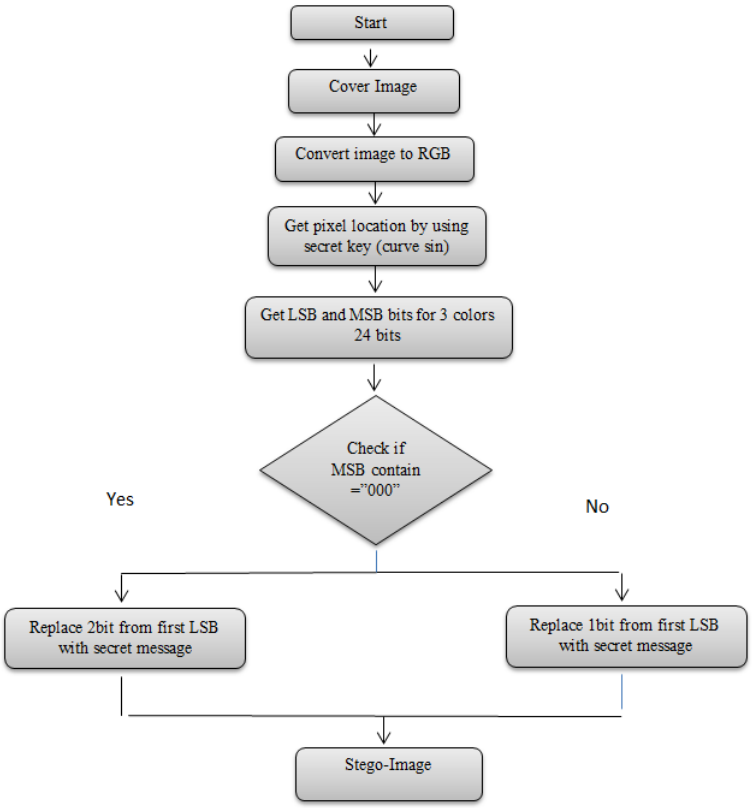

Figure 4: Flowchart embedding for sending part.

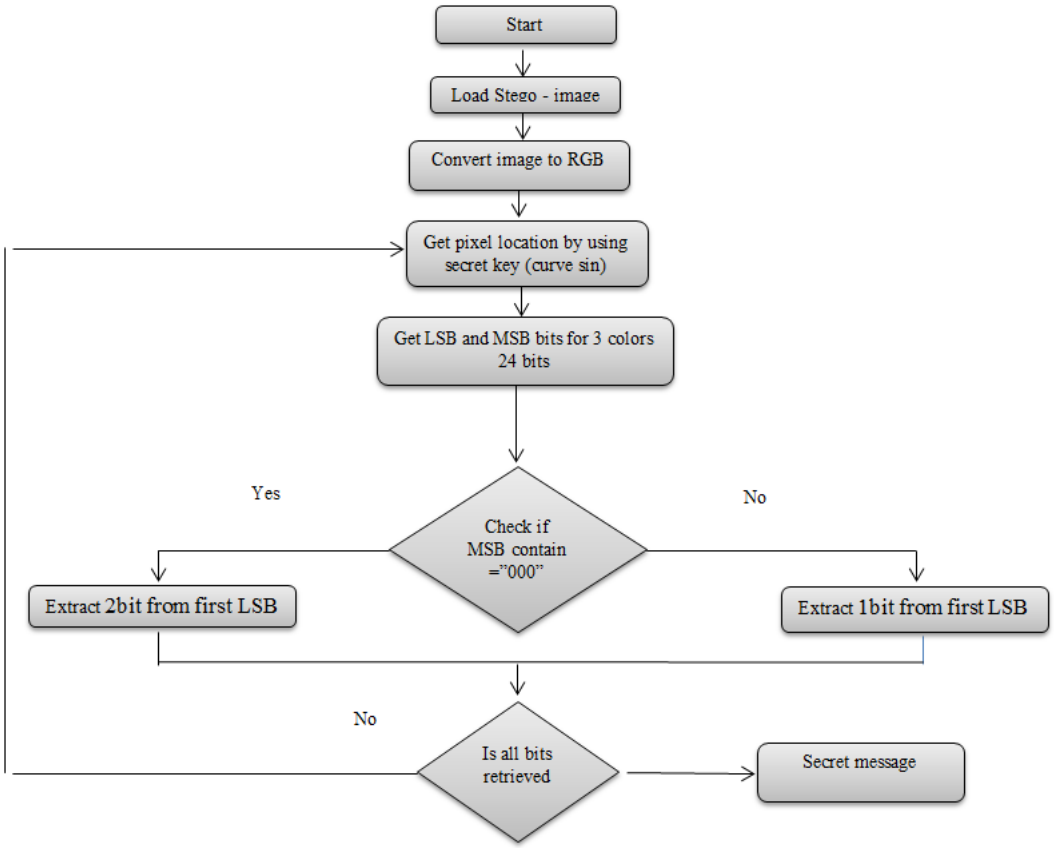

Figure 5: Flowchart extracting for receiving part.

7. EVALUATION AND RESULT

The proposed method has been used four factors to evaluate between the cover image and stego image and implement this method in language C# visual studio 2019. The method has experimental on different images like (Lena, Baboon, Mandi, ppepers, flours) as shown in Figure 6 with different extensions such as (BMP, PNG,..etc) and different image size based on using proposed idea using a secret key (points curve sin) to hide a secret message in these points. As a result, has been illustrated payload (capacity) by using the following equation 3 in section V and the measure PSNR is implementing the following equation 2 in section V between the cover image and stego image which result in high PSNR when using the various image of different size, Since the result is high in PSNR so the result MSE will be less, according to the equation 1 in section Because the result is inverse between PSNR and MSE.

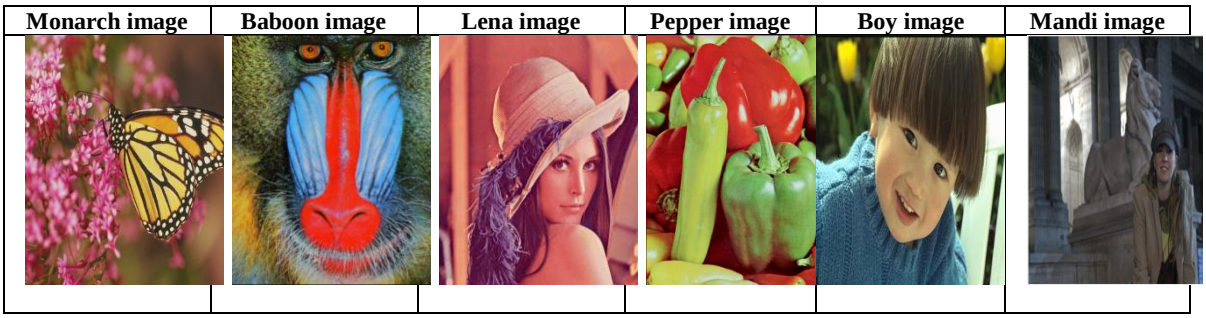

Figure 6: Different cover images apply to the proposed method.

In Table 1 represent the result of the proposed method by experiment on six images and different image format and is the different dimension of the image and insert message Hello world and payload in bits (98).

TABLE I: Measurements of the proposed method for (PSNR, MSE) between the cover image and stego-image

Cover image	Size of Image(bits)	PSNR	MSE
Mandi.JFIF	768x508	87.141	0.00012
Lena.PNG	512 x 512	83.742	0.00027
Baboon.Bmp	500 x480	84.608	0.00022
Boy.JPEG	768x512	87.35	0.0001
Peppers.PNG	512x512	83.339	0.00030
Monarch.JFIF	768x508	86.753	0.00013

Table 2 represents the result of the proposed method when inserting message between (1200-2400) bits and applies on six images which are different image formats, the result is high payload and decrease PSNR and less MSE.

TABLE II: The measures of the proposed method by using different payload bits and different images.

Cover image	Size of Image(bits)	PSNR	MSE	Payload (bits)
Mandi.JFIF	768x508	72.023	0.0040	2426
Lena.PNG	512x512	72.242	0.0038	1667
Baboon.Bmp	500x480	70.534	0.0057	1738
Boy.JPEG	768x512	72.897	0.0033	2426
Peppers.PNG	512x512	71.656	0.0044	1748
Monarch.JFIF	768x508	73.032	0.0032	2370

Table 3 represents the result of the proposed method when using different capacity bits in Monarch cover image which will be high PSNR and less MSE and has observed when decrease payload the result of the PSNR is high compare when high payload the PSNR is Less but in this method PSNR not much decrease but approximately for rate PSNR in less payload.

TABLE III: The measure of the proposed method and using different payloads in monarch

payload (bits)	2370	1970	866	426	290	50
PSNR	73.032	73.787	77.201	80.594	82.678	90.459
MSE	0.003	0.002	0.001	0.0005	0.0003	5.849

Table 4 represents the comparison between the proposed method and other methods when using the same secret message length and image and same payload to compare method is strong or not and when applying the proposed method will be very good and gives high PSNR and less MSE according to other methods.

TABLE IV: Comparisons between the proposed method and other methods.

Cover image and Capacity bits	Method name	PSNR	MSE
Baboon-90	U. Ali [5]	61.484	0.0202
	Proposed method	84.772	0.0002
	G. Maji [12]	71.597	0.0045
Mandi-250	Proposed method	82.970	0.0003
	R.Tavoli [10]	57.81	0.1075
Lena-981	Proposed method	69.537	0.0072

Table 5 represents the entropy for Mandi and Peppers (.bmp) in the cover image and stego-image.

Table V: Measure entropy for the cover image and stego-image.

Cover image	Size of Image(bits)	Entropy for cover image	Entropy for stego image
Mandi.bmp	768x508	7.1358	7.1358
Peppers.bmp	512 x 512	7.6698	7.6698

The last evaluation is a histogram which is comparisons between the original image and stego image will be used Mandi image and monarch as shown in Figure 7 which is the result stego image same of the histogram of the cover image.

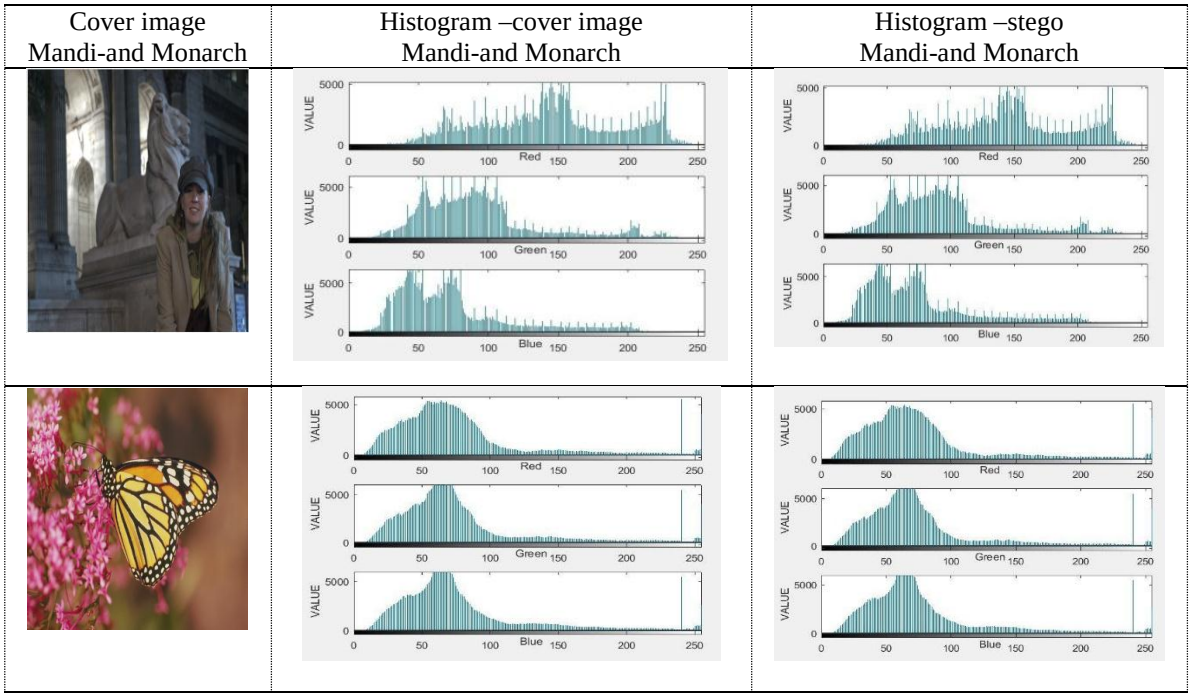

Figure 7: Comparisons histogram between the cover image and stego image.

8. Conclusions

In this paper, hybrid LSB and MSB based on color images (RGB) and using various image formats and different size images. Generally, LSB has been targeted in the systems of steganography, thus utilizing MSB provide more security to the system, the stego key is used for hiding information to restrict detection of secret message in an image which is an agreement between the sender and receiver. This method suggests using the value of MSB for check and will be hidden two-bit from LSB if MSB contains last 3 bit is 0 or hiding one bit if contain MSB last 3 bits is 1 which is hiding in the dark area more than the light area which is made not appear to human eye embed a message in image in another meaning not replace data in all bits in pixels just 2 bit or one bit and determine pixels location by using function curve sin which cannot hacker know pixel location, retains image quality by using 4 factors which is PSNR, MSE, Payload, Histogram. PSNR is high when insert and MSE is less and evaluate histogram the result is identical between the original image and stego - image. The result of this paper when applying on the different image gives high PSNR of 87.141 and less MSE of 0.00012 when inserting message 80 bits and reduction value PSNR of 72.023 and MSE of 0.0040 when inserting message 1200 bits and measure entropy is the same value for cover image and stego –image then this method increases security and complexity compared with the traditional method. This proposed method gave better value and more secure, that could not hacker estimate the pixel location and how to embed data by using LSB and MSB bits.

References

[1] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "Simple and secure image steganography using LSB and triple XOR operation on MSB," in 2018 International Conference on Information and Communications Technology (ICOIACT), pp.191-195, 2018.

[2] S.H.K.Manoj, G.S.K. Chetan, "The Various Applications of securing Communication Data with the help of Steganography," International Journal of Engineering and Techniques. Vol. 4, pp. 247-250, 2018.

[3] A. U. Islam et al., "An improved image steganography technique based on MSB using bit differencing," in 2016 Sixth International Conference on Innovative Computing Technology (INTECH), pp. 265-269,2016.

[4] N. Singh, "High PSNR based Image Steganography," International Journal of Advanced Engineering Research and Science, Vol. 6, No. 1, 2019.

[5] U. Ali, M. Sohrawordi, and M. P. Uddin, "A Robust and Secured Image Steganography using LSB and Random Bit Substitution," Am. J. Eng. Res.AJER, No. 8, pp. 39-44, 2019.

[6] [6] M. S. Taha, M. S. Rahim, S. A. Lafta, M. M. Hashim, and H. M. Alzuabidi, "Combination of Steganography and Cryptography: A short Survey," in IOP Conference Series: Materials Science and Engineering, Vol. 518, No. 5, p. 52003, 2019.

[7] A. Sharma, M. Poriye, and V. Kumar, "A Review of Image Steganography Techniques: Development Trends to Enhance Performance," International Journal of Advanced Research in Computer Science, Vol. 8, No. 5, 2017.

[8] Y. Y. Wai and E. E. Myat, "Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image," International Journal of Engineering Trends and Applications, Vol. 5, No. 4, 2018.

[9] A.M.Aye,"LSB Based Image Steganography for Information Security System," International Journal of Trend in Scientific Research and Development (IJTSRD),Vol. 3, pp.394-400,2018.

[10] R. Tavoli, M. Bakhshi, and F. Salehian, "A New Method for Text Hiding in the Image by Using LSB," Int. J. Adv. Comput. Sci. Appl., Vol. 7, No. 4, pp. 126-132, 2016.

[11] C. G. Tappe and A. V Deorankar, "An Improved Image Steganography Technique based on LSB," International Research Journal of Engineering and Technology (IRJET), Vol. 4, No. 04, 2017.

[12] G. Maji, S. Mandal, S. Sen, and N. C. Debnath, "Dual image based LSB steganography," in 2018 2nd International Conference on Recent Advances in Signal Processing, Telecommunications & Computing (SigTelCom), pp. 61-66,2018.

[13] M. A. Al Mamun, S. M. Alam, M. S. Hossain, and M. Samiruzzaman, "A Novel Image Steganography Using Multiple LSB Substitution and Pixel Randomization Using Stern-Brocot Sequence," in Future of Information and Communication Conference, pp. 756-773,2020.

[14] T. K. Hazra, M. Haldar, M. Mukherjee, and A. K. Chakraborty, "A Survey on Different Techniques for Covert Communication Using Steganography," *J.O.C.Eng.*, Vol. 20, pp. 42–52, 2018.

[15] N. A. H. Rustom and N. A. Farah, "A Review in Using Steganography Applications in Hiding Text Inside Digital Image (BMP)," *International Journal*, Vol. 7, No. 1, 2017.

[16] T. Pandikumar and T. Gebreslassie, "Information Security using Image based Steganography," *Int. Res. J. Eng. Technol.*, Vol. 3, No. 06, 2016.

[17] A. ALabaichi, M. A. A. Al-Dabbas, and A. Salih, "Image steganography using the least significant bit and secret map techniques.," Int. J. Electr. Comput. Eng., Vol. 10, 2020.