International Journal of Science and Research (IJSR)
ISSN: 2319-7064
ResearchGate Impact Factor (2018): 0.28 | SJIF (2019): 7.583

Security Enhancement of Image Steganography by Randomization Channel Approach

G. S. Gill

Department of Instrumentation, Kurukshetra University, Kurukshetra, India

Abstract: ***In today's modern communication world, security of communication is necessary. It prevents misuse of secret information. Security may be provided in many different ways. Protection of the copyright can be provided using watermarking and fingerprinting. Whereas, steganography can be used to protect the actual message one has to send. Steganography is different from the encryption in a way that is makes the communication imperceptible. It means no one can identify whether communication is taking place or not except sender and receiver. It uses a base to transmit actual message. In the following work three experiments have been done for image steganography. Least significant bit based steganography is used for all three experiments. Difference between the three is of the security level and pixels in which data is to be hidden which provides randomization. Main focus is to enhance the security level. First experiment is quite simple with direct hidden process. Second experiment is enhancement of first experiment with small changes in hiding process. A new method is then proposed which is the third experiment. This is more complex than the first two experiments and provides channel randomization which enhances the security level that is the main motive of the steganography. Experimental results are given for third experiment. Mean square error and Peak signal to noise ratio are calculated for all three methods. Comparison between three experiments is done on the basis of mean square error (MSE), peak signal to noise ratio(PSNR) and their level of security. Certain conclusions are then made on the basis of their comparison.***

Keywords: Image, Steganography, LSB, MSE, PSNR

1. Introduction

The digital data to be transferred from one place to another are in abundance now- a -days, and are being closely monitored by the people who desire to misuse it. These data can be any confidential data misuse of which can harm others or some random normal data misuse of which really doesn't matter. Hence, there is a need to develop some ways of hiding this useful information and prevent it from being hacked for which two different techniques can be used which are encryption and steganography. Not only had the modern day people, but also in the ancient days' people used to exercise this information hiding phenomenon while transmitting some confidential information. People used to write some message on the bald head of a person and he was made to carry this information to the destination after he had his grown and his head was again shaved at the destination to retrieve the information. Encryption focuses on coding of actual message in which it is known that some communication is taking place. This process of encryption is known as cryptography. Encryption doesn't hide the very existence of information in the message and hence attracts the hackers towards it which ultimately leads to compromise of information at times. On the other hand steganography not only encrypts the data, but also hides the very existence of information.

Steganography aims to hide the information in some irrelevant cover. Depending on the message being transmitted, steganography is classified in four ways: Image steganography, Text Steganography, Audio steganography and Video steganography. Following problem focuses on the technique of Image steganography. Image steganography is one of the most important and frequently used technique as majority of the information now-a-days is in image form on the internet media. Image steganography is the technique in which an "information containing" image (message image) is to be hidden inside a cover or base image. The final outcome image after Image steganography is known as a Stego image. Main motive behind steganography is to make communication imperceptible. The technique used in this paper for image steganography is Least Significant Bit (LSB) Steganography. In LSB steganography, the data bits of message image are stored in the LSB of each pixel of cover image. This limits the size of message image to be hidden to one eighth of the size of cover image in terms of pixels. Three different experiments are used. First is the direct hidden process. Second method is an enhanced version of first so as to enhance security. A new method is then proposed which is third experiment to enhance the security level to much higher levels.

In this problem image steganography has been performed on colored images. Both the message and cover images are in RGB domain. The LSB technique is further extended to hide the message in first LSB or second LSB or so on up to the MSB in cover image. Study of MSE and PSNR for all these extended LSB options is done to compare all three experiments.

2. Related Work

Steganography is a method to perform the communication in an imperceptible manner. Main motive behind steganography is to protect the secret or private information. It helps to maintain the secrecy of message. Different types of steganography are there. Steganography to be performed depends upon the image format as well. It can be performed using many different tools. Most commonly used tool is matrix laboratory (MATLAB). Cheddad *et al.* presented a survey of current methods of steganography [1]. A comparison study is also given between different techniques of security. Poornima and Iswarya presented a detailed discussion on steganography [2]. They also discussed different types of steganography in time as well as frequency domain.

LSB is the common method used for performing steganography. In this method message is hidden in the LSBs of the pixels of the cover. Many different algorithms have been given using LSB depending on the randomization of the pixels in which the message is to be hidden. Momin *et al.* presented survey of steganography using an LSB based algorithm [3]. Multiple algorithms have been discussed by them. Garg and Gulati proposed a comparative study by hiding message in LSB and MSB [4]. They presented comparison study using MSE and PSNR. RGB based steganography technique are used widely. It is because most of the images used now-a-days are RGB. So, there is need to provide security mechanisms for RGB images. Parvez and Gutub presented RGB based steganography. They discussed a new algorithm for storing variable number of bits in different channels [5]. Gutub *et al.* presented RGB based algorithm [6]. This algorithm increases the capacity as well as provides randomization. Bairagi *et al.* [7] presented a RGB channel based steganographic technique. This technique provided robustness to the system. They used a secure key to hide information.

3. Methodology

Many different tools can be used to perform image steganography. MATLAB is one of the most important tools. When the image processing toolbox is associated with the MATLAB input is given in the form of an image which is represented as a matrix in MATLAB. Certain operations can be performed on the image for its enhancement or to extract useful information from it.

Image steganography has been performed on RGB images. In the following work least significant Bit method has been used. Two RGB images have been used. One of these is used as the cover image and other one is as the message image. Size of the cover image is 512x512x3 and size of the message image is 100x100x3. In this problem three different methods have been used to perform the image steganography. Firstly two simple methods of steganography have been performed and then a new enhanced method is proposed so as to enhance the security level. After performing all three experiments, comparison of the results is done on the basis of the MSE and PSNR.

A. First experiment

In this method R, G and B components of cover and message images are separated. All three components of message image are then hidden inside the respective components of the cover image. Thus, a stego (cover image + message image) image is obtained by combining back the respective stego images of R, G and B components. This experiment is performed by using different bits of the cover image starting from LSB to MSB one by one. This means that firstly bits of R, G and B component of message image are hidden inside the LSB of the different pixels of the respective components of cover image until full message image is hidden and same operation is performed with second significant bit and so on up to MSB and then comparison is done on the basis of MSE and PSNR. Problem with this method is that it is easy to find the message hidden communication is sensed. Because, even if a hacker succeeds in just getting any 1 component then all other components can be easily extracted. Thus, it can be said that security level is less in this method.

B. Second experiment

This method is somewhat similar to first experiment with a difference that instead of hiding R component of message image in R component of cover image it is hidden inside the G component. Similarly, G component is hidden inside the B component and B component of message image is hidden inside the R component of the cover image. This method has also been performed for all the bits of cover image starting from LSB to MSB. Although, security in this method is more as compared to first method because it is difficult to identify the component of message image which is hidden inside any particular component of cover image yet, security level is not much high. It is because if a hacker gets any one component whether it is R, G or B other two can be easily determined.

C. Third experiment

A New method has been proposed to enhance the security of the steganography. In this method firstly R, G and B components are separated for both coverand message images. All the six components are then divided in three parts each. Now, 9 parts of message image are there which are to be hidden inside 9 parts of the cover image. This is to be done randomly that is, instead of hiding all parts of R component of message inside R component of cover, its some partshidden in B component and remaining in Gcomponent. Same is to be done for all the parts of the remaining components of message image. It provides security in two ways. Firstly, parts of different components are hidden inside random components. It means channel randomization has been done. Secondly, when all the parts are combined so as to form stego image then data is hidden in some part of the R component of stego image and then some part is purely cover and again some data is hidden and so on. Similar process is there for both B and G components as well. It provides the randomization of the pixels in which data is hidden. Randomization of channels along with randomization of pixels increases security to much higher levels. Fig. 1 given below is the algorithm for the message embedding of the proposed method. Fig. 2 given below is the algorithm for the message extraction from the stego image.

The algorithm given below in Fig. 1 is for hiding the message in the LSB. Firstly R, G and B components of both cover and message images are to be separated. Each component is to be divided into three parts. Total nine obtained parts each for cover and message images have been obtained and are converted into binary form. One part of message is to be hidden inside any one part of the cover image in arandom manner and same is to be done for all the nine parts of message image. After hiding all the parts of message image inside the parts of cover image R, G and B components of cover image are obtained bycombining three respective parts (in which data are hidden) of each component R, G and B components.

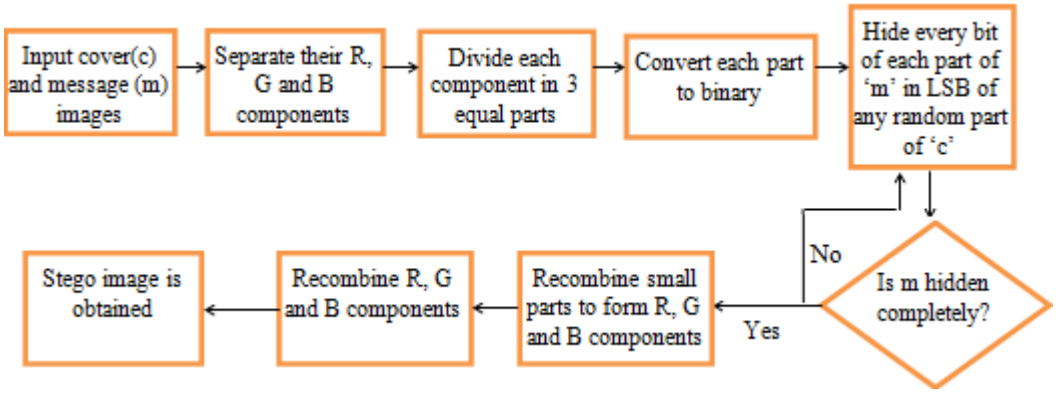

Figure 1: Algorithm for message embedding

The obtained image is the stego image as message image has been hidden inside it. It is to be performed for all the bits starting from LSB to MSB. Channel randomization and randomization of pixels are the main motive. The stego image should be similar to cover image so as to make communication imperceptible. The similarity of stego image with that of cover image can be checked by using MSE and PSNR concept. The results which are obtained for all different bits are to be compared on the basis of MSE and PSNR. The results of MSE and PSNR obtainedfor first experiment and second experiment are compared with the results obtained for proposed method that is third experiment. Equation (1) can be used to find MSE. Equation (2) can be used to find PSNR.

$$MSE = \frac{sum(sum(g))}{i*j} \quad (1)$$

Where g is the squared error image and $=\left(double(c) - double(s)\right)^2$ 'i' is the number of rows in cover image. 'j' is the number of columns in cover image. 'c' is the cover image . 's' is the stego image.

$$PSNR = 10 * log10(256\text{^}2 / MSE) \quad (2)$$

Fig. 2 given below is the extraction of message at the receiver's end. R, G and B components of the stego image obtained at the receiver's end has been separated and divided into three parts each.

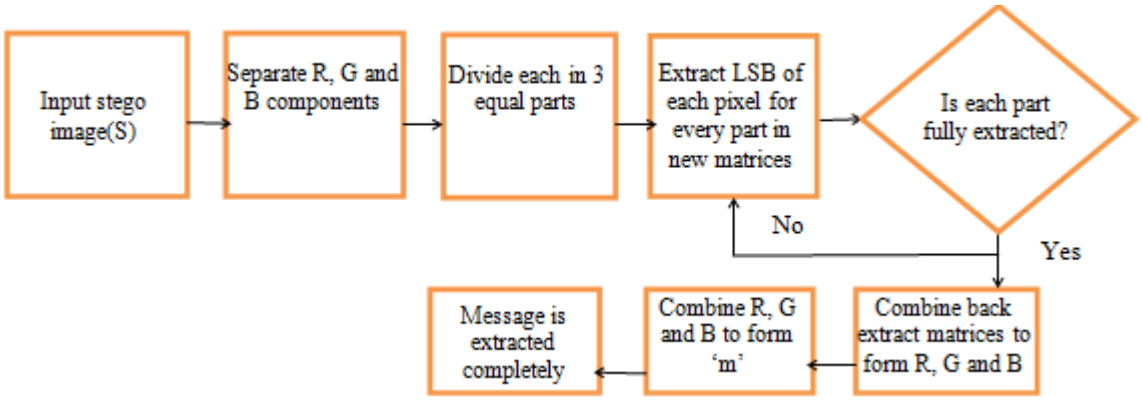

Figure 2: Algorithm for message extraction

Nine temporary matrices are then used to obtain the LSB of the pixels of all nine parts of stego image such that LSB values of one part collected in first temporary matrix and so on for all the nine parts. When all the LSBs have been extracted, respective parts of R, G and B are combined to give the message image. It isto be done for the same bit which was used for hiding at the sender's side. The obtained message image at the receiver's side is expected to be exactly similar to the message image which was being sent by the sender.

4. Experimental Results

In LSB method 1 bit of a pixel of message is to be hidden inside the LSB of 1 pixel of cover image. This implies 1 pixel of message image is hidden inside the 8 pixels of cover image. It can be said that size of cover image must be greater than or equal to 8 times of the size of message image. Fig. 3 is the cover image which was initially of size 4000x2248x3 and reduced to 512x512x3. Fig. 4 is the message image which was initially of the size 1600x900x3 and reduced to 100x100x3. It can be seen that the size of the cover image is greater than 8 times of the size of message image. Cover and message images are divided into their R, G and B components then each component is divided into three parts. Each part of cover image of every component will be of size 170x512, 170x512 and 172x512. When each component of message image is divided into three parts then each part will be of size 33x100, 33x100 and 34x100. Fig.5 to Fig. 12 are the stego images i.e. the combination of cover and message image obtained by hiding message inside cover starting from LSB to MSB. Fig. 5 to Fig. 12 are the stego images which have been obtained by hiding the message image inside LSB, 2nd LSB, 3rd LSB and so on up to MSB of the pixels of the cover image respectively. Fig. 13 is the extracted message image. It can be observed that Fig. 5 to Fig. 8 looks very similar to each other. No change in the stego image can be noticed just by looking at it. But, change in the stego image can be noticed from Fig. 9 to Fig. 12.

Figure 3: Cover image

Figure 4: Message image

Figure 5: Stego image (LSB)

Figure 6: Stego image(2nd LSB)

Figure 7: Stego image (3rd LSB)

Figure 8: Stego image (4th LSB)

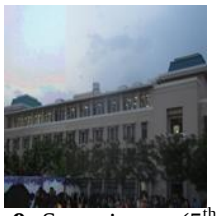

Figure 9: Stego image (5th LSB)

Figure 10: Stego image (6th LSB)

Figure 11: Stego image (7th LSB)

Figure 12: Stego image (MSB)

Figure 13: Extracted image

As one move from Fig. 9 to Fig. 12 the quality of the stego image goes on degrading which suggests that when any bit starting from 5th LSB to MSB is usedfor hidden process can be easily identified so it is advised not to use these bits for performing steganography. It is because the security level is very less if any of these bits is used for hiding message image. Although the difference among stego images by using bit starting from LSB to fourth LSB cannot be identified with casual eyes yet, some other methods (MSE and PSNR) are there to check out the difference between these images. Fig. 13 is the extracted message image. The extracted message image must be exactly similar to the image which was hidden by the sender. The similarity of both these images can also be checked using the MSE and PSNR value. As these should be exactly similarly the value of MSE and PSNR should be the ideal values for these two images. Ideal value of MSE is '0'. Ideal value of PSNR is 'Inf' which means not defined. If both of these values are obtained, it means the same message has been successfully extracted. Table I gives the values of MSE and PSNR for first experiment for bits starting from LSB to MSB. Table II gives the values of MSE and PSNR for second experiment for bits starting from LSB to MSB. Table III gives the values of MSE and PSNR for proposed method i.e. third experiment. MSE and PSNR values of first, second and third experiments are compared.

Table I: First experiment MSE and PSNR

Bit no.	MSE			PSNR		
	R	G	B	R	G	B
LSB	0.15	0.15	0.15	56.33	56.33	56.33
2	0.61	0.61	0.61	50.30	50.33	50.32
3	2.43	2.43	2.44	44.31	44.31	44.28
4	9.83	9.70	9.75	38.24	38.30	38.27
5	38.53	38.85	40.04	32.31	32.27	32.14
6	159.61	158.57	155.64	26.13	26.16	26.24
7	620.31	617.48	599.23	20.24	20.26	20.39
MSB	2508.06	2510.81	2494.56	14.17	14.17	14.19

Table II: Second experiment MSE and PSNR

Bit no.	MSE			PSNR		
	R	G	B	R	G	B
LSB	0.15	0.15	0.15	56.36	56.32	56.31
2	0.61	0.61	0.61	50.34	50.31	50.30
3	2.44	2.42	2.44	44.30	44.32	44.29
4	9.80	9.65	9.81	38.25	38.32	38.25
5	38.48	38.69	39.36	32.31	32.29	32.21
6	160.42	160.08	155.71	26.11	26.12	26.24
7	618.91	603.83	616.61	20.25	20.36	20.26
MSB	2514.44	2502.31	2510.44	14.16	14.18	14.17

Table III: Third experiment proposed method MSE and PSNR

Bit no.	MSE			PSNR		
	R	G	B	R	G	B
LSB	0.15	0.15	0.15	56.33	56.34	56.33
2	0.61	0.61	0.61	50.30	50.31	50.30
3	2.44	2.41	2.44	44.29	44.34	44.30
4	9.71	9.68	9.82	38.29	38.31	38.24
5	38.99	38.71	40.33	32.26	32.29	32.11
6	159.77	158.61	152.64	26.13	26.16	26.33
7	625.17	592.58	587	20.20	20.44	20.48
MSB	2555.44	2415.63	2398.38	14.09	14.33	14.37

It can be easily noticed that PSNR and MSE for all three methods for every bit is almost same. It implies that the change in MSE and PSNR values is dependent only upon the size of the message image and the size of cover image. It means that when Message is hidden using proposed method then MSE and PSNR will remain same but security will be enhanced to much higher level. If MSE and PSNR of proposed method are observed individually then it can be seen that as the bit moves from LSB to MSB the value of MSE goes on increasing and the value of PSNR goes on increasing. It suggests that stego image using LSB will look much similar to cover image while stego image using MSB can be easily distinguished just by looking at it. If table III is observed keenly as one moves down the table up to 4th bit there is very less change in the values. This result is similar to the above results (Fig. 9 – Fig. 12) where degradation in picture quality was visible only from 5th bit up to MSB while changes in stego image were not visible for LSB to 4th bit (Fig.5 – Fig. 8). Whenever ratio of the size of cover and message is same MSE and PSNR values will also be same.

5. Conclusion

Main aim of the steganography is to achieve the security along with the similarity of stego image with that of the cover image. Three different experiments are performed. Security level increases as one move from first experiment towards proposed method i.e. third experiment. Proposed method is little bit more complex than the other two methods but it enhances the security level. If the ratio of the number of pixel changed to the total number of pixels of cover image does not change then the MSE and PSNR remain same. It implies that MSE and PSNR basically depend upon the size of the cover image and the size of the message image because size of the message image tells about the number of pixels which are to be changed in the cover image. It can also be implied that as one moves from LSB to MSB, the quality of stego image degrades. But, quality is good up to 4^{th} bit so LSB to 4^{th} bit can be used to achieve steganography in which security level is high along with good PSNR. In future, work can be done on more techniques which can decrease MSE further thus increasing the value of PSNR along with enhancement in security.

References

[1] A. Cheddad, J. Condell, K. Curran, and P.McKevitt, “Digital image steganography: survey and analysis of current methods”, signal processing, vol. 90, pp. 727-752, March 2010.
[2] R.Poornima, and R.J.Iswarya, “An overview of digital image steganography”, IJCSES, vol. 4, pp. 23-31, February 2013.
[3] B.M. Vikranth, M. H. Momin, S. M. Mohsin, S. Rimal, and S. R.Pandey, “A survey of image steganography”, JETIR, vol. 2, pp. 1172-1174, April 2015.
[4] R. Garg, and T. Gulati, “Comparison of lsb&msb based steganography in gray- scale based images”, IJERT, vol. 1, pp. 788-799.
[5] M. T. Parvez, and A. A.Gutub, “RGB Intensity based variable-bits image steganography”, IEEE Asia-Pacific Services Computing Conference, Yilan, pp. 1322-1327, December 2008.
[6] A. Gutub, A.Qahtani, andA. Tabakh, “Triple A: secure RGB image steganography based on randomization”, IEEE computer systems and applications, Rabat, pp. 400-403, May 2009.
[7] A. K..Bairagi, S. Mondal, andR. Debnath, “A robust RGB channel based image steganography technique using a secret key”, IEEE ICCIT, Khulna, pp. 81-87, March 2014.
[8] C.P.Sumathi, T.Santanam, and G.Umamaheswari, “A study of various steganography techniques for information hiding”, IJCSES, vol. 4, pp. 65-71, December 2013.
[9] J.Fridrich, M. Goljan, and D.Soukal, “Wet paper codes with improved embedding efficiency”, IEEE Transactions on Information Forensics and Security, vol. 1 , pp. 493-501, February, 2006.
[10] C. D. Bawankar, K. N. Hande, A. A. Jaiswaland A. Bute, “ Pattern matching with external hardware for steganography algorithm”, International Journal of Information Technology and Knowledge Management, Vol. 2, pp. 289-295, December 2009.
[11] A. F. Nilizadeh, A. Reza and N. Nilchi, “Steganography on RGB images based on a “Matrix Pattern” using Random Blocks” IJMECS, vol. 4, pp. 8-18, May 2013.
[12] A. Kumar, and R. Sharma, “ A secure image steganography based on RSA algorithm and Hash-LSB technique”, IJARCSSE, vol. 3, pp. 363-372, July 2013.
[13] M. A. Al-Shatnawi, “A new method in image steganography with improved image quality”, Applied Mathematical Sciences, vol. 6 ,pp. 3907-3915, 2012.