IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Novel Gray Code based Image Steganography Model for Covert Communication

Sangeeta [1*], Kamaldeep Joshi[2], Jyoti Pandey[3], Rainu Nandal[4], Harkesh sehrawat[5]

[1,2,3,4,5] Computer science & Engg., UIET, Maharshi Dayanand University, Rohtak, India

[*]*Corresponding Author: Sangeetatomar777@gmail.com, Tel.: +918295886292*

Available online at: www.ijcseonline.org

Accepted: 22/Jun/2018, Published: 30/Jun/2018

***Abstract*—** In the steganography, data are covered in terms that prevent mystery data. It's for the most part intention is exchanging information starting with one area, then onto the next area. It implies disguised mystery information inside the other information in a way that a pundit can't discover the presence of genuine topics. In steganography we shroud data with a mixed media bearer i.e. picture, content, sound, video documents, and so forth. In this way, that eyewitness can't locate the concealed data which we need to send to the recipient. Steganography principle objective is to give heartiness, perceptibility, limit of shrouded information because of which it varies from different strategies, for example, watermarking and cryptography. In picture steganography we conceal our mystery information in the picture with the goal that the spectator can't feel its reality. Steganography need is that the cover picture must be accurately picked. A characteristic picture should not to be used, it is better for stenographer to make their own specific pictures. Disguising the mystery information in the pictures, different sorts of techniques are utilized as a part of which some are more grounded than others to hide the information. In this paper a new method is used by using the gray code. Firstly, select the pixels in which message is embedded and then these pixels convert into ASCII code and apply the gray code method in the 7th bits of pixels and encoded pixels. The main advantage is only one bit is changed in each step. This method makes extraction of real message difficult. If an attacker come to know about the secret message in an image then will be not able to know the real message as it has to be added in the 7th bit by changing the binary code to gray code.

Keywords— Steganography, LSB, Gray Code, ASCII Code, PSNR, *MSE*

I. Introduction

Steganography is basically used to cover the information within other information. Steganography is gotten from the Greek dialect "stages" signifies "cover" and "grafia" signifies" writing" use as secured composition. In the event that the mystery message identifies this innovation turns into a disappointment. The Viability of Steganography picks up by joining it with cryptography [14]. Steganography is being utilized over quite a while to trade mystery data starting with one place, then on to the next in numerous structures. Steganography is the workmanship that additional, conferring puzzle data in a legitimate medium transporter, e.g., picture, sound, and video files. It goes under the doubt that if the component is discernible, the intension of the strike is self-evident; in like manner the thought process is reliable to cover the presence of the real data. The more established and noted system for disguising the information in the computerized picture is LSB strategy. The LSB is the least complex strategy for concealing the information and generally utilized. In this technique the mystery information is covered up by changing just the last significant bit of the real picture [2]. Also, that is the reason there is no impact on the nature of the picture. Also, the disguising limit of the information can be expanded up to last four significant bits. Be that as it may, the principle disadvantage is effortlessly identified so that there are numerous alterations and changing to fortify the strategy is used time to time. Hiding the secret message is the major challenges in image steganography where the attackers used many types of stego analysis method that basis, they hack the data and break the privacy of the message [15]. So, we are using the gray code method by which we can add our message at the 7th bit of image and in this we add till +2,-2 in changing pixel, but our value can be changed up to 3. If an attacker wants to hack the secret message, then the message cannot be easily detected as we have added our message at the 7th bit by changing the binary code to gray code.

II. Literature review

Parvinder et al. expels the impediment of slightest critical piece strategy method by utilizing 6th and the 7th bit of pixel esteem for message addition. Yet, the possibility of message addition of pseudo irregular area utilizing calculation has been just 49% which in itself is a weakness. Regardless of each of the, one basic weakness of previously mentioned calculations for the addition and recovery of the message is the weight on particular bits (like the sixth and seventh piece

and so forth.) which makes the steganoanalysis simple. Here rather than LSB bits sixth and seventh piece of pixel esteems are utilized to shroud the mystery information inside a picture. This technique conquers the all disadvantages of the LSB addition strategy. However, it has its own particular disadvantage that the message bit will be embedded at pseudo random area at first occasion is less when contrasted with LSB [3].

S. Manaseer proposed a new method that is standard LSB and Condition Based LSB [5]. In this method last bit of the LSB is changed in the corner to corner. This technique changes the last bit or the second minimum last bit in light of the condition as takes after: If the most significant bit is 1, the calculation changes the second minimum Significant bit. Something else, the calculation changes the last bit. This procedure is more secure contrasted with others due to relying upon the reference of information; it conceals the reference not the genuine information.

K. Bailey et al. proposed the stego color cycle method; by this method the security of the data is increased. This technique is mainly used for the RGB images. In this technique data is concealed in different channels of the original image. This technique a cycle method is used, in that first secret bit is added in pixel 1 of the red channel and second added in the green and third added in the blue and continue till all bit is added [4]. But in this technique is problem that secret bit is added in a fixed cyclic manner and it is easily detected.

K. Joshi et al. proposed a new method for data hiding using 2-bit XOR that is dealing the picture (gray scale picture) which is 2 dimensional [6]. In this technique, vast measure of information can be concealed in light of the fact that 2 bits of information are concealed in one pixel. In that XOR activity is used in eighth bit, seventh bit, second and first bit of information. This proposed strategy likewise makes the stego picture of better quality and also gives the surety against assault.

K. Qazanfari et al. have proposed Histogram shifting method is utilized for graphical portrayal of picture. It shows the pixel value and thickness at a specific pixel. In this Pairs of peak points and zero focuses are utilized for accomplishing low installing distortion to give low information hiding limit. In histogram the most elevated esteem is called maxima and the least esteem is called minima. At the point when the pixel esteem is adjusted for implanting process it doesn't cross the minima and maximum limit. The quantity of the pixels constituting the top in the histogram of a cover picture is equivalent to the hidden limit [7].

P. Li et al. proposed a new technique of LSB-based steganography, by utilizing reflected Gray code for colored quantum pictures, and the hiding capacity of this method is up to 4 bits for each pixel. In this method, the mystery bit arrangement is considered as a succession of 4-bit portions. For the four bits in each portion, the first bit is inserted in the second LSB of B channel of the cover picture, and the staying three bits are implanted in LSB of RGB channels of each color pixel at the same time utilizing reflected-Gray code to decide the embedded bit of mystery data. Following the changing method, the LSB of stego-picture are not generally same as the mystery bits and the distinctions are up to right around half. Exploratory outcomes affirm that the proposed method demonstrates great execution [8].

A. Kumar Bairagi proposed a method of ASCII based cryptography with LSB based stegnography for the security reason for information exchange in the system and web. With this encryption are connec to the even or odd ASCII esteem of the character which specify to the information. A character in the plain content constantly changes to the ASCII code and including the key an incentive with it getting the figure content. This code is then changed over to the binary number furthermore, substitutes these bits in the LSB position in every pixel which portray the picture. On the contrary side, gather these bits from the picture and changing over this in a comparable decimal number which is the figure message and subtracting the key an incentive from it, we get the ASCII code of the plain content. Changing over this ASCII code to the comparable character portrayal, we get the first content (information). Typically, security examiner can easily discover the key, however in this approach a mix of two prime numbers is utilized for encryption [9].

C. Chan et al. proposed a LSB-based plan utilizing reflected-Gray code, which can be used to decide the implanted bits from mystery data. Following the changing rules, the LSBs of stego-picture are not generally equivalent to the mystery bits and the trial demonstrates that the distinctions are up to very nearly 50 %. As per the numerical finding and test comes about, the proposed plot has a similar picture quality and payload as the basic LSB substitution conspire. The proposed information, concealing plan on account of G1 (first bit Gray code) framework is proportionate to the basic LSB substitution method [10].

Chang et al. proposed a method to give bigger implanting limit and to limit the twisting of the stego-picture. This strategy misuses the relationship between neighboring pixels to assess the level of smoothness or difference of pixels. And the pixel is situated in the edge region; at that point it may endure bigger changes than those in smooth regions. The two-sided, three-sided, and four-sided side match strategies were used. The exploratory outcomes demonstrate that this strategy gives a substantial inserting limit without making perceptible twisting. In addition, the implanted information can be removed from the stego-picture without referencing the original picture [11].

Wu et al. purposed a new scheme that they are using the LSB replacement and pixel-value differencing (PVD) method. Initially, an alternate value of two successive pixels by using the PVD strategy is acquired. A little contrast value is situated on a smooth region and the bigger one is situated in an edged region. In the smooth regions, the mystery

information is covered up into the cover picture of the LSB technique while utilizing the PVD strategy in the edged regions. Since the range width is variable, and the zone in which the mystery information is hidden by LSB or PVD strategy are difficult to figure, the security level is the same as that of a solitary utilizing the PVD technique for the proposed technique. From the exploratory outcomes, contrasted and the PVD technique being utilized alone, the proposed strategy can shroud a substantially bigger data and keeps up a decent visual nature of stego-picture [12].

III. Proposed method

This proposed method is used to enhance the hiding security of the message. In this proposed method gray code technique is used. Firstly, select the pixels in which message is embedded and then these pixels convert into ASCII code and apply the gray code method in the 7^{th} bits of pixels and encoded pixels. When the message is inserted in the 7^{th} bit of the image, then the pixel value is changed less than or up to 2. Gray codes are also known as cyclic codes or unit distance codes in which the difference between the code groups differs only by 1. The main advantage is only one bit is changed in each step.

3.1 Embedded state

In embedded algorithm firstly, we take the binary stream of the watermark and select the length of the message that we want to send. After that select the cover image in which we add our secret message. In this we select the first pixel of images and convert into binary form. Apply the binary to gray code method and take the reference of 7^{th} bits of both pixel and the stego pixel. These bits are used as message bits according that bits we add pixel indicator value. Select next pixel until all pixels are read and so on.

Algorithm for embedded message

Input – Cover Image (I^c), Secret Message (K) , Secret Key($K^{key)}$

K= {k_1, k_2, k3…….k_n}

1. Initialize I^c ← Cover Image, K ← Secret Message
2. While Counter <= size of message block do
3. For each pixel
    a. Pick a pixel I (x, y) from the image and convert into eight bit binary number.
    b. Check the 7^{th} bit of pixel value of variable ‘N’ and ‘M’. (Where ‘N’ store the 7^{th} bit pixel value and ‘M’ store the converted pixel value by binary to gray code)
    c. Taken both value of N and M and after that compare with the message bit (message bit is stored in variable ‘k’.

4. If M=0 and N=0 then

If ‘k’ is ‘00’ then no change is required to the pixel value.
If ‘k’ is ‘01’ then +1 is added in the pixel value.
If ‘k’ is ‘10’ then -1 is added in the pixel value.
If ‘k’ is ‘11’ then +2 is added in the pixel value.
Else if M=0 and N=1 then
If ‘k’ is ‘00’ then -1 is added in the pixel value.
If ‘k’ is ‘01’ then no change is required to the pixel value.
If ‘k’ is ‘10’ then +2 is added in the pixel value.
If ‘k’ is ‘11’ then +1 is added in the pixel value.
Else if M=1 and N=0 then
If ‘k’ is ‘00’ then +1 is added in the pixel value.
If ‘k’ is ‘01’ then +2 is added in the pixel value.
If ‘k’ is ‘10’ then no change is required to the pixel value.
If ‘k’ is ‘11’ then -1 is added in the pixel value.
Else M=1 and N=1 then
If ‘k’ is ‘00’ then +2 is added in the pixel value.
If ‘k’ is ‘01’ then -1 is added in the pixel value.
If ‘k’ is ‘10’ then +1 is added in the pixel value.
If ‘k’ is ‘11’ then no change is required to the pixel value.

5. If k<=0
6. Choose next two bits of the message and select next pixel.
7. Counter =counter+1.
8. Repeat steps 3 to7.
9. End

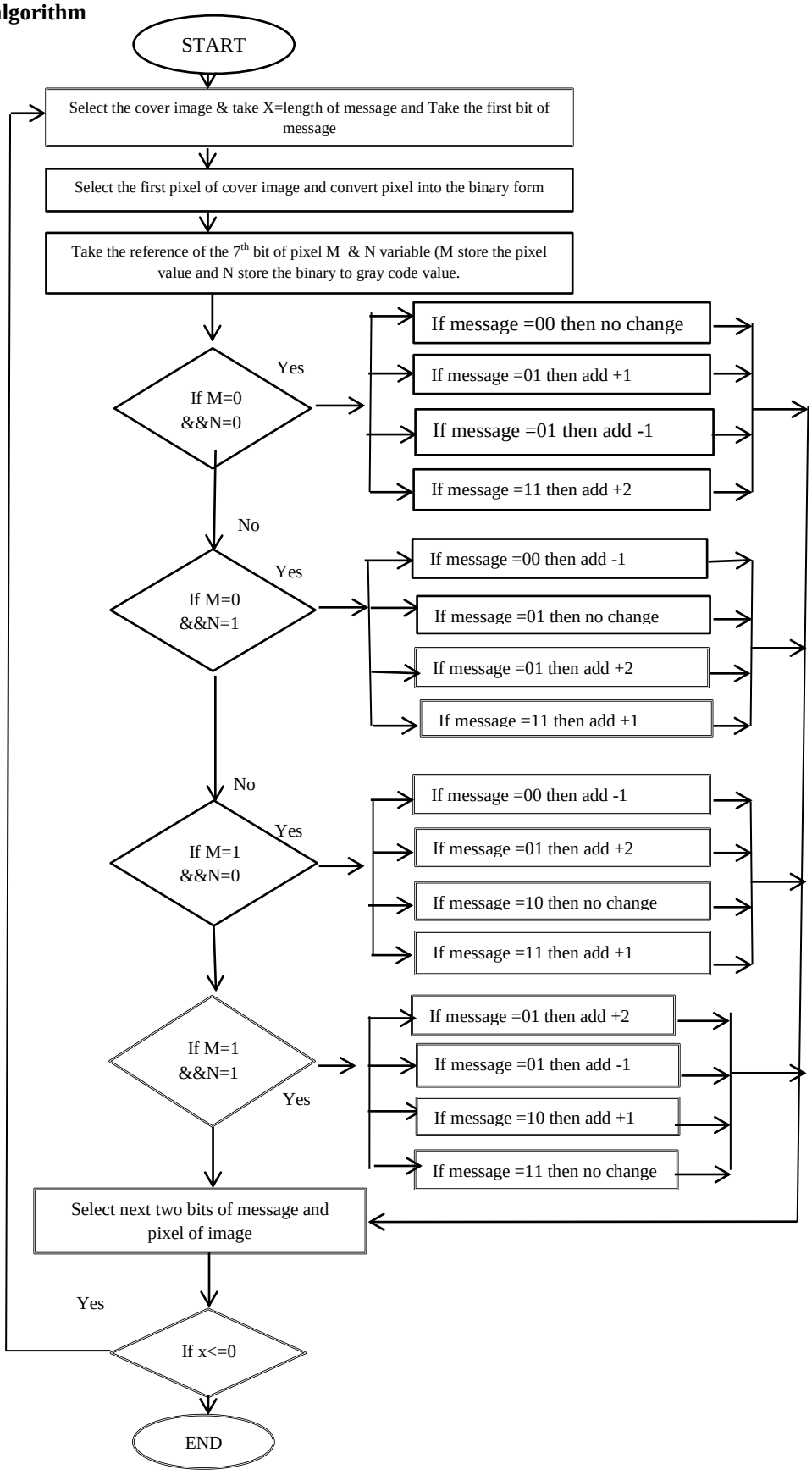
3.2 Extraction state

In extraction algorithm firstly, we take the stego image and select the first pixel of stego image and first message bit. After that convert the stego pixel into binary form and then apply gray to the binary code method. Select next pixel and apply above method until the message is retrieved.

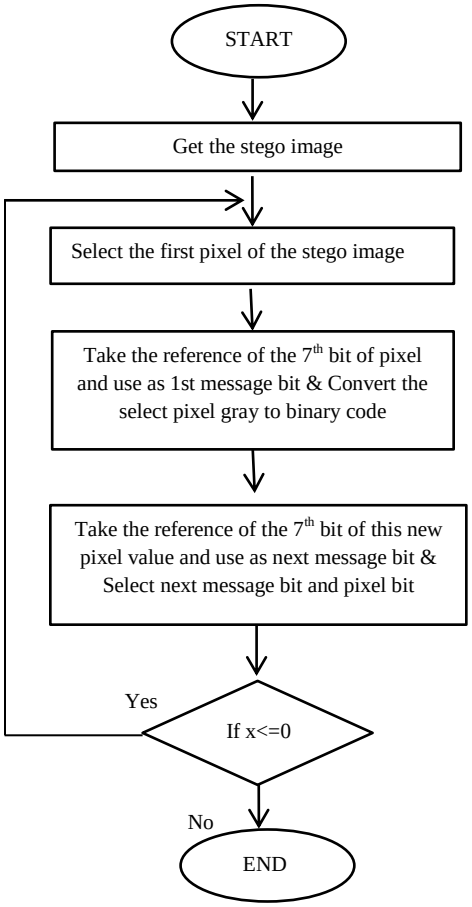
Input Stego Image (I^s), Secret Message (K), Secret Key ($A^{Key)}$

1. Initialize I^s ← Stego Image, K ← Secret Message
2. For each pixel
    a. Pick a pixel I^s (x, y) from the stego image and convert into eight bit binary number.
    b. Check the 7^{th} bit of pixel value of variable ‘A’ and ‘B’. (Where ‘A’ store the 7^{th} bit pixel value and ‘M’ store the converted pixel value by gray code to binary value)
3. These bits are used as our message bits.
4. Convert message bits into ASCII value to the original message.
5. Repeat step 2 to 4 until all the message bits are extracted.
6. End

3.3. Flowchart of embedded algorithm



3.4 Flowchart of extraction algorithm



IV. Example of proposed method

Let us assume that the secret message to be embedded is k = {11001001} and the four pixel values being selected are, p = {81, 93, 59, 76}.

At sender side's side:

First pixel P1 = 81 (01010001)

G1 = (01111001)

The 7th bit of P1 and G1 form the pair '00' but initial two message bits to be inserted are '11'. Therefore, we need to add +1 to the value of P1. Hence, P1' is 82(81+1). Where P1' is the stego pixel.

Now 2nd pixel, i.e. P2 = 93 (01010010)

G2 = (01110011)

The 7th bit of P2 and G2 form the pair '11' and 3rd and 4th message bits are '01'. Therefore, we need to add -1 to the value of P2. Hence, P2' is 92(93-1). Where P2' is the stego pixel.

Now 3rd pixel, i.e. P3 = 59 (00111011)

G3 = (00100110)

The 7th bit of P3 and G3 form the pair '11' and 5th and 6th message bits are '11'. Hence, a value of P3'=P3=59, Where P3' is the stego pixel.

Now 4th pixel, i.e. P4 = 76 (01001100)

G4 = (01101010)

The 7th bit of P4 and G4 form the pair '11' and 7th and 8th message bits are '01'. Therefore, we need to add +1 to the value of P4. Hence, P4' is 77 (76+1). Where P4' is the stego pixel.

Now, the value of pixels in the stego image that are transferred is P' {82, 92, 59, 77}

At receiver's side:

The set of selected pixels is P' {82, 92, 59, 77}

Now first pixel value of P1' = 82 (01010010)

G1'= (01100011)

The 7th bits combined to form a message bit '11'.

Now 2nd pixel value of P2' = 92 (01011100)

G2'= (01101000)

The 7th bits combined to form a message bit '00'.

Now 3rd pixel value of P3' = 59 (00111011)

G3'= (00101101)

The 7th bits combined to form a message bit '10'.
Now 3rd pixel value of P3' = 59 (00111011)
G3'= (00101101)
The 7th bits combined to form a message bit '10'.
Now 4th pixel value of P4' = 78 (01001101)
G4'= (01110110)
The 7th bits combined to form a message bit '01'.
Hence, the receiver's side received message stream is {11001001}.

V. Experimental results

To evaluate the performance of the proposed method, the algorithm is implemented by using the MATLAB R2017 a. Many different sizes and different types of images like gray and RGB are used for evaluating the performance of the proposed algorithm. PSNR is used to find out the degree of similarity between stego image and the original image [16]. PSNR is mainly defined by this formula:
$PSNR = 10. \log_{10} 255*255/MSE$

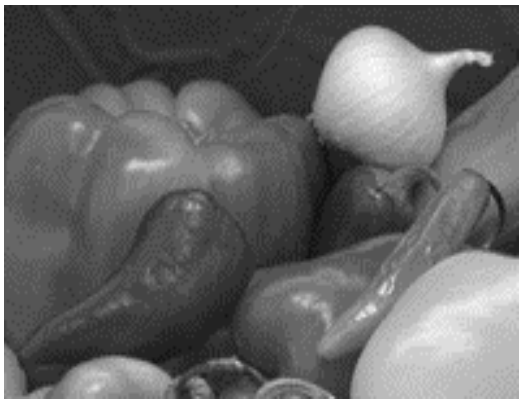
There are different types of comparisons are done on the basis of original image and stego image. In figure 1 shows the original image and stego image with their sizes. With these respects, we compare our proposed method. And Figure 2 shows the histogram of original and stego image. Table 1 shows the PSNR while using the different image with different sizes. It shows that our proposed method gives effective results [11]. Table 2 shows that comparison between our proposed method with other methods [10, 12].

Original image

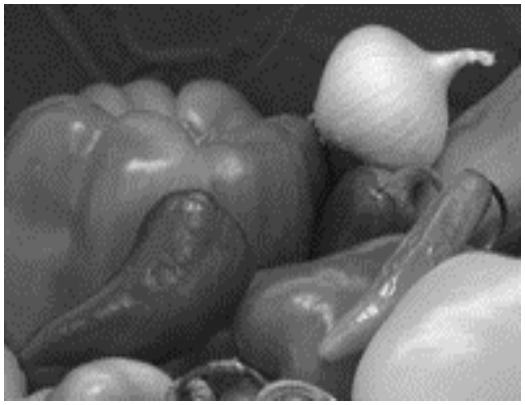
(a)
Image size 537*358 and its PSNR is 100.9712

Stego image

(b)
Image size 537*358 and its MSE is 2.08



(c)
Image size 135*198 and its PSNR is 89.3905



(d)
Image size 135*198 and its MSE is 1.122

(e)

Image size 291*240 and its

PSNR is 91.8012

(f)

Image size 291*240 and its

MSE is 8.5911

(g)

Image size 537*358 and its

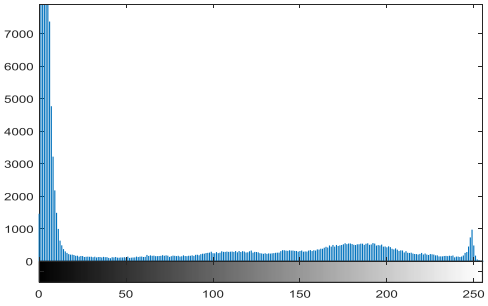
PSNR is 89.6580

(h)

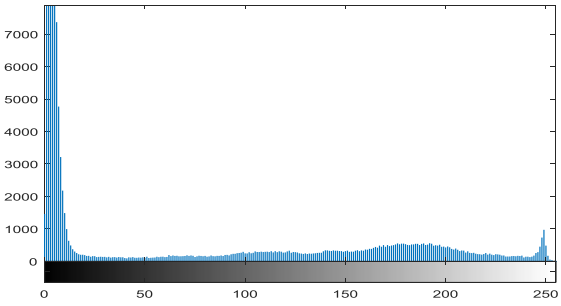
Image size 537*358 and its

MSE is 8.442

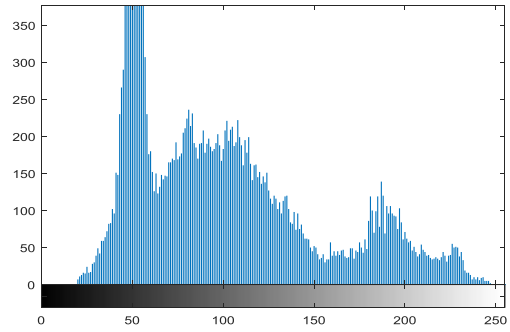
Figure: 1 Original and stego image



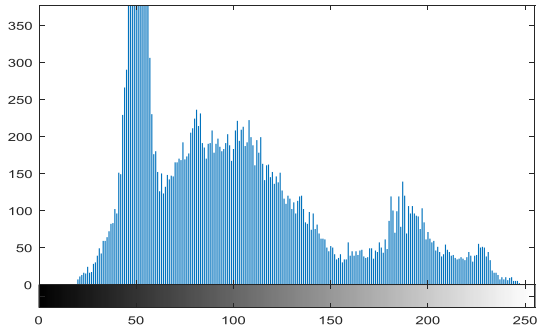
(a) Original Moon image histogram



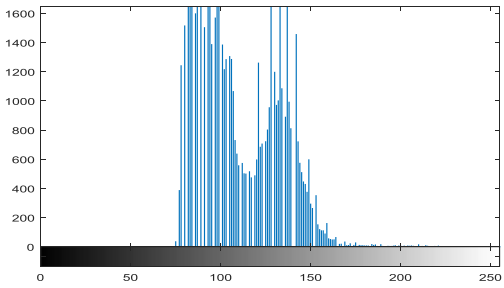
(b) Stego Moon image histogram



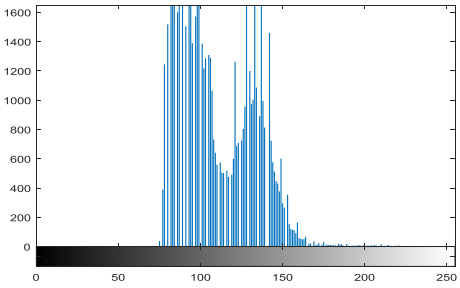
(c) Original Onion image histogram



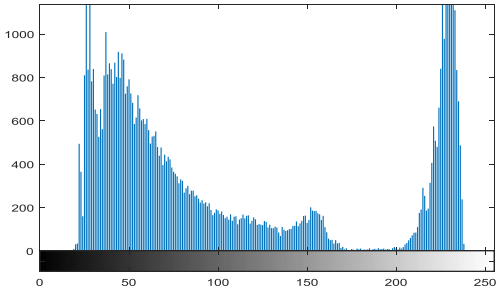
(d) Original Onion image histogram



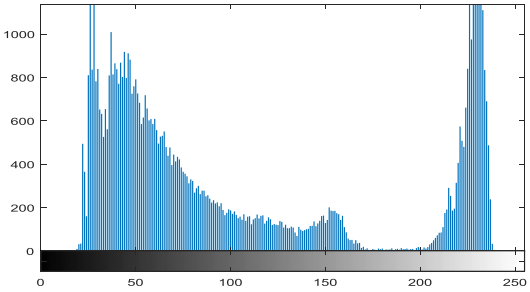
(e) Original Pout image histogram



(f) Stego Pout image histogram



(g) Original Autumn image histogram



(h) Stego Autumn image histogram

Figure: 2 Original and stego image histogram

Table: 1 Obtained PSNR at the different message size using different image size

Different Image with different sizes	PSNR of 4 bytes message size	PSNR of 8 bytes message size	PSNR of 16 bytes message size
Moon Image (537*358)	94.9488	90.9794	87.9591
Onion Image (135*198)	87.6296	84.6193	80.6399
Pout Image (291*240)	88.7903	87.0294	84.8109
Autumn Image (537*358)	88.8662	87.6168	84.3432
Rice Image (256*256)	89.3059	86.2956	84.5347
Glass Image (182*282)	92.1998	86.7591	83.4492

Table: 2 Comparison of proposed method with other methods

Algorithm	Proposed algorithm	Information hiding method (Faruq et al. method)[17]	Chang et al. method [10]	Side match (Tsang & Chang) [11]	PVD with LSB (Wu et al.) [12]
Operated Case	Pepper Image using different message size	(1) W=2 & P=32 (2) W=2 & P=64 (3) W=4 & P=20 (4) W=4 & P=32 (5) W=8 & P=16	(1) K=4 (2) K=6 (3) K=8	(1) Two-sided (2) Three-sided (3) Four-sided	(1) Case 1 (2) Case 2
PSNR	(1) 57.045 (2) 55.432 (3) 50.234 (4) 47.789 (5) 40.499	(1) 54.019 (2) 51.989 (3) 46.337 (4) 45.002 (5) 38.810	(1) 47.770 (2) 45.720 (3) 44.080	(1) 41.220 (2) 45.030 (3) 48.180	(1) 38.80 (2) 36.160
Capacity in bits	(1) 145,128 (2) 216,096 (3) 320,720 (4) 440,800 (5) 766,040	(1) 134,792 (2) 215,054 (3) 316,528 (4) 430,006 (5) 641,493	(1) 283,211 (2) 315,078 (3) 330,662	(1) 389,004 (2) 267,242 (3) 164,538	(1) 528,512 (2) 766,040

VI. Conclusion

There is a well-known fact that "Data hiding in image increases the crime in the real world". Steganography can be used as both legally and illegally. Good user uses it for securing communication while hacker uses it illegally to gain other data. Concealing the secret data in the images, various types of methods are used in which some are stronger than others to conceal the data. Steganography's definitive targets, which are imperceptibility, vigor (protection from different picture preparing strategies and pressure) and limit of the concealed information are the primary factors that differentiate it from related procedures, for example, watermarking and cryptography. Hiding the secret message is the major challenges in image steganography where the attackers used many types of stego analysis method that basis, they hack the data and break the privacy of the message. So, we are using the gray code method by which we can add our message at the 7^{th} bit of image and in this we add till +2,-2 in changing pixel, but our value can be changed up to 3. If an attacker wants to hack the secret message, then the message cannot be easily detected as we have added our message at the 7^{th} bit by changing the binary code to gray code. The LSB method also faces the same challenge regarding the selection of which bits are used for hiding the data without effect the actual image pixels. So, keeping in view the complexity and importance of the data hiding, researchers must keep on developing new prioritization techniques for data hiding.

References

[1]. S. Shahreza and M. Shahreza, "Steganographyin Textiles", 4th International Conference on Information Assurance and Security, Volume 3, Issue 6, pp. 5661, 2008.

[2]. S. Batra, R. Rishi and Rajkumar , "Insertion of Message in 6th, 7th and 8th bit of pixel values and its retrievals in case intruder changes the least significant bits of image pixels", International Journal of security and its applications, Volume 4,Issue 3, pp. 1-10, 2010.

[3]. Parvinder, S. Batra and H. Sharma, "Evaluating the Performance of Message Hidden in First and Second Bit Plane", W SEAS Transaction on Information International Journal of Computer Applications, Volume. 2, Issue. 86, pp. 1220- 1222, 2005.

[4]. K. Bailey, and K. Curran, "An evaluation of image based steganography methods", Multimedia Tools, Volume 2, Issue 2, pp. 55–88, 2006.

[5]. S. Manaseer, A. Aljawawdehand and D. Alsoudi, "A new Image steganography depending on reference & LSB", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 12, Issue 9, pp. 1950-1955, 2017.

[6]. K. Joshi, R. Yadav and G. Chawla, "An Enhanced method for data hiding using 2 bit XOR in image steganography", International Journal of engineering and technology, Volume 8, Issue 6, pp. 3043-3055, 2017.

[7]. K. Qazanfari, R. Safabakhsh, "A new steganography method which preserves histogram: generalization of LSB", International Journal of Engineering, Volume 277, Issue 7, pp. 90-101, 2017.

[8]. P. Li and A. Lu ,"LSB-based Steganography Using Reflected Gray Code for Color Quantum Images", International Journal of Theoretical Physics, Volume 57, Issue 5, pp. 1516-1548, 2018.

[9]. A. Kumar Bairagi, "ASCII based Even-Odd Cryptography with Gray code and Image Steganography: A dimension in Data Security", International Journal of Engineering, Volume 01, Issue 02, pp.2078-5828, 2011.

[10]. C. Chen, C. Chang, "LSB-Based Steganography Using Reflected Gray Code", IEICE - Transactions on Information and Systems, Volume E91-D, Issue 4, pp. 1110-1116, 2008.

[11]. Chang and Tsang ,"Performance Evaluation of a Steganographic Method for Digital Images Using Side Match", Conference on Innovative Computing, Information and Control, Volume 25, Issue 12, pp.1431-1437, 2006.

[12]. H.Wu, Tsai, N. Wu, Hwang**, "**Image steganographic scheme based on pixel-value differencing and LSB replacement methods**",** IEE Proceedings - Vision, Image and Signal Processing, Volume 152, Issue 5, pp.611-615, 2005.

[13]. K. Joshi and R. Yadav , "A New Method of Image Steganography using Last Three Bit Plane of Gray Scale Images", Indian Journal of Science and Technology, Volume 10,Issue 38, 2017.

[14]. K. Joshi and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication", Conference: Third International Conference on Image Information Processing, pp. 86-90, 2015.

[15]. M. Chaudhary, K. Joshi, R. Yadav, R. Nanda, "Survey on Image Steganography and its Techniques", International Journal of Engineering and Technology, 2017.

[16]. A Saini, K Joshi, K Sharma, R Nandal, "An Analysis of LSB Technique in Video Steganography using PSNR and MSE", International Journal, Volume 8, Issue 5, 2017.

[17]. A. Faruq and H.S. Ghwanmeh, "An innovative information hiding technique utilizing cumulative peak histogram regions", Journal of Systems and Information Technology, Volume 14, Issue 4, pp. 336-352, 2012.

