International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 5.143, Volume 02, No. 03, July - September, 2020, pp.271-280

AN IMPROVED IMAGE STEGANOGRAPHY TECHNIQUE USING MODIFIED DATA IMAGE

Dr. Satish Chand Singhal[*]

ABSTRACT

The science of secret communication is known as steganography. Steganography hides the secret data from unauthorized user. Unlike cryptography, steganography hides the existence of secret information rather than hiding its meaning only. Many different file formats can be use as cover media but these days the digital image based steganography is most popular on internet and web. The capacity of hiding secret data is limited in steganography and it depends on size of the cover image. There is a tradeoff between the stgo image quality and the capacity of steganography. Therefore, the quality of stego image and capacity of steganography are still a challenging field. In this paper, a new image steganography technique has been proposed. In this technique the secret data is change into a new format. The new data cannot be decoded without knowing the actual algorithm. In this new data, there is less counts of number of '1' compare to original data, due to this mostly the stego image's pixel value follows the cover image pixels value after using the XORing method between the cover image and the secret data. The count of number of '1' has been reduced by 20 %(nearly) compare to the original data. By using proposed method, not only the security of secret data increases but also it increases the quality of the stego image. The result shows that the proposed method improved the value of PSNR and MSE of the stego image and it fulfills all the aspects of image steganography.

Keywords: *Image Steganography, Data Image, PSNR, Stego Image*.

Introduction

In present days, internet is widely use for communication. Internet is very fast medium to send the information from one place to another place but there is some disadvantages of internet. By using internet the secret information can be hacked by hackers and they can be use these information for wrong purpose. To provide the security first of all watermarking and cryptography has been developed, in these techniques the secret information was changed into a new format.Unfortunately, sometimes it is not enough to keep the information secret, it may also be necessary to keep the existence of the information secret. The technique used to implement this is called steganography [4]. The term steganography was first coined by an occultist, namely Trithemius. The main aim in steganography is to hide the very existence of the message in the cover medium steganography includes a vast array of methods of secret communication that conceal the very existence of hidden information. Traditional methods include use of invisible inks, microdots etc. Modern day steganographic techniques try to exploit the digital media images audio, video etc.

Proposed Method

The higher embedding capacity or less mean square error (MSE) is the focal points of proposed method. The proposed algorithm converts the secret data image into a new format and embeds it into the RGB cover image By using this new secret data the output of steganography (stego image) have very fewer changes compare to cover image. Due to this higher PSNR and lower MES compare to simple

---

[G] Associate Professor, Department of Physics, Sri SantSuderdas Government Girls PG College, Dausa, Rajasthan, India.

LSB method have been achieved. The proposed algorithm has three phases. In the first phase, each pixel of the data image has been changed according to proposed method. After this phase, the resultant data image has less number of count of '1' so that it will increase the quality of the stego image. After the first phase, in second phase each pixel of the data image will break into 8 different sub pixels. In third phase firstly the cover image is broken into three planes RGB and then each pixel of these planes are XORing with each pixel of the data image of related planes (which is generated after second phase).

Phase One

In this section, the secret data image is used. First of all the data image is break into 3 planes these are red plane (D_R), green plane (D_G), blue plane (D_B). After breaking the data image, the format of each plane of the data image has been changed according to proposed method. For hiding the data image XORing method has been used, and the behavior of XOR gate shown in table 1.

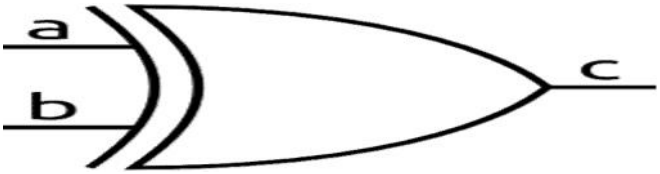


Figure 1 Symbol of XOR gate

Table 1: Truth Table of XOR gate

Input	Input	Output
A	B	C
0	0	0
0	1	1
1	0	1
1	1	0

According to truth table, if A= '0' then C= B and if A= '1' then C=inverse of B. Means in XOR gate if one input is '0' the output follows the other input, and if one input is '1' the output is inverse of other input. According to proposed method, the two inputs of XOR gate are the cover image pixels and the data image pixels. If the data image have been changed into a new format, so that output of XOR gate follows the cover image and the data image will also be hide in it. The proposed method is based on this phenomena, means if the data image has been changed into a new format, in which number of '1' is less compare to the original data image so that the output image or the stego image can follow the cover image. For converting the data image in a new format various steps are used. They are:

Step 1: Read first plane (red plane) of the data image and make a matrix with these pixels values.

Step 2: Take first element (A) of the matrix as the reference pixel.

Step 3: Take next element of the matrix (B).

Step 4: Compare the value of A and B and store the output in a new matrix called C.

- If B > A then C= 192 + (B – A) and
- If A > B then C= (A – B) and
- If A = B then C=0

Step 5: Repeat from step 3 until the whole element of the matrix does not change. The first phase will be completed with the output of the new matrix. This method will be applied on all three planes of the data image.After applying this new data image has been generated with the help of new matrix of each plane, in which the number of '1' is less compare to the original data image.

In this method, a case has been arrived in which the output is generated by the summation of 192 and difference of A and B. The reason behind adding 192 is that after adding this special number the upper 2 bits of the pixel are '1'. The region behind this is that after converting the data image matrix into a new format it can be easily determine that which pixel value is greater and which pixel is less compared to reference pixel.

The flow chart for converting the data image in new form is:

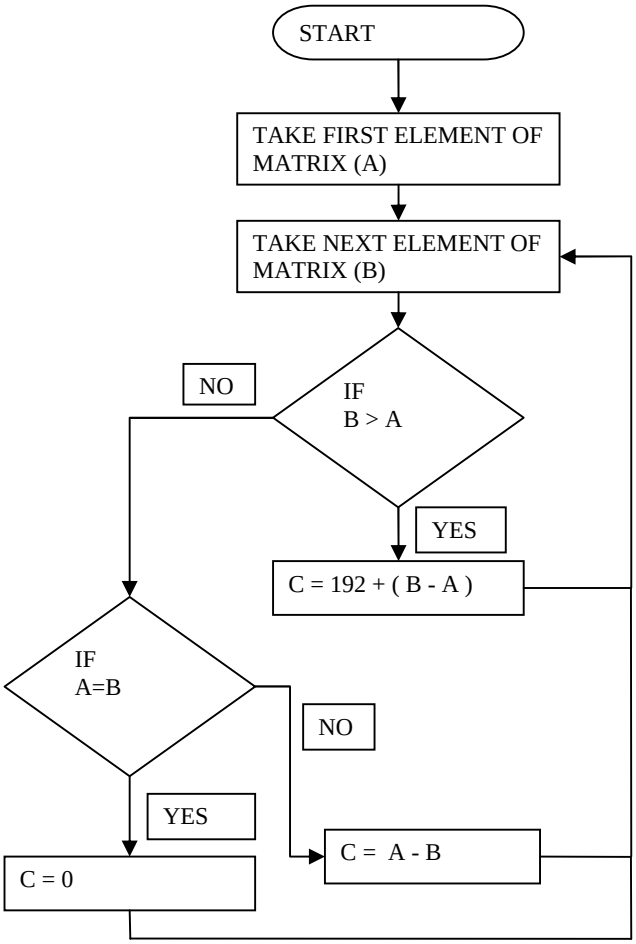


Figure 2: Data Changing Method

Let us take an example: The red plane of original data image having pixels values are shown in table 2, and there binary representation shown in table 3.

Table 2: Pixel value of the Original Data Image

226	226	222	222	224
232	236	217	167	167

Table 3: Binary Representation of the Original Data Image Pixel

11100010	11100010	11011110	11011110	11100000
11101000	11101100	11011001	10100111	10100111

Number of '1' in table 3 is 83. Here reference pixel A= 226, then the new pixels values according to proposed method are shown in table 4 and there binary representation is shown in table 5.

Table 4: Pixel value of the modified data image

226	**226**-226=0	**226**-222=4	**226**-222=4	**226**-224=2
192+(232-**226**) =198	192+(236-**226**) =202	**226**-217=9	**226**-167=59	**226**-167=59

Table 5 Binary Representation of the Modified Data Image Pixel

11100010	00000000	00000100	00000100	00000010
11000110	11001010	00001001	00111011	00111011

In table 5 number of '1' is 27, which is very less compare to table 3.

Phase Two

In this section, new matrix which is the output of phase one has been used. In this phase, each pixel of the data image has been breaking into 8 sub pixels so that each part can easily XOR with the cover image pixel. This process will be done in some steps.

Step 1: Take a pixel value from the new data image.

Step 2: Convert this pixel value in an 8-bit binary format.

Step 3: Bit-And the pixel value with "00000001" and store the output in a new matrix.

Step 4: 1-bit right shift the binary pixel value and repeat from step 3 until all bits are not shifted.

Step 5: repeat step 2, 3, 4 for each pixel of the data image.

Flow chart for this method is shown in figure 3.

According to this phase, each pixel is expanded into 8 different sub pixels. The LSB of these 8 different pixels shows the value of the original pixel.

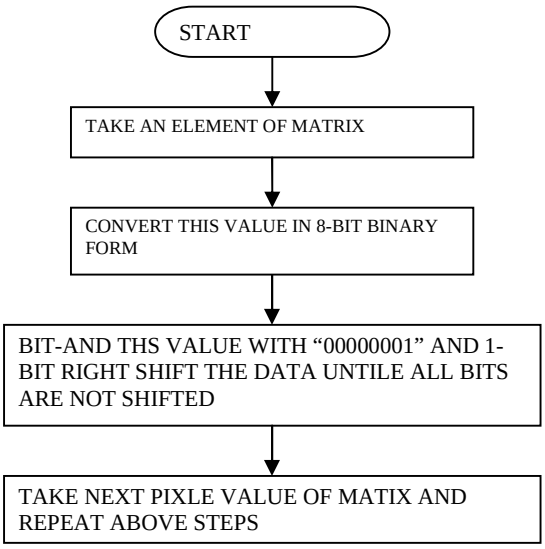


Figure 3: Data pixels Extraction Method

Let a pixel A=226

Binary representation of this pixel is A=11100010

Now Bit-And the value of A with '00000001" then

C_1= "11100010" AND "00000001"

C_1= "00000000"

The LSB of A is stored in LSB of C. now 1-bit right shift the value of A then "01110001"

Now again Bit-And the value of A with '00000001" then

C_2= "01110001" AND "00000001"

C_2= "00000001"

This process is repeated until all bits of A are not stored in LSB of matrix C's element. All these process are repeated with all pixel of the data image. In this method if the input has N element then the output of this section have an 8xN element. The output of this section is shown in table 6. Let the output of phase one is

226	0	4	4	2

Binary representation of new matrix

11100010	00000000	00000100	00000100	00000010

Table 6: Sub Pixels of the Modified Data Image

00000000	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000001
00000000	00000000	00000001	00000001	00000000
00000000	00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000000
00000001	00000000	00000000	00000000	00000000

Phase Three

This is the last and most important section of proposed method. In this section, the data image is completely store or hides into the cover image and generate the stego image. This section is done in various steps.

Step 1: Read the cover image and divide it into three planes: red plane, green plane, blue plane.

Step 2: Convert the pixels values of each plane of data image into 8-bit binary form. With the help of dec2bin command.

Step 3: Take the pixels from the output of phase two & cover image and apply XORing between these two binary values.

Step 4: Repeat step 2 and step 3 for all pixels of the cover image and the data image.

Table 7: Pixel Value of the Cover Image

10100100	00111111	01001011	01011111
10011101	01100011	01011011	00110011

Let the output of phase two is:

00000000	00000001	00000000	00000000
00000000	00000001	00000001	00000001

Output of XORing of above two matrices or stego image matrix is shown in table 8.

Table 8: Pixel Value of the Stego Image

10100100	00111110	01001011	01011111
10011101	01100010	01011010	00110010

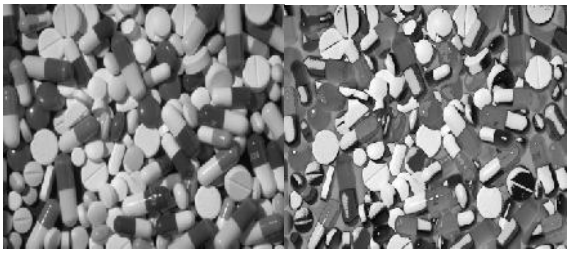
Experimental Result and Discussion

The proposed method has three phases, in phase I, the data image has been changed into a new format to decrease the numbers of '1'. In proposed method, various data images have been worked on and some of these original data images and modified data images are analyzed here.

(a) (e)

a. (f)

(b) (g)



(c) (h)

Figure 4: Original data image (a) – (d); Modified data image (e) – (h)

After modifying the data image, apply the next phase of proposed method.

- Break the data image and the cover image into three planes red, green, blue.
- Each pixel of the modified data image is then divided into 'N' sub pixels.
- After all these process applying the M-bit XORing method between the cover image pixels and the modified data image sub pixels.
- After hiding data stego image is generated, which is use for transmission.

Table 9: Comparison between Original Data Image and Modified Data Image

	Data image	Arctic	Lenna	Founviere	Pills
Red plane	Original	26502	18563	15074	17269
	Modified	30688	13127	11332	15431
Green plane	Original	25242	15125	15598	15987
	Modified	14332	14353	11470	15142
Blue plane	Original	24385	16344	15847	15918
	Modified	14659	13385	11791	15332
Total change in count of "1"		16450	9167	11926	3269
% Change		21.608	18.32	25.6368	6.6478

Figure 4 (a) – (h) shows the cover image and the generated stego image. Here the Lenna image has been used as the data image and the modified Lenna image is hiding with the help of 1-bit XORing method. For 1-bit XORing method, 512x512 sized cover image and 64x64 sized data image have been used. Change in the cover image does not affect the features of the data image.

(a1) (b) (c1)

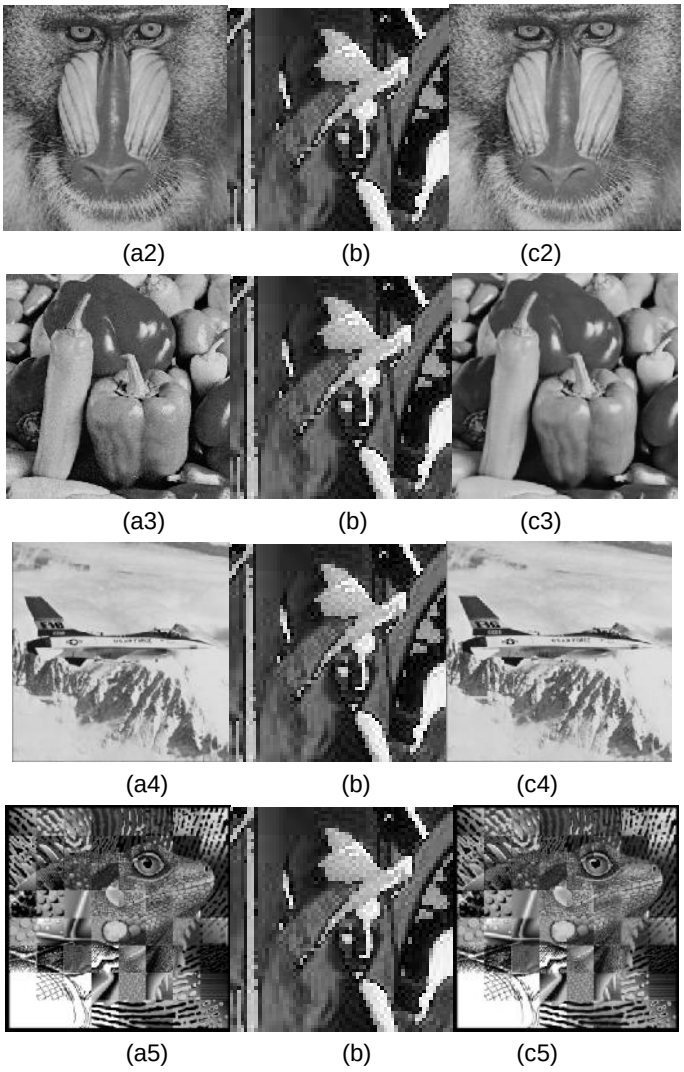


Figure 5: 1-bit XORing method with cover image(a1)-(a5), data image(b), stego image(c1)-(c5)

Visual distortion in the stego image is minimal, if the cover image has been changed for the same data image. The fundamental requirement of any image steganography algorithm is minimum visual distortion in the resulting stego image and it should be same for the different cover images. The results illustrate that the proposed algorithm conforms to these requirements.

Now Consider the same cover image (Fruits) and same the data image (Lenna) with different N-bit XORing method.

Cover image (512x512) | Data image (256x256) | Stego-image (512x512)


Cover image
(512x512)


Data image
(512x512)

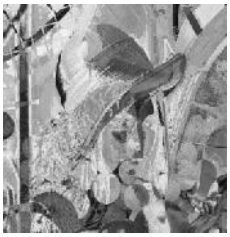

Stego-image
(512x512)

Figure 6: 4-bit & 8-bit XORingmethods with same cover image and different size of data image.

Table 10: Different values of MSE with different cover image and different data image by using 1-bit xoring

Data image → Cover image ↓	Lenna	Arctic	Fouviere	Pills
Fruits	0.0273	0.0600	0.0226	0.0299
Baboon	0.0266	0.0587	0.0221	0.0295
Papper	0.0265	0.0585	0.0220	0.0294
Jet-plane	0.0263	0.0582	0.0218	0.0292
Frymire	0.0189	0.0421	0.0154	0.0210

Table 11: Different values of PSNR with different cover image and different data image

Data image → Cover image ↓	Lenna	Arctic	Fouviere	Pills
Fruits	63.7717	60.3459	64.5852	63.3754
Baboon	63.8810	60.4411	64.6824	63.4387
Papper	63.8949	60.4586	64.7110	63.4532
Jet-plane	63.9328	60.4839	64.7481	63.4783
Frymire	65.3556	61.8901	66.2434	64.9134

Table 12: Comparison table of MSE and PSNR for existing method and proposed method

n-bit LSB	MSE		PSNR	
	Existing method[2]	Proposed method	Existing method[2]	Proposed method
1-bit	0.5	0.0273	51.1	63.7717
2-bit	2.5	0.02753	44.1	53.7323
4-bit	42.7	13.1624	31.8	36.9375
8-bit	8640	125.8114	8.6	27.1336

In this table, the value for MSE and PSNR have been compared for existing method [2] and proposed method. In this comparison, the image of Fruits is used as the cover image and the image of Lenna is used as the data image.

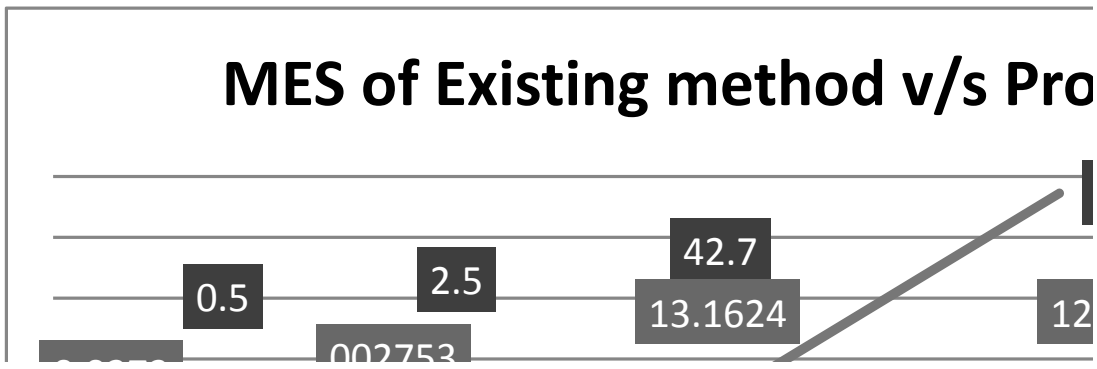


Figure 7: MSE comparisons between existing method and proposed method

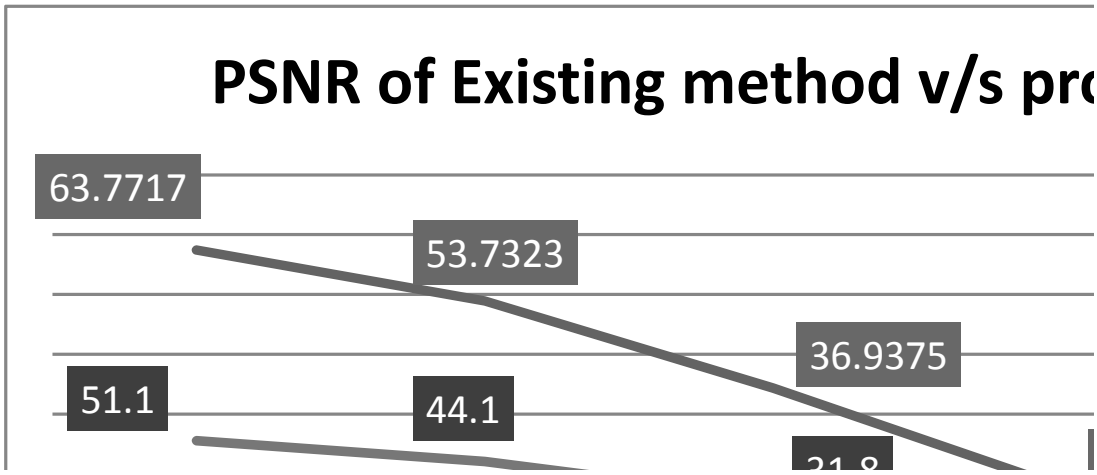


Figure 8: PSNR comparison between existing method and proposed method

Conclusion

In this paper, a new image steganography technique has been developed. By using this new proposed method, high quality of stgo image has been achieved. The value of PSNR and MSE also modified by proposed method. The PSNR value of stego image is higher compare to other steganography method; due to this a high-quality stego image has been achived. In proposed method, the format of the data image has been changed. New data image have less number of '1' compare to the original data image. With the help of proposed method, the quality of the stego image is increase by 20% (nearly). Security of the data image is also increased by using proposed method.

References

- Abbas Cheddad, Joan Condell, Kevin Curran, Paul McKevitt,"Digital image steganography: Survey and analysis of current methods", Elsevier journal of Signal Processing 90, 727–752, 2010.
- Arvind Kumar and Km Pooja,"Steganography-A hiding Technique", International journal of Computer Application, vol. 9, no. 7, November 2010.
- Atallah M. Al-Shatnawi,"A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, vol.6, no.79, 3907–3915, 2012.
- Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh,"FPGA Hardware of the LSB Steganography Method", IEEE potentials, 978-1-4673-1550-0, 2012.
- Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh,"FPGA Hardware of the LSB Steganography Method", IEEE potentials, 978-1-4673-1550-0, 2012.
- Chi-Kwong Chan, L.M. Cheng ,"Hiding data in images by simple LSB substitution", Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong-Kong,May-2002.
- FangjunHuang,"New Channel Selection Rule for JPEG Steganography", IEEE Transactions on Information Forensics and Security, vol.7, no.4, 2012.
- Himanshu Gupta, Prof Ritesh Kumar and Dr. SoniChanglani,"Enhanced Data Hiding Capacity using LSB-Image Steganography Method", International Journal of Emerging Technology and Advanced Engineering, vol.3, June 2013.
- Leung, H.Y., Cheng, L.M., Cheng, L.L., Chi-KwongChan,"Hardware Realization of Steganographic Techniques", Intelligent Information Hiding and Multimedia Signal Processing, Third International Conference on IIHMSP 2007, vol.1, pp.279,282, 26-28, November 2007.
- Mohammed Salem Atoum,"A Steganography Method Based on Hiding secrete data in MPEG/Audio Layer III", IJCSNS International Journal of Computer Science and Network Security, vol.11, no.5, 2011.

- Mr. VikasTyagi, Mr. Atulkumar, Roshan Patel, SachinTyagi,"Image Steganography Using Least Significant Bit with Cryptography", Journal of Global Research in Computer Science, vol.3, no.3,2012.
- Ozdemir Cetin, A. TuranOzcerit,"A new steganography algorithm based on color histograms for data embedding into raw video streams", Computers & Security, vol. 28, no. 7, pp. 670-682, October 2009.
- R.Anderson and F. Petitcolas,"On the limits of steganography", IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
- Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin,"Hiding data in images by optimal moderately significant-bit replacement" IEE Electron. Lett., vol. 36, no. 25, 2000.
- Samir K Bandyopadhyay, Debnath Bhattacharyya1, Debashis Ganguly1, Swarnendu Mukherjee1 and PoulamiDas,"A Tutorial Review on Steganography", Heritage Institute of Technology.
- Souvik Bhattacharyya, Indradip Banerjee, GautamSanyal,"A survey of steganography and steganalysis technique in image, text, audio, and video as cover carrier", Journal of global research in computer science, vol. 2, no.4, 2011.
- Weiqi Luo, Fangjun Huang, JiwuHuang,"Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE Transactions on Information Forensics and Security, vol.5, no.2, pp. 201-214.M., 2010.
- Youssef Bassil, "Image Steganography method based on brightness adjustment", Advances in computer Science and its application, vol.2, no.2, 2012.

❖◆❖