Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-10, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

LSB Data Hiding Technique in Various Sizes of Digital Images Using GUI Interface

Geeta Rani[#] ,Poonam Beniwal[*1] & Kumar Sourabh[*2]
Department of Electronics & Communication,
#M.Tech Scholar,ECE Deptt.,OITM/GJU-Hisar(125001), Haryana India
[*1]Assistant Profssor & ECE Deptt,OITM/GJU-Hisar(125001), Haryana India
[*2]Assistant Profssor & ECE Deptt,OITM/GJU-Hisar(125001), Haryana India

Abstract – *In this paper a process to Increase security of hidden data in Image and Prevent data extraction has been presented. We will encrypt data by use data hiding key and hide data using LSB technique. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. By using the key, the chance of getting attacked by the attacker is reduced.*
Keywords- GUI, LSB*, PSEUDO, PSNR, SNR*

I. INTRODUCTION

Steganography is derived from the Greek word steganographic which means covered writing. It is the science of secret communication. The goal of steganography is to hide the existence of the message from unauthorized party. The modern secure image steganography presents a task of transferring the embedded information to the destination without being detected by the attacker. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. In this paper we purposed an image based steganography that Least Significant Bits (LSB) techniques and pseudo random encoding technique on images to enhance the security of the communication. In the LSB approach, the basic idea is to replace the Least Significant Bits (LSB) of the cover image with the Bits of the messages to be hidden without destroying the property of the cover image significantly. The LSB-based technique is the most challenging one as it is difficult to differentiate between the cover-object and stego-object if few LSB bits of the cover object are replaced. In Pseudo-Random technique, a random-key is used as seed for the Pseudo-Random Number Generator is needed in the embedding process. Both the techniques used a stego-key while embedding messages inside the cover image. By using the key, the chance of getting attacked by the attacker is reduced.

To simplify the process we have designed the technique in graphical user interface (GUI). By using GUI an encoder does not have to learn the program of the technique or to rewrite the code for it, user can simply do this by GUI technique. [5]

II. RESULTS AND ANALYSIS

- Data hide in image1

Data is hiding in the image1 with the size of 16.5 kb and pixel 305*165.

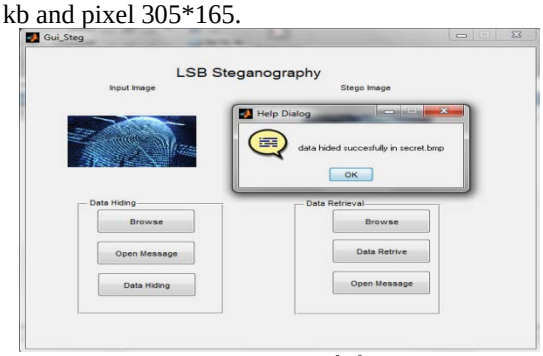

Fig 1: Data hide

The fig 1 shows that data hiding successful in input image.

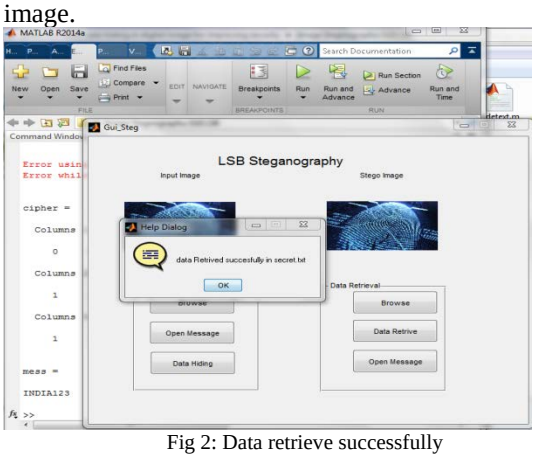

Fig 2: Data retrieve successfully

The fig 2 shows that hidden data is retrieve successfully from the encrypted image.

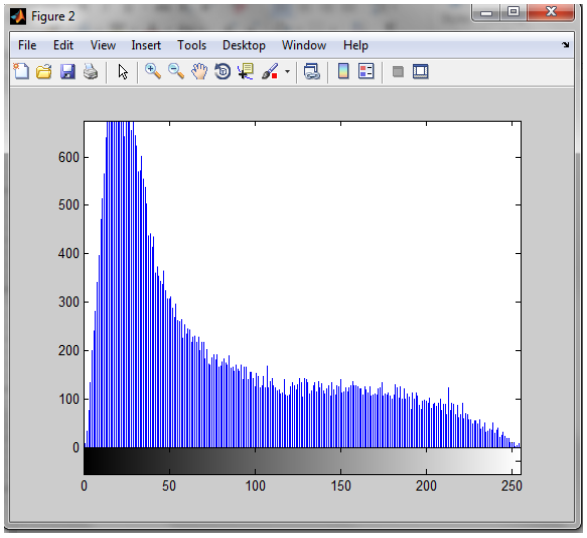

Fig 3: Histogram of image 1

The fig 3 shows the histogram of the input image 1.We calculate the different noises for image 1 that effect the quality of image.
The Peak-SNR value by salt and pepper noise is 21.4862 and the SNR value is 14.1796 and the Peak-SNR value by poisson noise is 29.1308 and the SNR value is 21.8243

- Data hide in image 2

Data is hiding in the image1 with the size of 11.7 kb and pixel 236*213.

Fig 4: Data hide in image 2

The fig 4 shows that data is hide successfully in image 2.

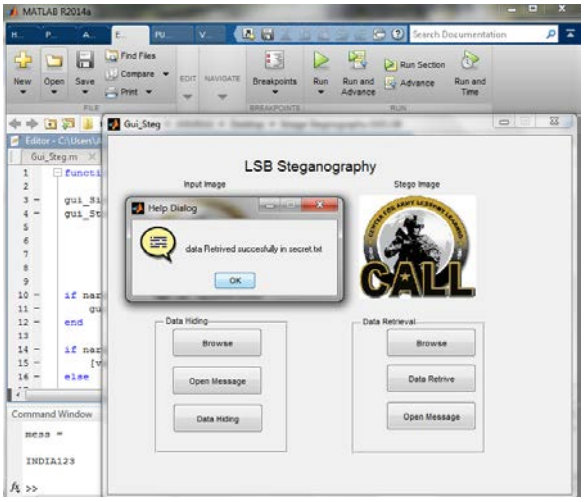

Fig 5: Data successfully retrieve

The Fig 5 shows that data is successfully retrieve from the encrypted image.

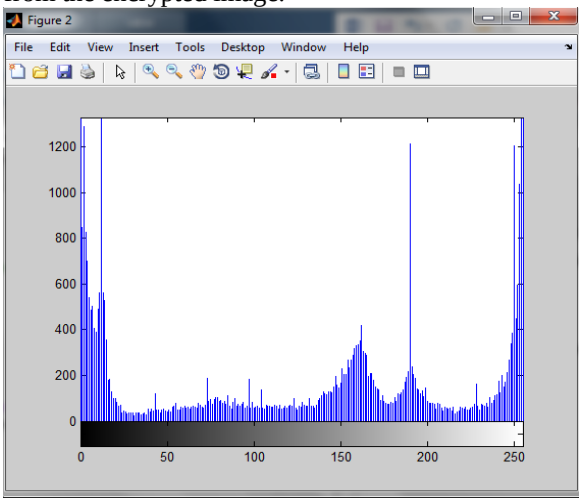

Fig 6: Histogram of image 2

The fig 6 shows the histogram for the image 2.

We calculate the different noises for the image 2.and the values of the Peak-SNR value by salt and pepper noise is 20.8544 and the SNR value is 17.3141.
The Peak-SNR value by poisson noise is 28.0250 and SNR value is 24.4847.

- Image hide in image 3

Data is hiding in the image1 with the size of 6.15 kb and pixel 294*171.

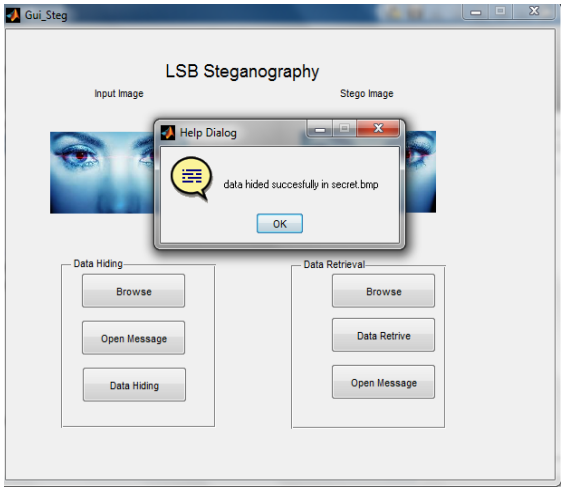

Fig 7: Data hide in image 3

The fig 7 shows that data is hide successfully in image 3.

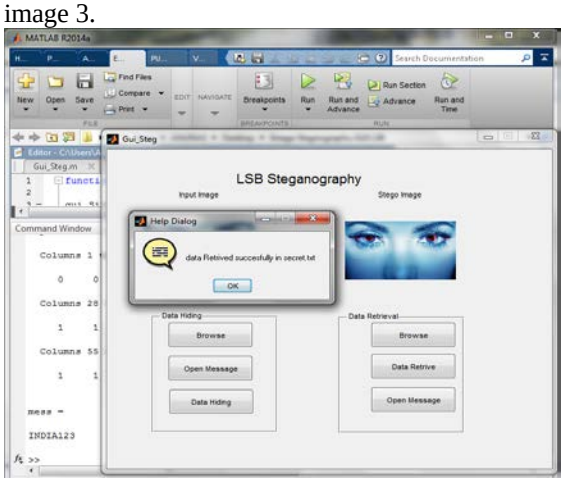

Fig 8: Data successfully retrieve

The Fig 8 shows that data is successfully retrieve from the encrypted image.

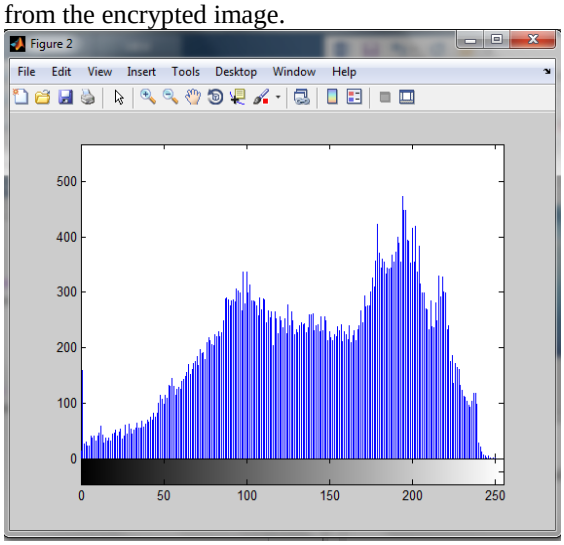

Fig 9: Histogram of image 2

The fig 9 shows the histogram for the image 2.

We calculate the different noises for the image 2 and these noises are:
The Peak-SNR value by salt and pepper noise is 22.0686 and the SNR value is 18.1186
The Peak-SNR value by poisson noise is 26.5308 and the SNR value is 22.5808.

- Data hide in image 4

Data is hiding in the image1 with the size of 6.15 kb and pixel 220*229

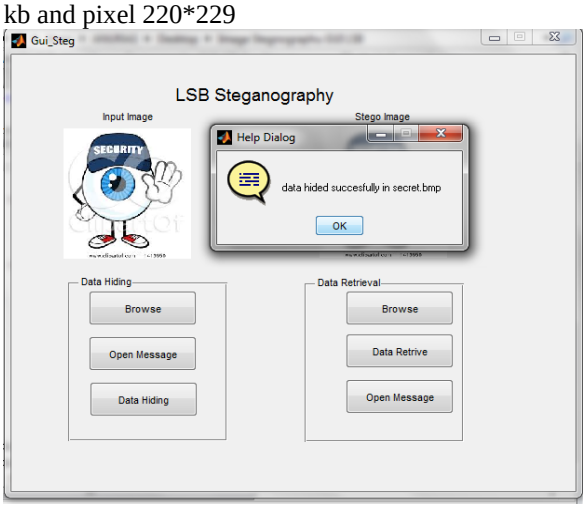

Fig 10: Data hide in image 4

The fig 10 shows the data hide in image 4 successfully.

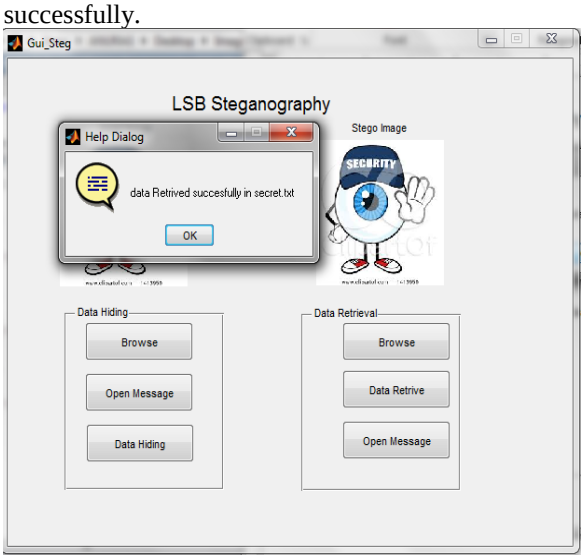

Fig 11: Data successfully retrieve

The Fig 11 shows that data is successfully retrieve from the encrypted image.

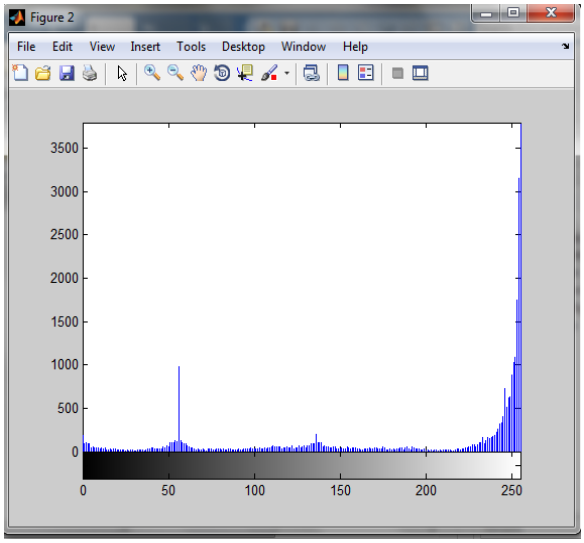

Fig 12: Histogram of image 2

The fig 12 shows the histogram for the image 2.

We calculate the different noises for the image 2 and these noises are:
The Peak-SNR value by salt and pepper noise is 20.3643 and the SNR value is 19.3867.
The Peak-SNR value by poisson noise is 27.1010 and the SNR value is 26.1234.

- Data hide in image 5

Data is hiding in the image1 with the size of 4.02 kb and pixel 225*225

Fig 13: Data hide in image 5

The fig 13 shows that data is hide successfully in image 5.

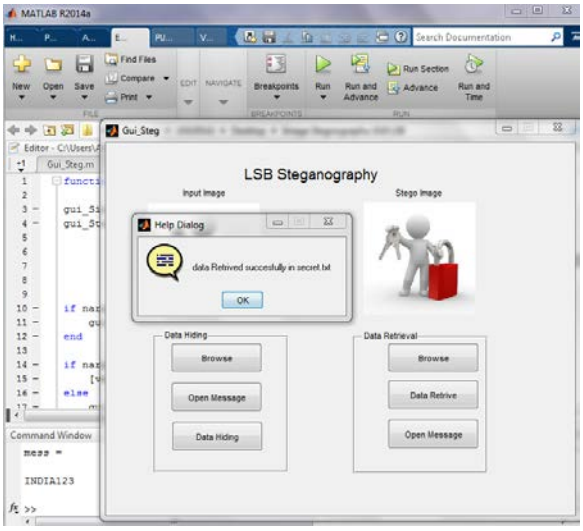

Fig 14: Data successfully retrieve

The Fig 14 shows that data is successfully retrieve from the encrypted image.

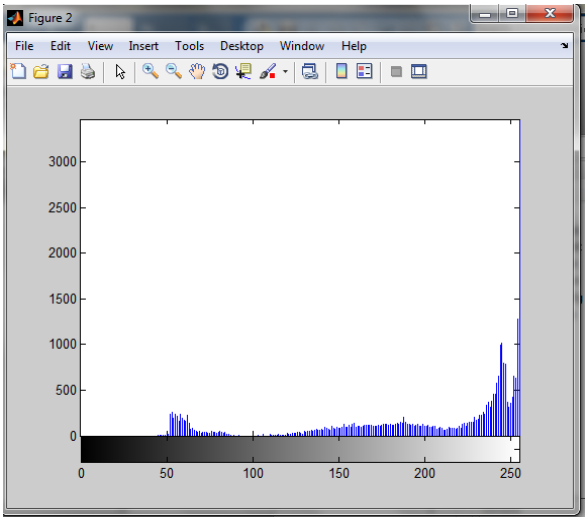

Fig 16: Histogram of image 5

The fig 16 shows the histogram of image 5.

The Peak-SNR value by salt and pepper noise is 20.6723 and the SNR value is 19.6854
The Peak-SNR value by poisson noise is 26.5873 and the SNR value is 25.6004

V. CONCLUSIONS

Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique on images to obtain secure stego-image. Our results indicate that the LSB insertion after encryption of Data for various size of images gives better results. The image resolution doesn't change much and is negligible when we embed the message into the image but image size will increase

because of data hiding. So, it is not possible to damage the data by unauthorized personnel. Overall we can conclude that data security has been improved as attacker cannot extract encrypted Data.

We also calculate the PSNR and SNR ratio for pepper and salt noise and poisson noise for different size of images. We conclude that psnr and snr may varies with the size of image and every image have different psnr and snr values for each noise.

IV. REFERENCES

[1] N. F. Johnson, and S. Jajodia, "Steganography: Seeing the Unseen", 1998, IEEE Computer.
[2] Piyush Goel, "Data Hiding in Digital Images : A Steganographic Paradigm, 2008
[3] A. Ker,"Steganalysis of Embedding in Two Least-Significant Bits", 2007, IEEE Trans. on Information Forensics and Security.
[4]] Kumar, H. ; Anuradha, "Enhanced LSB technique for audio steganography", Computing Communication & Networking Technologies (ICCCNT), 2012 Third International Conference, 2012 , Page(s): 1 - 4
[5] Ankita Agarwal(2012)," Security Enhancement Scheme for Image Steganography using S-DES Technique".
[6] Sandeep Singh, Aman Singh(2013)," A Review on the Various Recent Steganography Techniques".
[7] Vipul Sharma, Sunny Kumar (2013), "A New Approach to Hide Text in Images Using Steganography".
[8] Ajit Singh, Swati Malik(2013), "Securing Data by Using Cryptography with Steganography".
[9] Jagbir Singh, Savina Bansal, R.K. Bansal (2013), "Performance Analysis of Data Hiding Using Adjacent Pixel Difference Technique".
[10] Sonam Pathak, Rachana kamble(2013), "A Review: Chaotic System with DES (Data Encryption Standard) Image Encryption Technique".
[11] Dr.K.Sathiyasekar, S.Karthick Swathy Krishna K S (2014), "A Research Review On Different Data Hiding Techniques".
[12] Krati vyas1, B.L.Pal2 (2014) , "A Proposed Method in Image Steganography to Improve Image Quality with LSB Technique", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1.
[13] Roy, S. (2014), "Online payment system using steganography and visual cryptography", Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE.
[14] Kshetrimayum Jenita Devi, "A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique", 2013.Johnson, N.F. Jajodia, S., "Exploring Steganography: Seeing the Unseen",Computer Journal, February 1998.
[15] http://www.slideshare.net/SarinThapa/steganography-the-art-of-hiding-data
[16] http://www.maximumcompression.com/lossless_vs_lossy.php
[17] http://www.guillermito2.net/stegano/tools/