ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Shape based data Hiding Steganography as well as Steganalysis for Secure Communication System

Khushboo Jain[1], Amrit Kaur[2]

PG Student [ECE], Department of Electronics & Communication Engineering, University College of Engineering, Punjabi University, Patiala, India[1]

Assistant Professor, Department of Electronics & Communication Engineering, University College of Engineering, Punjabi University, Patiala, India[2]

Abstract: With the increase in rate of unauthorized access and attacks security of confidential data is important. In this paper shape based data hiding algorithm is proposed for steganography as well as Steganalysis is done. In this algorithm, shape is taken to hide the data in an image. The secret information can be hidden only in the pixels which are available in the shape, instead of hiding secret information in whole image. After that at Receiver the data is extracted from shape. In this paper, Mean Square Error and Peak Signal Noise Ratio are calculated for different shapes.

Keywords: MSE,PSNR, LSB.

I. INTRODUCTION

The popularity of internet and its technologies increases day by day and so are the threats to the security of our information transmitted through the internet. The unauthorized or illegal access of the data or tampering of data is very high. In order to provide security of data being accessed by unauthorized people, information hiding is required [1].

Steganography is an art and science of hiding information in some cover media. The word steganography comes from Greek origin, means "concealed (covered) writing". The word 'steganos' means "covered or protected" and 'graphie' means "writing" [2]. The basic concept is that it has a cover object that is used to cover the original message image, a host object that is the message or main image which is to be transmitted and the steganography algorithm to carry out the required object. The output is an image called stego-image which has the message image hidden inside it. This stego image is then sent to the receiver where the receiver retrieves the message image by applying the de-steganography (Fig. 1 and Fig. 2) [3].

Figure.1. Steganography at Sender Side

Figure.2. De-Steganography at Receiver Side

Application of Steganography

1. **Copyright Protection:** A secret copyright notice can be embedded inside an image to identify it as intellectual property. In addition, when an image is sold or distributed an identification of the recipient and time stamp can be embedded to identify potential pirates. A watermark can also serve to detect whether the image has been subsequently modified.
2. **Feature Tagging**: Captions, annotations, time stamps, and other descriptive elements can be embedded inside an image, such as the names of individuals in a photo or locations in a map. Copying the stego-image also copies all of the embedded features and only parties who possess the decoding stego-key will be able to extract and view the features.
3. **Secret Communications**: In many situations, transmitting a cryptographic message draws unwanted attention. The use of cryptographic technology may be restricted or forbidden by law. However, the use of stenography does not advertise covert communication and therefore avoids scrutiny of the sender, message, and recipient. A trade secret, blueprint, or other sensitive I formation can be transmitted without alerting potential attackers or eavesdroppers.
4. **Digital Watermark:** A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal.
5. **Use by terrorists:** Steganography on a large scale used by terrorists, who hide their secret messages in innocent, cover sources to spread terrorism across the country. It come in concern that terrorists using steganography when the two articles titled "Terrorist instructions hidden online" and "Terror groups hide

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

behind Web encryption" were published in newspaper [4].

The paper is organized as follow; section II starts with literature Survey, section III starts with the Proposed Methodology in which proposed block diagram, proposed algorithm with examples. Section IV illustrates the results in which proposed work MSE and PSNR are compared with existing Modified LSB technique. The conclusions and further scope are drawn in section V.

II. LITERATURE SURVEY

Samidha et.al [5] this paper describes various image steganography techniques, based on spatial domain and by considering pixel values in binary format. Spatial domain based on physical location of pixels in an image. Generally 8 bit gray level or color images can be used as a cover to hide data. Again binary representations of these pixels are considered to hide secret information. Random bits from these bytes are used to replace the bits of secret. For the above purpose to be achieved, many parameters of an image are considered like physical location of pixels, intensity value of pixel, etc. In [6], authors explore the steganography, its history, features, tools and various techniques like LSB, masking, filtering and other transformation used for hiding messages in an image.

In [7], various technologies used in image steganography are proposed. This paper presents review used for hiding a secret message or image in spatial and transform domain. This paper also proposed technique for detecting the secret message or image i.e. Steganalysis. In [8], paper presents a method for encrypting and decrypting a secret file which embeds into image file using random LSB insertion method in which bits of secret message are spread into image bits randomly. These random numbers are generated by using a key. In this paper motivation is taken from ref. [5, 7 and 8] and proposed a technique for data hiding. In this technique Shape based data hiding technique is implemented using Modified LSB technique. In this work in place of replacing EX-ORing of cover frame pixel and data is done to reduce the probability of pixel variation in cover frame. Also Steganalysis of Shape based data hiding technique is done to extract the data from shape.

III. PROPOSED METHODOLOGY

In this proposed model, the RGB color cover image and color message image are read simultaneously. After that shape is selected to hide the message in cover image.

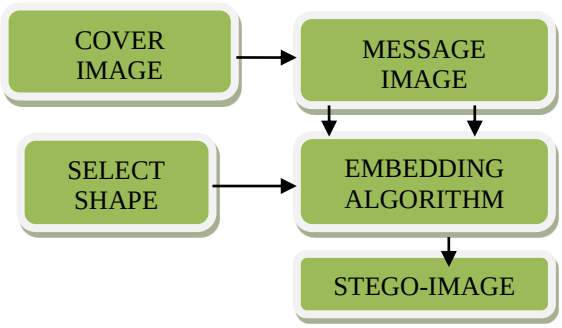

Figure.3. Proposed Block Diagram of Steganography

At receiver side, Steganalysis is done. The RGB color cover image and Stego color image are read simultaneously. After that shape is selected to extract the message image from stego image.

To measure the imperceptibility of stego image, MSE and PSNR are calculated and compared with the existing techniques.

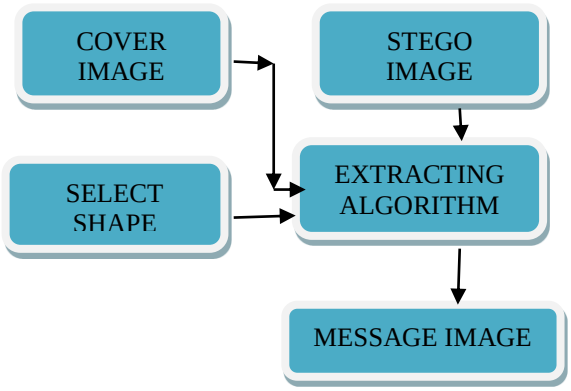

Figure.4. Proposed Block Diagram of Steganalysis

Proposed Algorithm for Steganography

1. Read the Cover image. Extract their plane.
2. Read the Message image and extract their planes.
3. Select the shape in which data is to hidden.
4. Hide the different planes of message in cover image plane in shape.
5. Stego-image is generated at transmitter side.

Proposed Algorithm for Steganalysis

1. Read the cover image and extract their plane.
2. Read the Stego- image and extract their planes.
3. Select the shape in which the data hidden.
4. Extract the splited bits from Stego image.
5. After that splited pixels are combining to extract the original message image.

Table 1

255	120	111	109	112	115
108	96	105	145	205	255
245	240	207	110	199	189
119	117	129	127	147	143
99	179	189	190	104	181
191	219	230	161	151	171

Table 2

255	120	111	109	112	115
108	96	105	145	205	255
245	240	207	110	199	189
119	117	129	127	147	143
99	179	189	190	104	181
191	219	230	161	151	171

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Table 3

255	120	111	109	112	115
108	96	105	145	205	255
245	240	207	110	199	189
119	117	129	127	147	143
99	179	189	190	104	181
191	219	230	161	151	171
231	222	112	190	151	189
170	225	140	179	111	129

Table 4

255	120	111	109	112	115
108	96	105	145	205	255
245	240	207	110	199	189
119	117	129	127	147	143
99	179	189	190	104	181
191	219	230	161	151	171

IV. SIMULATION RESULTS

In this paper, simulating the image processing part of shape based data hiding in MATLAB software.The effectiveness of any Steganographic method can be determined by comparing stego-image with the cover image. There are some factors that determine the efficiency of a technique. These factors are [9]

1. **Mean Square Error (MSE)**: It is defined as the average squared difference between a reference image and a distorted image. The small the MSE, the more efficient the image steganography technique. MSE is computed pixel-by-pixel by adding up the squared differences of all the pixels and dividing by the total pixel count.

$$\text{MSE}=\frac{1}{M*N}\sum_1^M\sum_1^N(Fij-Gij)^2$$

M: numbers of rows of cover image
N: number of column of Cover Image
Fij: Pixel value from cover image
Gij: Pixel value from Stego Image
Higher value of MSE indicates dissimilarity between Cover image and Stego image.

2. **Peak Signal to Noise Ratio (PSNR)**: It is defined as the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. This ratio measures the quality between the original and compressed image. The higher the value of PSNR represents the better quality of the compressed image.

$$\text{PSNR}=10\log_{10}\frac{Imax^2}{MSE}\text{ dB}$$

Where I*max* is the maximum intensity value.

MSE is the mean square error

The cover file images details are given in Table 5, 6.These images are taken from Matlab Images Demos.

Table 5: For Shape 1

Cover Image	Resolution	Data Image	Resolution
Lena.jpg	512x512	Football.jpg	128x128
Onion.jpg	512x512	Forest.jpg	128x128
Trees.jpg	512x512	Kids.jpg	128x128
Coloredchips.jpg	512x512	Pears.jpg	128x128
Fabric.jpg	512x512	Canoe.jpg	128x128

Table 6: For Shape 2

Cover Image	Resolution	Data Image	Resolution
Lena.jpg	1024x1024	Football.jpg	128x128
Onion.jpg	1024x1024	Forest.jpg	128x128
Trees.jpg	1024x1024	Kids.jpg	128x128
Coloredchips.jpg	1024x1024	Pears.jpg	128x128
Fabric.jpg	1024x1024	Canoe.jpg	128x128

For simulation, table 3 and table 4 shapes code simulated and results are tabulated in Table 7.

Table 7: Simulation Results

Cover Image	Mean Square Error for Shape 1	PSNR for Shape 1	Mean Square Error for Shape 2	PSNR for Shape 2
Lena.jpg	0.53	47.59dB	0.13	47.99dB
Onion.jpg	0.44	47.68dB	0.11	48.01dB
Trees.jpg	0.59	47.53dB	0.14	47.98dB
Coloredchips.jpg	0.63	47.49dB	0.15	47.97dB
Fabric.jpg	0.51	47.61dB	0.13	47.99dB

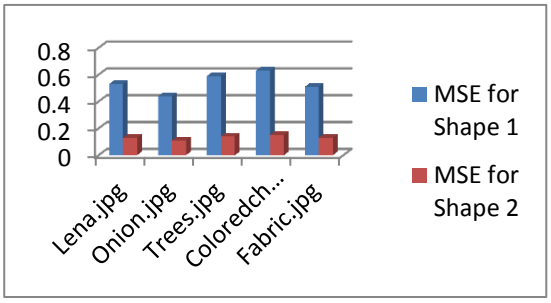

Figure.5. Histogram for Mean Square Error

DOI 10.17148/IJARCCE.2015.4640

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

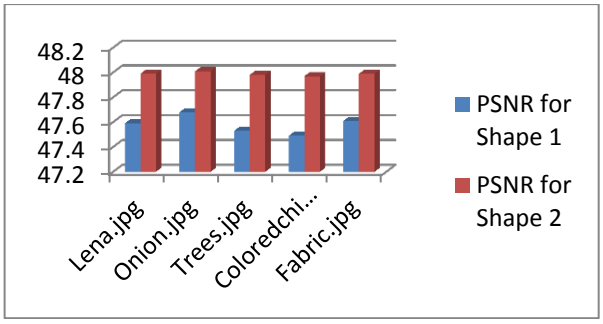

Figure.6. Histogram for Peak Signal to Noise Ratio

V. CONCLUSION

In this paper, Shape based Data hiding technique is proposed. The shape based data is more secure and efficient because data can be hiding in cover image in any shape. In this paper, works have been done on four images and table 2 and table 4 shapes are designed and simulated on MATLAB 2013. The result shows that MSE and PSNR depend upon the variation in pixels and how much data is hiding in cover image.

REFERENCES

[1] Dr. Sudeep D. Thepade, Smita S. Chavan, "Consine, Walsh and Slant Wavelet Transform for Robust Image Steganography", Tenth International Conference on Wireless and Optical Communication Networks, pp. 1-5, July 2013.
[2] GunjanChugh, RajkumarYadav, and Ravi Saini, "A new Image Steganographic Approach Based on Mod Factor for RGB Images", International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 7, pp.27-44, 2014.
[3] NadeemAkhtar, Shahbaaz Khan, and PragatiJohri, "An improved Inverted LSB Steganography", International Conference on Issues and Challenges in Intelligent Computing Techniques, pp. 749-755, February 2014.
[4] Arvind Kumar, Km Pooja, "Steganography- A Hiding Technique", International Journal of Computer Applications, vol 9, November 2010.
[5] Dr. DiwediSamidha, DipeshAgrawal, "Random Image Steganography in Spatial Domain", International Journal of Computer Science and Information Security, vol. 7, March 2013.
[6] Neil F. Johnson Sushiljajodia, "Exploring Steganography: Seeing the Unseen", IEEE, pp. 26-34, Feb 1998.
[7] S. Ashwin, J. Ramesh, K. Gunavathi, "Novel and Secure Encoding and Hiding Techniques using Image Steganography: A Survey", International Conference on Emerging Trends in Electrical Engineering and Energy Management, pp. 171-177, December 2012.
[8] M.S Sutaone, M.V Khandare, "Image based Steganography using LSB Insertion Technique", IEEE Xplore, pp. 239-242, May 2012.
[9] KousikDasgupta, J.K Mandal and ParamarthDutta, "Hash based Least Significant Bit Technique for Video Steganography", International Journal of Security, Privacy and Trust Management, vol.1, April 2012.