International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 1, February 2020, pp. 809~815
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp809-815

Hide text depending on the three channels of pixels in color images using the modified LSB algorithm

Rusul Mohammed Neamah, Jinan Ali Abed, Elaf Ali Abbood
Computer Department, Science College for Women, University of Babylon, Iraq

Article Info

Article history:

Received Feb 4, 2019
Revised Sep 25, 2019
Accepted Oct 10, 2019

Keywords:

Encryption
LSB algorithm
MSE and PSNR
Secret key
Xnor gate

ABSTRACT

At the moment, with the great development of information and communications technology, the transfer of confidential and sensitive data through public communications such as the Internet is very difficult to keep them from hackers and attackers. Therefore, it is necessary to work on the development of new and innovative ways to transfer such information and protect it to ensure that it reaches the desired goal. The goal of a new technique to hide information design not only hides the secret message behind the center cover, but it also provides increased security. The most common way to transfer important and confidential data is through embedding it into cover medium files in a way that does not affect the accuracy of the carrier file, which is known as hiding. In this paper, encryption and concealment techniques were used to protect data transferred from attackers. The proposed method relied on encryption of confidential information using the encryption key and the Xnor gate, after which the encrypted information was hidden in a color image using the LSB algorithm. The method of concealment depends on the extraction of chromatic channels of three RGB for each pixel and specifying the channel in which the bit of the encryption message will be hidden. Some metrics have been adopted to measure the quality of the resulting picture after hiding as PSNR and MSE, and achieve good results.

Corresponding Author:

Rusul Mohammed Neamah,
Computer Department, Science College for Women,
University of Babylon,
Babylon, Iraq.
Email: rusulneamah@gmail.com

1. INTRODUCTION

At the existing time, the security of data and information transmission over the Internet has become a vital concern and a vital issue. With the advancement of information and communication technology, and means of storage and exchange of information in different ways or so-called data transmission across the network starting with one site then onto the next, it became necessary to protect this information from the risks threatened by hackers and assailants. Therefore, work on developing the methods used to transfer confidential and important data to avert their access to the hands of attackers' intruders through communications, and to ensure the authenticity and security of these communications has become very important.

There is principally having two vital fields accessible for information security in mystery correspondence: cryptography and data hiding. Cryptography is a system in which the mystery information is mixed and the mystery message will be separated effectively just by the ideal beneficiary who has the secret key [1].Steganography is a branch of information hiding, which includes two sub-sections are the watermark and data management, which is through the concealment of confidential data in other files such as image files

or video files or audio or text files. Anyone can find two parties communicating secretly with encryption but he will not understand unless he knows the mystery key. In any case, in Steganography, the unintended beneficiaries won't whine that there is secret information in the cover medium on the grounds that the information in the cover medium ought not to be seen by any means.

The three features of steganography are indistinctness, limit (implanting payload), and strength (required against basic assaults). Limit is managed by the number of secret bits inserted in each cover pixel. A higher limit could embed progressively secret data into the cover picture. Impalpability is typically estimated by pinnacle motion to-clamor proportion (PSNR). The higher PSNR esteem is, the better stego picture quality is. Power intends to keep the secret information from being assaulted or stolen. There is a principal trade-off between limit, strength and subtlety in steganography system [2]. The method of concealment based on LSB technology is good in imperceptibility, but the hidden data capacity is low because only one bit of confidential data is hidden in one pixel of the middle of the cover medium.

In this paper, we propose another steganography technique in light of modified version of LSB algorithm which uses one channel from three channels of that RGB pixel, the selection of a particular channel is done on the second bit of LSB bits of that RGB pixel. In addition, the secret information is encoded before embedding in selected channel by using Xnor gate and secret key agreed by the sender and recipient, thus obtaining different carrier pixels for the same input image and confidential data, this makes the algorithm more ambiguous, making it harder to detect confidential data on eavesdropping devices and attackers.

2. RELATED WORKS

Recently, the most popular and repetitive technique that has attracted many researchers for modification or hybridization the least significant bit technique in steganography images. Chakraborty, et. al., proposed hiding a secret data in the carrier photo by using modified median edge detection to select the area of carrier picture, the confidential data is then inclusion in the edge area of the cover picture [3]. Ahmed T, Thahab proposed Burrows Wheeler Transform used to divide the cover image into non-nested blocks before embedding and the confidential information is inclusion in each block according to their sequence in the output of the Burrows Wheeler Transform. The technique of hiding is based on the virtual bit, which is produced from MSB (the most significant bit) and LSB (the least significant bits) of the carrier pixel [4].

S. Rubab and M. Younus proposed algorithm to hide the text in any RGB image of any size using Huffman encryption and 2D Wavelet Transform [5]. Juneja and Sandhu also suggested the use of an edges-identification method. Pixels edges of the cover image are detected by advanced edge detection filter and messages are embedded in LSBs of the pixels utilizing pseudo-irregular numbers [6]. Ashwini B. Akkawar and Komal B. Bijwe are implemented LSB and Link List method to include text or image in 24-bit color images [7].

Jung and Yoo proposed merging interpolation and LSB substitution for information hiding. Interpolation method, a preprocessing of cover images for getting better capacity and quality, scales up and down the cover image, whereas LSB substitute method is then applied for embedding [8]. Amanpreet Kaur and Sumeet Kaur proposed algorithm to hide text image file in the cover image by using edge detection algorithm because of the embedding capacity is more compared with smooth areas, they created hybrid edge detection by a combination of canny edge detection and a fuzzy edge detector and using it with 2k correction method [9].

Youssef Bassil proposed a steganography technique that substitute the three LSBs of every color channel of the pixels specified by the canny edge detection algorithm as a part of the perimeters inside the cover picture with secret data [10]. Youssef Taouil and El Bachir Ameur introduced a technique of concealing information depend on the separation of the wavelet Faber-Schauder. A merging of the confidential information is carried out in Least Significant Bit (LSB) of the integer part of the wavelet coefficients. Confidential data is degraded into couples of bits, subsequently each couple is changed into another couple on the basis of replacement which allows to get the most conceivable matches between the data and LSB of coefficients [11].

Wisam Abed Shukur and Khalid Kadhim Jabbar suggested that the Dev.-PSO algorithm be used to determine the optimal paths to reach the desired targets in the specified search space based on their disposal. The agency group is used to determine the process of the desired goals in the search space to resolve the problem [12]. Sahib Khan and Tiziano Bianchi suggested an Ant colony optimazation (ACO) to hide secret data it is used to discover complicated region of cover picture, after which least significant bits (LSB) exchange is used to hide the confidential information in pixels of the detected complex areas [13].

Saad Ahmed, Rabeea Jaffari and Liaquat Ali Thebo the work proposed to get better algorithm that uses the pixel value gauge technology to hide the confidential message in the most important bits (MSBs) of the cover picture [14]. Xintao Duan et.al proposed a new plan to hide information depend on U-Net

architecture. At start, in double traineeship, the training deep neural network contains an invisible network and a recover network; then, the transmitter uses the lurking network to imply the confidential picture into a whole picture without any moderation and send it to the recipient [15]. Zhiguo Qu, Zhenwen CHENG and Xiaojun Wang proposed two different implying style. One implying methodology is single pixel-inserted coding, referred to as SPE secret writing for brief, the second embedding methodology is that the multiple pixels inserted coding, referred to as MPsE coding [16].

Namita Tiwari and Madhu Shandilya two suggested ways to show RGB image information, one is the pixel pointer technology and the other is a triple algorithm A. It uses the same LSB principle, where the confidentioal data is hidden in the least significant bit of pixels, with more randomness in selecting the number of bits used and the color channels used [17]. Hasan Abdulrahman, Marc Chaumont et.al proposed information analysis based on color correlation and machine learning classification [18]. Hasan Abdulrahman et.al work proposed two kinds of features, calculated between the color picture channels. The first type of feature reflects local Euclidian shifts, and the second reflects the mirror shifts [19]. Mustafa Cem Kasapbas and Wisam Elmasry work proposed implying encrypted data and address information is used to use the Fisher-Yates Shuffle algorithm to locate the next pixel. To hide one byte, least significant bits (LSB) is hard-done by for all color channels in the chosen pixels [20].

Mervat Mikhail, Yasmine Abouelseoud and Galal Elkobrosy proposed technique uses two independent chaotic sequences to determine where data bits are inserted in the carrier picture using a modified version of the least important bit method (LSB). The message bits are implied using the LSB 3-3-2 insert method for the messy pixel selected for the carrier image [21]. Ketaki Bhaskar, Mitali Bakale, Priyanka Chaure and Priti Shirke proposed Huffman, zigzag and OPAP techniques are used to prevail over size limits and provide both high embedding magnitude and stunning stego-image deficiencies. Text data can be included in the carrier photo [22].

Venus and Rachna work proposed a new random coding method to hide information with pictures. In this method, the user can randomly hide text or picture across pixels in a canvas photo file [23]. S.Vimala, M.Rajakani and Uma Poomi the proposed work uses Absolute Moment Block Truncation Coding (AMBTC) method conceal data as part of the pressed picture [24]. Munesh Kumar et.al proposed work hide files (text file, audio file, etc.) using the LSB and AES algorithm where AES uses the password protection system and so on if anybody can find a stego picture they cannot read a letter because information is as yet in the encryption model and LSB is used to conceal the information [25].

3. THE PROPOSED METHOD

In our proposed method, two processes inside concealing stage (channel selection and inserting data) run simultaneously for embedding or inserting text message into an image. The selection process occurs by taking three RGB channels per pixel and two bits of LSB bits for these three bytes (each of red, green and blue channels) of this pixel. The second bit acts as an indicator that specifies the channel path to hide bits of the encrypted message while the first bit is replaced with the bit of the encrypted message. Before embedding, the secret message is processed by encryption using the encryption key and the application Xnor gate. After selecting the proper channel, now the encryption message bits are hiding in the selected channel using encoding, the bits of the encrypted message are replaced with the first bit of the LSB bits in the selected channel. In this way, the encrypted message is included in the entire image of the cover.

Once the embedding process is completed, the image is transformed into a stego-image. Note that the following schematic diagram in Figure 1, depicts the entire concept briefly. During the extraction process, each pixel of the stego image is converted to a byte array of RGB channels where the second bit of LSB bits from the three bytes specifies the channel that contains the encrypted message bit. Finally, the first bit value of LSB bits of selected channel indicates the desired encryption message bit. In this way, the entire message is being obtained by assembling all the bits of the encrypted message. Then, the Xnor gateway is applied using the same encryption key to obtain the confidential message bits. Figure 2, displays the schematic diagram of the proposed extraction technique. In this proposed method uses 24-bit RBG images as cover images. Like this type of images, each pixel consists of 3 bytes that specifies the light intensity of red, green and blue channels in that pixel.

3.1. Data embedding algorithm

Algorithm of the embedding process

1. Read the secret message and encryption key.
2. Perform the Xnor encoding on the secret message.
3. Read the cover image.
4. Selection of one of three RGB channels based on second bit of LSB bits of three channels in decimal and return in B_s.
   4a- If (B_s mod 3) =0

Then Red channel is selected.
4b- If (B_s mod 3) = 1
Then Green channel is selected.
4c- If (B_s mod3) =2
Then Blue channel is selected.

5. Apply the LSB algorithm to the selected channel and coding by storing the encrypted bit instead of the first bit of LSB bits.
6. Stego image is achieved.

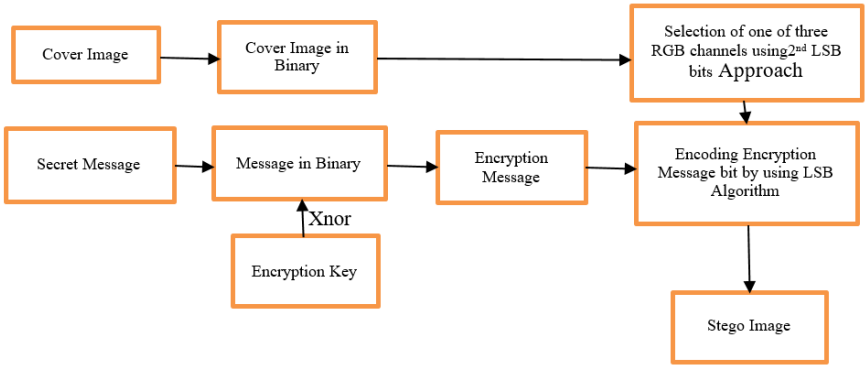

Figure 1. General structure of the proposed coding technology

3.2. Data extraction algorithm

Algorithm of Extraction

1. Get stego image.
2. Selection of one of three RGB channels based on second bit of LSB bits of three channels in decimal and return in B_s.
   2a- If (B_s mod 3) =0
   Then Red channel is selected.
   2b- If (B_s mod 3) = 1
   Then Green channel is selected.
   2c- If (B_s mod 3) =2
   Then Blue channel is selected.
3. Apply the LSB algorithm on the selected channel to get the encrypted message bits.
4. Input the encryption key and applied Xnor decoding on encryption message bits.
5. The secret message is obtained.

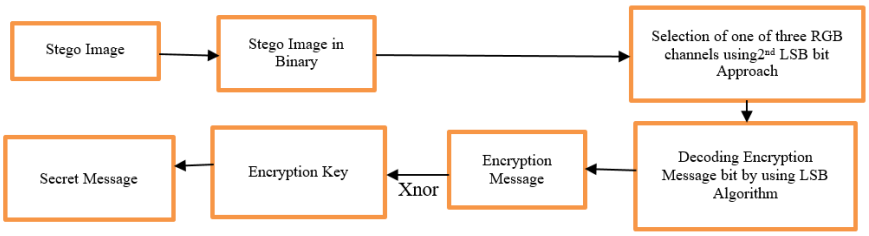

Figure 2. General structure of the proposed extracting technique

In order to clarify the method of concealment, we assume that the bits of the secret message is 10011010 and encryption key is 01011100 and the message after encryption by Xnor gate is 00111001, the first four bits of the encryption message will be taken (0011) and taken four pixels of the image cover, every pixel contains a red, green and blue channel. The first bit of the message is 0 will be hidden in one of the channels of the first pixel. The second bit of LSB bits for these three channels is 101 = 5 and after applying the

modulus arithmetic (5 mod 3), the result is 2. Note that the modulation 3 specifies the number of the channel in which the bit of the encrypted message will be hidden. Therefore, according to the proposed algorithm, the blue channel will be selected to embed the bit from encrypted data. Now, bit of the encrypted data will be exchanged with the first bit of LSB bits in the selected channel (a blue channel). In this way, the first bit of the encrypted message has been hidden. In the same way, the rest of the encrypted message bits (2nd, 3rd and 4th bits) are hidden in 2nd, 3rd and 4th pixels. Table 1, explains this process.

To illustrate how to retrieve encrypted message bits from stego-image with an example, we take the four stego-image pixels from previous encoding steps as shown in Table 1. The 2nd bit of LSB is 1012=510 and after module it with 3 the result is 2. Therefore, the first bit of the encrypted message can be found in the blue channel 0. In the same way, the bits of other encrypted message can be extracted from the rest of the pixels. Table 2 illustrate decoding process. After extracting encrypted message bits, now we can implement the Xnor gate using the same encryption key in order to get the original message bits. From Table 1 and Table 2, that same message bits were collected before the encryption and decryption process.

Table 1. Include encrypted messages using the suggested encoding algorithm

Pixel	Channel	Channels' Value in Binary(Cover Image)	2nd LSB of Three Channels	Selected Channel	Message Bit	Channels' Value in Binary(Stego image)
1st	R	11011010	$101_2=5_{10}$	2 B	0	11011010
	G	10010101				10010101
	B	10011011				10011010
2nd	R	01110011	$110_2=6_{10}$	0 R	0	01110010
	G	00000111				00000111
	B	11001100				11001100
3rd	R	11000100	$010_2=2_{10}$	2 B	1	11000100
	G	01001110				01001110
	B	10110000				10110001
4th	R	10001100	$001_2=1_{10}$	1 G	1	10001100
	G	10001000				10001001
	B	01111110				01111110

Table 2. Retrieving encrypted message using proposed decoding algorithm

Pixel	Channel	Channels' Value in Binary(Stego Image)	2nd LSB of Three Channels	Selected Channel	Message Bit
1st	R	11011010	$101_2=5_{10}$	2 B	0
	G	10010101			
	B	10011010			
2nd	R	01110010	$110_2=6_{10}$	0 R	0
	G	00000111			
	B	11001100			
3rd	R	11000100	$010_2=2_{10}$	2 B	1
	G	01001110			
	B	10110001			
4th	R	10001100	$001_2=1_{10}$	1 G	1
	G	10001001			
	B	01111110			

4. RESULTS

The proposed technique is implemented in matlab 7.12.0 using windows version 7 with word file different number of letters. This work simulated using jpeg format color image of 512*512. To determine the effectiveness of the proposed technology to conceal confidential information, there are measures through which the efficiency of the method is determined. The most common methods are MSE "Mean-Squared Error" and PSNR "Peak Signal-to-Noise Ratio". Mean-Squared Error: the MSE represents the total quadratic mistake between the original image and the stego image, it is determined as in the following equation.

$$\text{MSE}=\frac{1}{mn}\sum_{x=0}^{m-1}\sum_{y=0}^{n-1}[I(x,y)-K(x,y)]2 \quad (1)$$

Where m and n represent the height and width of the images respectively. I (x, y) and K (x, y) signify pixel value of cover and stego images respectively. PSNR (Peak Signal-to-Noise Ratio) is a statistical measure used as a standard model for evaluating different types of image quality assessment methods. PSNR is an estimated in decibel (dB) and is calculated:

$$PSNR=10\log10\left(\frac{255^2}{MSE}\right) \quad (2)$$

The experimental results display that the proposed technique achieves agreed concealment ability with minimal distortion. Table 3 shows the expected calculations for the MSE and PSNR measurements during the application of the proposed technique on 512x512 images and various volumes of confidential texts.

Table 3. It shows the results of MSE and PSNR when applying the proposed method on different images and different sizes of secret messages

Color image size(512*512)	Secret text 4700bits		Secret text 14500bits		Secret text 24250bits	
	MSE	PSNR	MSE	PSNR	MSE	PSNR
Airplane	0.0457	60.44	0.0448	55.54	0.0445	52.84
Lina	0.0336	61.74	0.0347	56.75	0.0339	53.65
Peppers	0.0879	57.65	0.0865	42.84	0.0862	39.99
Baboon	0.0740	58.39	0.0732	42.84	0.0729	40.89

Figure 3, demonstrates the cover and comparing stego image after hiding confidential 24250 bit text in 512x512 from Lina's image with color histogram plots for each of the three channels. It is seen that there are little contrasts in the histograms of cover and stego image of Lina. For other images, similar characteristics are gotten.

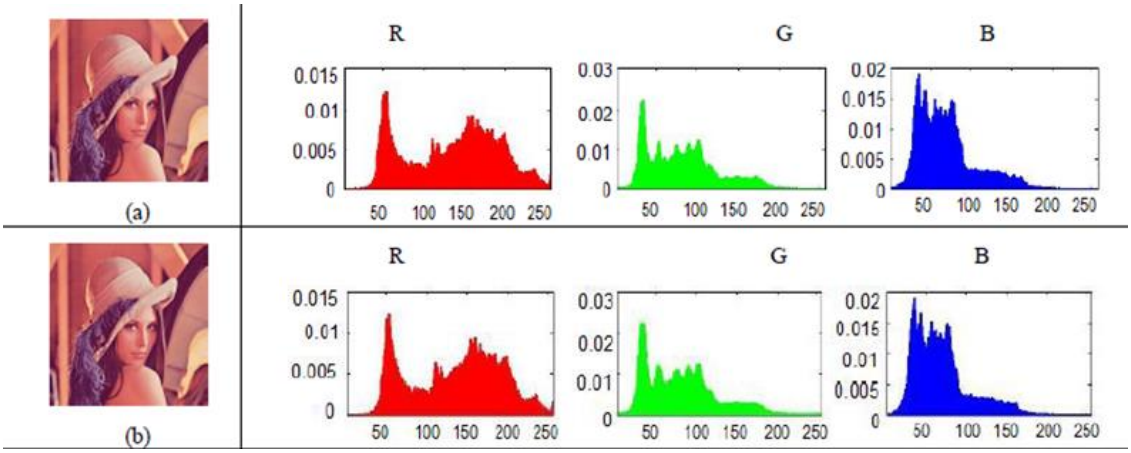

Figure 3. (a) The original Lina image and RGB histogram, (b) The stego image and RGB histogram

5. CONCLUSION

The main objective of developing methods of concealing information when transferred over the Internet is to increase the efficiency and security of these methods to protect them from hackers and attackers. In this paper, we used color images and extracted the three RGB channels per pixel. Using the second bit of bits LSB for each channel is specified in which channel the encrypted message bit is hidden by replacing the first bit of LSB bits with the bit of the encrypted message so that all bits of the encrypted message has been hidden inside the cover image. This method gives good results in terms of measuring the resulting image res olution after hiding and comparing it to the original image.

REFERENCES

[1] B. Schneier, "*Applied Cryptography: Protocols, Algorithm and Source Code in C*," Second Edition, Wiley 2nd Edition, 996.
[2] Johnson N., Duric Z., and Jajodia S., "*Information hiding: Steganography and watermarking -attacks and countermeasures*," Boston, MA: Kluwer Academic Publishers, 2001.
[3] S. Chakraborty, A. S. Jalal and C. Bhatnagar, "LSB Based Non Blind Predictive Edge Adaptive Image Steganography," *Multimedia Tools and Applications*, pp. 1-15, 2016.

[4] Ahmed T. Thahab, "A Secure Image Steganography based on Burrows Wheeler Transform and Dynamic bit Embedding," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 1, pp. 460~467, Feb 2019.
[5] S. Rubab, M. Younus, "Improved Image Steganography Technique for Colored Images Using Huffman Encoding with Symlet Wavelets," *International Journal of Computer Science*, vol. 9, no. 1, pp. 194-196, 2012.
[6] M. Juneja and P. S. Sandhu, "An Improved LSB Based Steganography Technique for RGB Color Images," *International Journal of Computer and Communication Engineering (IJECE)*, vol. 2, pp. 513-517, 2013.
[7] Ashwini B. Akkawar and Komal B. Bijwe, "Hybrid Approach for Embedding Text or Image in Cover Images" *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 5, no. 5, May 2016.
[8] K. H. Jung and K. Y. Yoo, "Stenographic Method Based on Interpolation and LSB Substitution of Digital Images," *Multimedia Tools and Applications*, vol. 74, pp. 2143-2155, 2014.
[9] Amanpreet Kaur, Sumeet Kaur, "Image Steganography Based on Hybrid Edge Detection and 2k Correction Method," *International Journal of Engineering and Innovative Technology*, vol. 1, no. 2, pp. 167-170, 2012.
[10] Youssef Bassil, "Image Steganography based on a Parameterized Canny Edge Detection Algorithm," *International* Journal of Computer Applications, vol. 64, no. 4, pp. 35-40, 2012.
[11] Youssef Taouil and El Bachir Ameur "Steganographic Scheme Based on Message-Cover matching" *International Journal of Electrical and Computer Engineering (IJECE)*, Vol. 8, No. 5, pp. 3594 – 3603, October 2018.
[12] Wisam Abed Shukur and Khalid Kadhim Jabbar "Information Hiding using LSB Technique based on Developed PSO Algorithm" *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.8, No.2, pp. 1156~1168, April2018.
[13] Sahib Khan and Tiziano Bianchi, "Ant Colony Optimization (ACO) based Data Hiding in Image Complex Region," *International Journal of Electrical and Computer Engineering (IJECE)*, Vol.8, No.1, pp. 379~389, February 2018.
[14] Saad Ahmed, Rabeea Jaffari and Liaquat Ali Thebo, "Data Hiding Using Green Channel as Pixel Value Indicator" *International Journal of Image Processing (IJIP)*, Volume (12), Issue (3), 2018.
[15] Xintao Duan, Kai Jia , Baoxia Li , Daidou Guo , En Zhang and Chuan Qin "Reversible Image Steganography Scheme Based on a U-Net Structure" *IEEEAccess volume 7* ,pp. 9314-9323 January 7, 2019.
[16] Zhiguo Qu, Zhenwen CHENG and Xiaojun Wang "Matrix Coding-Based Quantum Image Steganography Algorithm" *IEEE*, Volume 7, pp. 35684-35698 January 23, 2019.
[17] Namita Tiwari and Madhu Shandilya "Secure RGB Image Steganography from Pixel Indicator to Triple Algorithm-An Incremental Growth" *International Journal of Security and Its Applications*, Vol. 4, No. 4, October, 2010.
[18] Hasan Abdulrahman, Marc Chaumont, "Philippe Montesinos and Baptiste Magnier Color Images Steganalysis Using RGB Channel Geometric Transformation Measures Security Comm.," *Networks* 00:1–12, 2015.
[19] Hasan Abdulrahman, Marc Chaumont, Philippe Montesinos and Baptiste Magnier "Color images steganalysis using rgb channel geometric transformation measures" *Security And Communication Networks*, Vol. 9, pp. 2945-2956, 4 February 2016.
[20] Mustafa Cem Kasapbas and Wisam Elmasry "New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check" *Sadhana*, 43:68, (2018).
[21] Mervat Mikhail , Yasmine Abouelseoud and Galal Elkobrosy "Text Hiding in a Digital Cover Image using Two Dimensional Indexing based on Chaotic Maps" *International Journal of Computer Applications* (0975 - 8887) Volume 138 - No.12, March 2016.
[22] Ketaki Bhaskar, Mitali Bakale, Priyanka Chaure and Priti Shirke "Image Steganography for data hiding Using Huffman code, Zigzag and OPAP" *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, Volume 4, Issue 6, December 2015.
[23] Venus and Rachna, "Implementing Random Encoding for Image Steganography" *International Journal of Science and Research (IJSR)*, Volume 5 Issue 7, July 2016.
[24] S.Vimala, M.Rajakani and Uma Poomi "Steganography using Absolute Moment Block Truncation Coding" *International Journal of Advanced Engineering Research and Science (IJAERS)*, Vol-3, Issue-5 , May- 2016.
[25] Munesh Kumar, Gaurav Yadav, Ashish Kumar Keshari and Sandhya Katiyar "Image Processing using Steganography" *International Journal of Engineering Science and Computing*, Volume 7 Issue No.4, pp. 10619-10624, April 2017.