Int. J. Advanced Networking and Applications
Volume: 09 Issue: 05 Pages: 3596-3600(2018) ISSN: 0975-0290

Robust Lossless Secure Image Steganography Using Spiral Scan

Dr. S. Kiran
Department of CSE, Y.S.R.Engineering College of YV University, Proddatur, Andhra Pradesh
Email: rkirans125@gmail.com
R. Pradeep Kumar Reddy
Department of CSE, Y.S.R.Engineering College of YV University, Proddatur, Andhra Pradesh
Email: pradeepmadhavi@gmail.com
Dr. A. Ashok Kumar
Department of Physics, Y.S.R.Engineering College of YV University, Proddatur, Andhra Pradesh
Email: drashok.yvuce@gmail.com
N. Subramanyan
Department of CSE, Y.S.R.Engineering College of YV University, Proddatur, Andhra Pradesh
Email: subramanyam.neelam@gmail.com

ABSTRACT

Steganography is the principles and techniques of embedding data within other data. Cryptography is the principles and techniques of changing the data one form to another form. Image Steganography is the process of hiding data within an image. Steganography along with encryption techniques provides an additional security to the data. Several techniques exist for image steganography, in this work, a new lossless image steganography technique along with cryptographic method is presented. Lossless compression is a class of algorithms that allows the original data to be perfectly reconstructed from the compressed data. Present work concentrates the lower nibble of pixels in the cover image for embedding the information; further encryption techniques will be applied. It is not possible for the hacker to retrieve the secured data from the cover image.

Keywords - **Compression, Cover image, Cryptography, lossless, Nibble, Steganograpy.**

Date of Submission: March 09, 2018 Date of Acceptance: March 23, 2018

I. INTRODUCTION

With the rise of Internet sharing of information[1] has dramatically increased, along with some security necessities are required for secure sharing of data. For secure transformation of images, steganography[2] and cryptographic techniques are required. Cryptography[3] is the process of transforming readable information into understandable form which is not understandable.

The original data which is called plaintext, the data after transforming into unreadable form is called ciphertext[3]. Encryption is the process of generating the cipher text from plaintext with the help of some mathematical operations with the key. The reverse process of encryption is called decryption[3]. Fig.1 shows the encryption and decryption process.

Figure 1. Encryption and Decryption process

Cryptographic systems need both an algorithm and a secret key. Unlike cryptography, to protect data from eavesdroppers steganographic techniques are used which attempts to hide the data from eavesdroppers.

Terminologies used in image steganogrphy[4][5] are cover image, secrete image, secret key and embedding technique. Cover image is the carrier of the secrete image. Secrete image is the image which is to be hide in cover image. To embed secrete image in cover image depending on the technique secrete key is used which is optional.

Image compression[6] is a technique works by removing redundancies and irrelevant information of the image, thereby giving the reduced size image. Compression is of two types lossless and lossy. In lossless compression, after decompression original is perfectly retrieved from the compressed image, where as in lossy compression some data loss happen. Lossy compression gives good compression over lossless compression. Compression ratio is ratio between the original uncompressed image to size of the compressed image. Section II discusses the existing work, proposed work details along with example is presented in section III. Results and conclusions are discussed in sections IV and V.

II. EXISTING METHOD

In the existing system[7], cryptographic technique is used for encrypting the secrete message in the cover image. First, secrete message which needs to be transfer is considered, and multiple transposition technique is used for encryption. In this, plain text is read in column wise and written in row wise. Size of the matrix is considered as key. Next, a RGB color cover image is considered, the encrypted message is embedded in each channel of the cover image. Alteration component technique is used for embedding the information in the cover image. In each

Volume: 09 Issue: 05 Pages: 3596-3600(2018) ISSN: 0975-0290

pixel, 7th bit position is used for embedding the information.

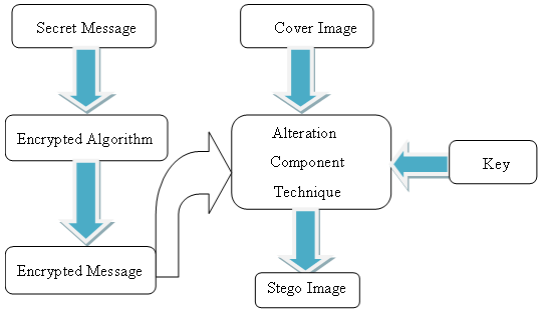

Figure 2. Image steganography process

III. PROPOSED METHOD

Proposed method focuses on the lossless compression technique, at maximum three grayscale images are going to be embedded[8] into RGB components of a cover image[8] by using lossless technique.

3.1 Encryption

In proposed lossless technique, consider two pixels from cover image and one pixel from source image to hide the data. As shown below the source image pixels is taken as 10110011 01110011 and target image pixel is taken as 1100 1110.

Cover image pixels		Source image pixels	
1011<u>0011</u>	0111<u>0011</u>	<u>1100</u>	<u>1110</u>
L1	L2	HOB	LOB

Figure 3. Processing of embedding source image pixel into cover image pixel.

Replace L1 of cover image with Higher Order Bits (HOB) of source image and L2 of cover image with Lower Order Bits (LOB) of source image. Then the final output is shown in below.

1011<u>1100</u> 0111<u>1110</u>

3.2 Detailed Example:

For example, consider a 5x5 matrix block of sample image shown in Fig.4.

135	123	145	321	156
154	224	783	667	234
788	543	812	162	654
654	123	342	111	345
765	221	342	131	124

Figure 4. Matrix of color image elements

3.2.1 Extraction of RGB Components

By using the matrix shown in Fig. 4, first divide the matrix into R, G and B planes shown in Fig.5, represent them as three individual matrices. The Fig.5 shows the individual RGB channels.

200	193	193	165	151	97	87	90	81	83	92	84	90	98	99
196	190	150	126	113	89	91	68	62	47	93	96	94	101	88
211	193	181	187	198	127	142	102	84	96	123	148	117	93	98
214	189	167	174	208	119	137	2	92	139	109	139	108	101	129
166	61	193	211	170	84	91	127	152	93	91	104	120	129	95
(a)					(b)					(c)				
Red Component					Green Component					Blue component				

Figure 5. Extraction of RGB components

3.2.3 Example of Gray Scale Image

In lossless method it is possible to embed minimum of three gray scale images. For example the three grayscale image matrices of 2x2 size shown in Fig. 6.

55	55	53	221	53	62
182	104	45	123	172	124

Figure 6. Matrices of gray scale images

3.2.4 Pixel Values of Gray Scale Images

The Fig.7 shows the assumption of three grayscale image pixels in a 2x2 matrix form as shown in Fig.6.

33	69	75	123	33	69
179	117	90	192	179	117

Figure 7. Gray scale image pixel values

3.2.5 Embedded Matrix

In Lossless technique two pixels of cover image are used for embedding for one grayscale image pixel[8]. First, calculate binary values for each pixel in both RGB channel and gray scale images. Next, embed the higher order bits[9] of each pixel in gray scale image into lower order bits of first pixel in RGB channel and lower order bits of each pixel in gray scale image into higher order bits of each second pixel in each RGB channel. After embedding all pixels the final embedded matrix is shown in Fig.8.

194	193	196	165	151	100	91	87	91	83	82	81	84	101	99
203	179	151	117	113	85	90	70	54	47	91	99	87	101	88
211	193	181	187	198	127	142	102	84	96	123	148	117	93	98
214	189	167	174	208	119	137	92	92	139	109	139	108	101	129
166	161	193	211	170	84	91	127	152	93	91	104	120	129	95

Figure 8. Embedded matrix

3.2.6 Spiral Scan Method

Spiral scan method[10] is used to provide additional security to the data. Apply spiral scan method for each component of RGB. After applying spiral scan method combine RGB components to generate a cipher RGB

Volume: 09 Issue: 05 Pages: 3596-3600(2018) ISSN: 0975-0290

image. The following Fig.9 shows the pixel values of embedded RGB channels applying after spiral scan.

3.2.7 Cipher Image Matrix

After spiral scan, the next step is to combine the individual channel images into a RGB color channel. After combining individual channel images, the final cipher image matrix shown in Fig.10.

181	193	189	167	174
187	117	151	179	203
211	214	166	161	193
211	170	208	198	113
151	165	196	193	194

102	142	137	92	92
84	54	70	90	85
127	119	84	91	127
152	93	139	96	47
83	91	87	91	100

117	148	139	108	101
93	101	87	99	91
123	109	91	104	120
129	95	129	98	88
99	101	84	81	82

Figure 9. After spiral scan method

102	142	137	92	92
84	54	70	90	85
127	119	84	91	127
152	93	139	96	47
83	91	87	91	100

Figure 10. Cipher image matrix

3.3 Decryption

First step in the decryption process is to splitting the RGB cipher image matrix into individual matrices.

3.3.1 Splitting into Red Green and Blue Channels

Consider the final cipher RGB image matrix after encryption. Embedded grayscale image sizes are required for decryption to get original images. Split the RGB image into Red, Green and Blue channels these RGB channels are embedded by spiral scan method and gray scale image in the encryption. Fig. 11 shows the pixel values of RGB channel of applying after reverse spiral scan.

181	193	189	167	174
187	117	151	179	203
211	214	166	161	193
211	170	208	198	113
151	165	196	193	194

102	142	137	92	92
84	54	70	90	85
127	119	84	91	127
152	93	139	96	47
83	91	87	91	100

117	148	139	108	101
93	101	87	99	91
123	109	91	104	120
129	95	129	98	88
99	101	84	81	82

Figure. 11 Pixel values of embedded Red, Green and Blue channels.

3.3.2 Getting Gray Scale Image

Fig.12 show the matrices after applying reverse spiral scan on individual channels of Fig.11.

194	193	196	165	151
203	179	151	117	113
211	193	181	187	198
214	189	167	174	208
166	161	193	211	170

100	91	87	91	83
85	90	70	54	47
127	142	102	84	96
119	137	92	92	139
84	91	127	152	93

82	81	84	101	99
91	99	87	101	88
123	148	117	93	98
109	139	108	101	129
91	104	120	129	95

Figure. 12 Pixel values of RGB channels after applying reverse spiral

3.3.3 Gray Scale Image Pixel Values

Next step is to separate grayscale images from the embedded RGB channel image matrices shown in Fig. 12. The extracted 2x2 image matrices from the matrices of Fig.12 are shown in Fig.13.

33	69
179	117

75	123
90	102

33	69
179	117

Figure.13 Gray scale image pixel values

This is lossless image steganography, so the matrices in Fig.13 shows the values are exactly same to the embedded 2x2 image matrices in encryption.

3.4 Encryption Algorithm

1. Read an RGB Image.
2. Extract the individual RGB components.
3. Consider two pixels from each RGB channel and one pixel from each gray scale image.
4. Consider the number grayscale images to be embed is maximum 3.
5. Consider each component of RGB channel image two pixels for embedding one gray scale image pixel. Set the higher ordered 4 bits of the grayscale image pixel into the lower order 4 bits of first pixel in each RGB component image and lower order 4 bits into higher order 4 bits of second pixel in each RGB component image.
6. Repeat the step 5 for each RGB image component with differ gray scale image.
7. Apply spiral scan method for each component of RGB.
8. Combine RGB components to generate a cipher RGB image.

Figure.15 shows the flowchart of the encryption process.

3.5 Decryption Algorithm

1. Consider cipher RGB image.
2. Splitting RGB image into red, green, blue channels.
3. Apply reverse spiral scan to all channels to extract image which is embedded of grey scale image.
4. Extract the grey scale out from the embedded R component image.
5. Repeat the step 4 for each RGB image component.
6. Combine RGB components to generate a original RGB image.

Fig.16 shows the flowchart of the encryption process

Volume: 09 Issue: 05 Pages: 3596-3600(2018) ISSN: 0975-0290

Main advantage with this method is images are perfectly retrieved without any loss of data after decryption. It is limited to pattern images as cover images. It is applicable only for png images.

IV. RESULTS

Following are the some important performance parameters of image steganography.

4.1 Embedding ratio

Embedding ratio is the amount of data embedded in a cover image, it is the ratio between the size of the hiding data to the original image size.

$$Embedding\ Ratio = \frac{Size\ of\ the\ Hiding\ Data}{Size\ of\ the\ Original\ Image} \quad (1)$$

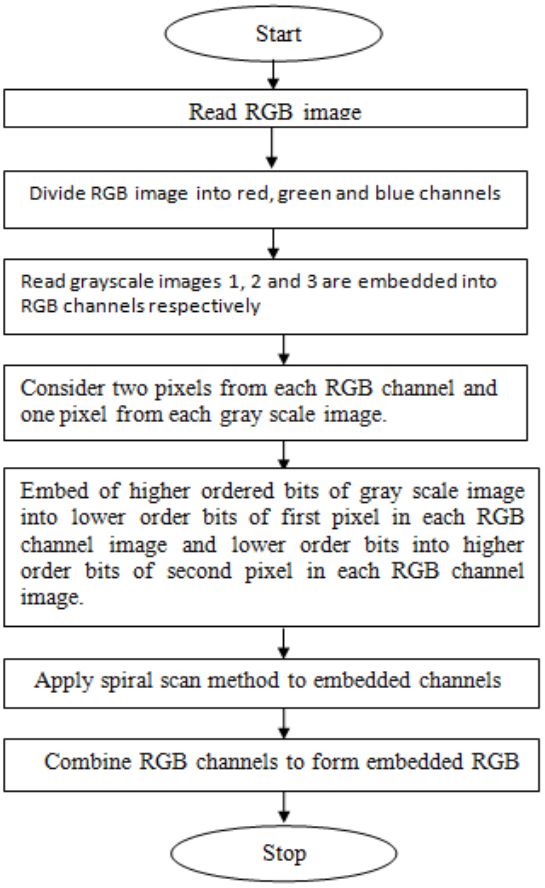

Figure 15. Flow chart of lossless encryption

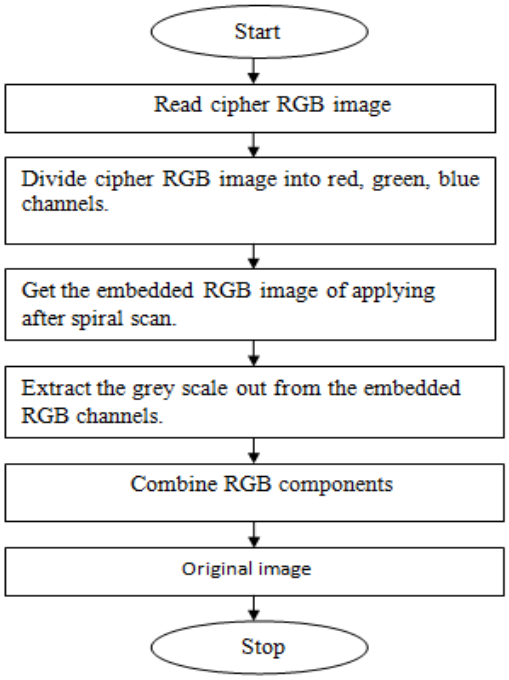

Figure 16. Flow chart of lossless decryption

It is the parameter used for measuring the amount of data embedded into the cover image. High embedding ratio results more amount of data embedded in the cover image. The following table shows the embedding ratios for existing method and proposed method.

Table 1. Comparison of existing and proposed methods

Name of the Input Image		Wood texture	Stone texture	Water wave	RGB color
Original image size in pixels		275 x 183= 50325	500 x 500= 250000	585 x 390= 228150	960 x 640= 614400
Existing Method	No.of bytes possible to encode	6290 x3= 18870	31250 x3= 93750	28518 x3= 85554	76800 x3= 230400
	Embedding Ratio	0.374	0.375	0.372	0.375
Proposed Method	No.of bytes possible to encode	25162 x3= 75486	125000 x3= 375000	114075 x3= 342225	307200 x3= 921600
	Embedding Ratio	1.497	1.5	1.5	1.5

4.2 Embedding Capacity

The maintenance of the statistical properties and perceptual quality leads a better image steganography. The capacity of the information embedded is the ratio of the total number of bits per pixel to the number of bits embedded in each pixel.

It is represented by bits per pixel. Representation of capacity in terms of percentages called the Maximum Hiding Capacity (MHC).

Volume: 09 Issue: 05 Pages: 3596-3600(2018) ISSN: 0975-0290

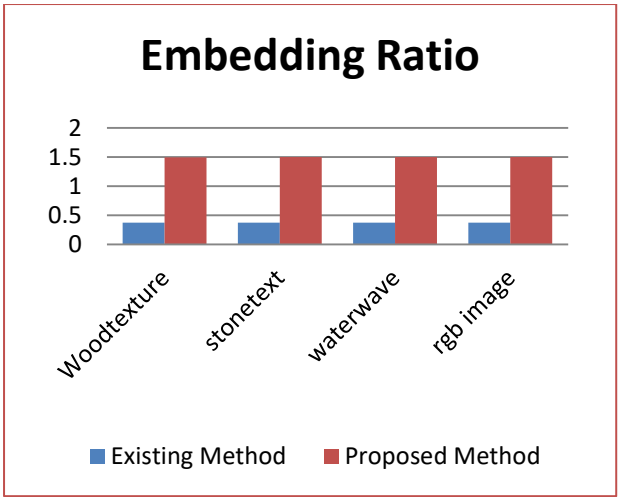

Figure 17. Graph showing embedding ratios.

V. CONCLUSION

Image steganography is the process of embedding secret information into the cover image. A robust secure lossless image steganography using spiral scan has been proposed. Three grayscale images are embedding into an RGB cover image. The proposed method giving good embedding ration compared with existing method. It is applicable to png and raw images. If lossy version is considered, it results to high embedding ratio and high embedding capacity than the lossless version. It can be further extended to random cover images.

REFERENCES

[1] Petitcolas, F.A.P., Anderson, R.J. & Kuhn, M.G., *"Information Hiding – A survey"*, Proceedings of the IEEE, 87:07, July 1999.

[2] Wang, H & Wang, S, *"Cyber warfare: Steganography vs. Steganalysis"*, Communications of the ACM, 47:10, October 2004.

[3] Pranab Garg, Jaswinder Singh Dilawari, *"A Review Paper on Cryptography and Significance of Key Length"*, IJCSCE Special issue on"Emerging Trends in Engineering ICETIE 2012.

[4] Chandramouli, R., Kharrazi, M. & Memon, N., *"Image steganography and steganalysis: Concepts and Practice"*, Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.

[5] Sumeet Kaur, Savina Bansal, *"Steganography and Classification of Image Steganography Techniques"*, Published in: Computing for Sustainable Global Development (INDIACom), 2014 International conference.

[6] Gaurav Vijayvargiya, Dr. Sanjay Silakari, Dr.Rajeev Pandey, *"A Survey: Various Techniques of Image Compression"*, (IJCSIS) International Journal of Computer Science and Information Security, *Vol. 11*, No. 10, October 2013.

[7] Rashi Singh, Gaurav Chavla, *" Data Hiding at 7th bit (RGB) with cryptography"*, IJCSMC, *vol 3*, issue 5, may 2014.

[8] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[9] Shreelekshmi R, Wilscy C, Madhavan V. *"Cover image preprocessing for more reliable LSB replacement steganography"*. In: Proc. of International Conf. on Signal Acquisition and Processing; 2010. p. 153–56.

[10] S.S.Maniccama, N.G.Bourbakis, "Image and video encryption using SCAN patterns" Pattern Recognition Volume 37, Issue 4, April 2004, Pages 725-737.

Authors Biographies

Dr.S.Kiran is Assistant Professor in the department of Computer Science and Engineering at Yogivenama University , Proddatur. He acquired M.Tech Degree from Nagarjuna University, Guntur. He completed Ph.D in computer science from S.K.University. He has been continuously imparting his knowledge to several students in research activities. He published many articles National and International journals. His research areas are image Processing, Cryptography and Network Security, Software Engineering and Data mining and Data ware house.

R. Pradeep Kumar Reddy received his B.Tech. Degree in Computer Science and Engineering from Bellary Engineering College, Bellary (VTU)., M.Tech. Degree in Computer Science and Engineering at S.R.M University, Chennai and currently pursing PhD. from Yogi Vemana University under the esteemed supervision of Dr. C. Naga Raju. Currently He is working as Assistant Professor in the Department of CSE at YSR Engineering College of Yogi Vemana University, Proddatur. He has got 12 years of teaching experience. He has published 10 research papers in various National and International Journals and about 8 research papers in various National and International Conferences. He has attended 10 workshops. He is a member of ISTE.

Dr. A. Ashok Kumar, Assistant Professor, Department of Physics at Y.S.R. Engineering College of Yogi Vemana University, Proddatur. He completed Ph.D from Department of Physics, Sri Venkateswara Unviversity, Tirupati. His areas of research includes Material Science and fabrication of semiconductor devices, Corrosion of Metals, applications of image processing in Engineering.

N.Subramanyan, Academic Consultant, Department of CSE at Y.S.R. Engineering College of Yogi Vemana University, Proddatur. He completed M.Tech. degree in Information Technology from RGM College of Engineering and Technology, Nandyal. His areas of research includes image processing, cryptography and network security.