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

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Secure Image using Steganography

G. Saranya[1], N. Pravaeena[2]

Student, Department of Computer Applications, Pioneer College of Arts and Science, Coimbatore, India[1,2]

Abstract: Information security is one of the most exigent problems in today's technological world. In order to secure the transmission of secret data over the public network (INTERNET) various schemes have been presented to the last decennium. Stenography combined with cryptography, can be one of the best choices for solving this problem. This paper advance a new steganographic method based on the gray-level modification for true color images using image reciprocity, secret key and cryptography.

Keywords: Steganography, grapters, Network, Encrypt, Decrypt.

I. INTRODUCTION

Today's stenography systems are used to multimedia objects like image,audio,video,etc.,as Cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message.

In simple words it would be like that, hiding information into other information's. Stenography hiding information and cryptography protecting information are totally different from one to another. Due to invisibility or hidden factor is it difficult to recover information without known procedure in stenography. Depending on the type of the cover object there are many suitable steganography techniques which are followed in order to obtain security.

STEGNOGRAPHY

Taking the cover object as image in stenography's known as image steganography. Generally, in this technique pixel intensities are used to hide information.

NETWORK STEGANOGRAPHY

When taking cover object as network protocol, such as TCP, UDP, ICMP, IP ETC., Where protocol is used as carrier, is known as network protocol steganography can be achieved in unused header bits of TCP/IP fields.

VIDEO STEGANOGRAPHY

Video steganography is a technique to hide any kind of files or information into digital video format. Video is used as carrier for hidden information. Generally Discrete Cosine Transform (DCT) alters values.

II. LITERATURE REVIEW

The existing method is a new robust approach to map secret data to one of the three channels of the RGB image. The proposed method uses the idea of transposition, bitxoring, bits shuffling, secret key, and cryptography two designs and advance steganogrphic system [13]. Multiple security level:

1) All the three channels of the input carrier image are transposed before they can be used to map secret data in order to receive the attacker. The secret key and secret data is encrypted using multiple encryption algorithms that are applied on it one after another. Secret data is mapped to blue channel of the carrier image using gray-level modification method (GLM).

2) The proposed method uses to different modules named as encryption modules

3) mapping diagrammatic representation of the proposed frame work.

Secret key and secret data module:

1) Select the secret data and a suitable secret key for encryption.

2) Convert the secret key into one-dimensional (1-D) array of bits.

3) Apply the bitxor operation on these bits with logical 1.

4) Shuffle these encrypted bits such that the bits with even and odd indices are interchanged.

5) If secret key bit=1

Then perform bitxor operation of secret message bit with logical 1.

Else

Do not perform bitxor operation.

End if

6) Repeat step 4 until all secret data bits are encrypt

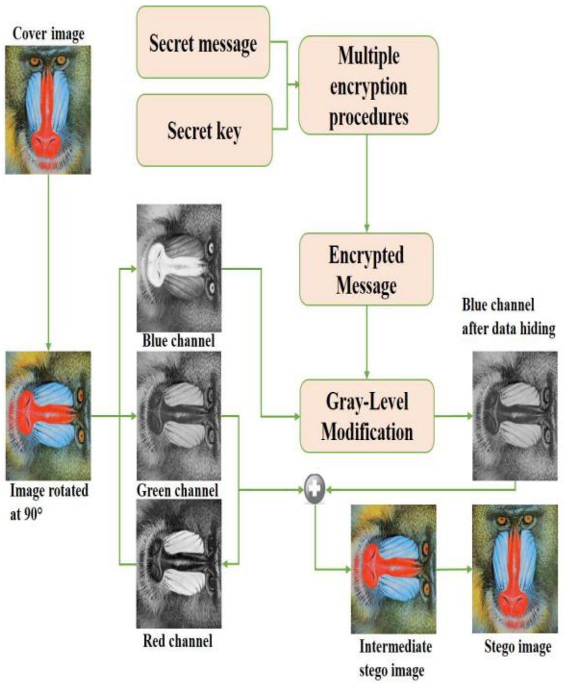

Fig. 1 Over all Pictorial Representation of Proposed Framework

III. ENCRYPTION MODULE

This module is responsible to encrypt both the secret key and secret data .the final output of this, module is encrypted form hide information into the image.

Embended algorithm

Input: Cover colour image, secret key, and secret data
Output: Stego image
1) Select the color cover image and divide it into red, green, and blue channels
2) Apply image transpose on all the three channels of the input image
3) Encrypt the secret key and secret data according to the encryption module
4) If the first bit of secret data=1
Then convert all pixel values of blue channel to odd by adding 1
Else
Convert all pixel values of blue channel to even by adding 1
Map the secret data of step 4 based on secret key bits (SKB) such that
5) if SKB=0 && pixel value=even OR SKB=1 && pixel value=odd

Then leave the pixel unchanged
Else if SKB=0 && pixel value=odd
subtract 1 from pixel value 7
Else if SKB=1 && pixel value=even
Then add 1 to pixel value

6. Repeat step 5 until all secret bits are mapped with the gray-levels of carrier image

7. Take the transpose of all three planes and combine them to make the stego image

Extraction Algorithm

Input: Steno image, secret key
Output: Secret data
1) Select the color stego image and divide it into red, green, and blue channels
2) Apply image transpose on all the three channels of the stego image
3) Extract LSB of the blue channel
4) Repeat step 3 until all secret bits are successfully extracted
5) Decrypt these bits by applying the reverse method of encryption module to get the origina text

IV. RESULTS AND ANALYSIS

This section presents the experimental results based on various image quality assessment metrics for performance evaluation. The proposed method is compared with the Karim et al. method [40] and are implemented using MATLAB R2013a. The evaluation is done using multiple experiments from different perspectives on different standard color images of varying dimensions.
For example, one experiment is to embed a text file of eight kilobyte (8KB) in different standard color images of dimension (256×256) like Lena, baboon, peppers, army, airplane, building, and house. Another experiment is to embed in table 1.

The PSNR values for the proposed algorithm are greater than the Karim' et al. [40] algorithm which shows high quality of stego images. Similarly, the MSE values of the proposed algorithm are small as compared to the Karim et al [40] method. Furthermore, the RMSE scores of proposed method are smaller than the Karim et al. [40] method. This means that the proposed algorithm provides promising results in terms of PSNR, confirming its better performance.
The comparison graph of the proposed method and the Karim et al. [40] method is shown in Figure 2.

The graph is drawn on the basis of fifteen different smooth and edgy images. The PSNR values are shown on the y-axis and image names on the x-axis. The graph clearly shows that there is up and down in the values of PSNR of the Karim et al. [40] method but the values of PSNR in the proposed method are almost the same and do not vary significantly. This verifies that the proposed method performs well for all types of images(edgy and smooth) as compared to the Karim et al [40] method.

Table 2 shows the comparison of both methods using PSNR with variable amount of cipher that is embedded in the standard colour image (baboon) of the same dimension (256×256).

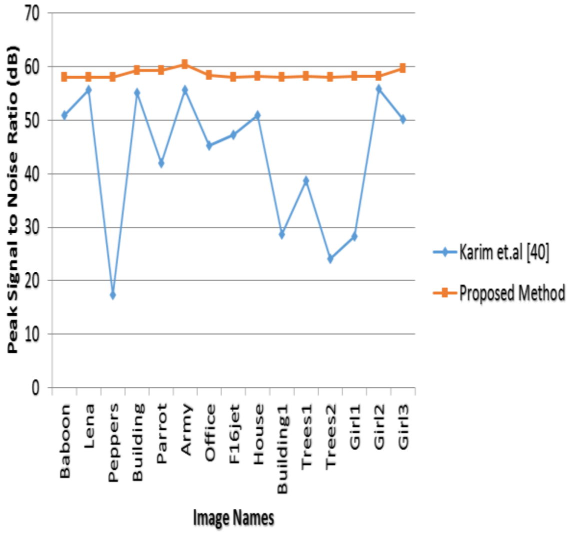

Fig. 2 Comparative Analysis of both methods using PSNR by HVS

Table 2 clearly shows that the proposed method gives more PSNR score as compared to the Karim et al. [40] method. Similarly, the comparative analysis graph of both the methods with variable amount of cipher embedded in a standard colour image of the same dimension is shown in **Figure 3.** The graph is drawn on the basis of PSNR values of **Table 2**.

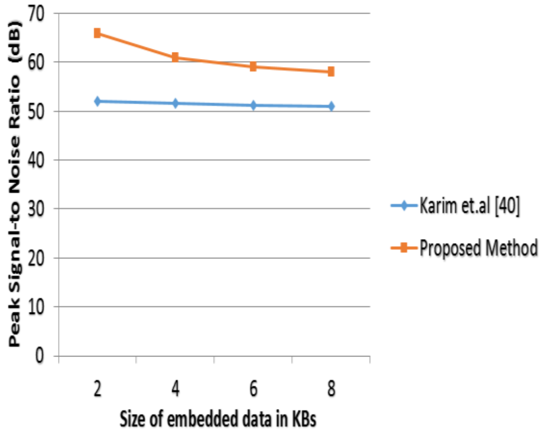

Fig. 3 Comparative analysis using PSNR with variable amount of embedded cipher

The comparative graph of the proposed algorithm as compared to the Karim et al. [40] algorithm clearly shows its better results in terms of PSNR which validate the effectiveness of the proposed method. The method but the PSNR score of the proposed algorithm is increasing as the image size is increased. Similarly, the comparative graph of both methods using PSNR with variable dimensions, same image and same amount of cipher embedded is also shown in **Figure 3** which vividly describes the effectiveness of the proposed technique.

The similarity between two images can be measured by using the correlation function. NCC is a statistical error metric that has been used to measure the similarity between two digital images in this research work. **Table 3** shows NCC for both the algorithms. If the NCC value is unity, both images become identical to each other. The value of NCC in **Table 3** close to unity shows that both the images are similar and differences are small.

Table 3 clearly shows that the NCC values for the proposed algorithm in all cases are greater than the Karim et al. [40] algorithm. This shows that the proposed algorithm provide better results in terms of NCC also and verifies its effectiveness.

V. CONCLUSION

In this paper, a new method is proposed to map secret data to the gray-levels of the carrier image by utilising the concepts of transposition, bitxoring, bits shuffling, secret key, and cryptography with high imperceptibility and security. An average PSNR of 58dB, RMSE with 0.6673, and NCC with 0.9917 is achieved using the proposed method which are better than the existing method in the literature with PSNR=40, RMSE=0.8115, and NCC=0.981. The proposed method improved the security as well as the quality of stego images and provided promising results in terms of high PSNR, NCC, and less histogram changeability as compared to existing methods.

The distinguishing properties of the proposed algorithm include transposition, bitxoring, and bits shuffling, adding multiple security levels to the proposed method. These different security levels create multiple barriers in the way of an attacker. Therefore, it is difficult for a malicious user to extract the actual secret data.

REFERENCES

[1] Chang Y-T, Wu M-H, Wang S-J. Steganalysis to Data Hiding of VQ Watermarking Upon Grouping Strategy. In: Information and
M, Mehmood I, Baik SW. Image Super-resolution Using Sparse Coding Communi[cation Technology, Springer, 2014. p. 633-642.

[2] Sajjad Over Redundant Dictionary Based on effective Image Representations. J Visual Commun Image Rep 2015;26(1):50-65.

[3] Qin C, Chang C-C, Chiu Y-P. A Novel Joint Data-Hiding and Compression Scheme Based on SMVQ and Image Inpainting. IEEE Trans Image Process 2014;23(3):969-978.

[4] Cheddad A, Condell J, Curran K, Kevitt PMc. Digital Image Steganography: Survey and Analysis of Current Methods. Sig Process 2010;90(3):727-752.

[5] Hamid N, Yahya A, Ahmad RB, Al-Qershi OM. Image Steganography Techniques: An Overview. Int J Comp Sci Secu 2012;6(3):168-187.

[6] Liao X, Shu C. Reversible Data Hiding in Encrypted Images Based on Absolute Mean Difference of Multiple Neighboring Pixels. J Visual Commun Image Rep 2015;28(3):21-27.

[7] Sajjad M, Ejaz N, Baik SW. Multi-kernel Based Adaptive Iterpolation For Image Super-resolution. Multi Tool App 2012;72(3):2063-2085.

[8] Jamil Ahmad NUR, Jan Z, Muhammad K. A Secure Cyclic Steganographic Technique for Color Images using Randomization. Tech J Uni Engg Tech Taxila 2014;19(3):57-64.

[9] Qazanfari K, Safabakhsh R. A New Steganography Method which Preserves Histogram: Generalization of LSB< sup>++</sup>. Info Sci 2014;277(7):90-101.

[10] Yang C-H, Weng C-Y, Wang S-J, Sun H-M. Adaptive Data Hiding in Edge Areas of images With Spatial LSB Domain Systems., IEEE Trans Info Forens Sec 2008;3(3):488-497.

[11] Zhang W, Zhang X, Wang S. A Double Layered “Plus-Minus One” Data Embedding Scheme. Sig Process Let, IEEE 2007;14(11):848-851.

[12] Mielikainen J. LSB Matching Revisited. Sig Proces Let, IEEE 2006; 13(5):285-287.

[13] Roy R, Sarkar A, Changder S. Chaos Based Edge Adaptive Image Steganography. Procedia Tech 2013;10(1):138-146.

[14] Hong W. Adaptive Image Data Hiding in Edges Using Patched Reference Table and Pair-Wise Embedding Technique. Info Sci 2013;221(1):473-489.

[15] Chen W-J, Chang C-C, Le T. High Payload Steganography Mechanism Using Hybrid Edge Detector. Exp Sys App 2010;37(4):3292-3301.

[16] Ioannidou A, Halkidis ST, Stephanides G. A Novel Technique for Image Steganography Based on a High Payload Method and Edge Detection. Exp Sys App 2012;39(14):11517-11524.

[17] Luo W, Huang F, Huang J. Edge Adaptive Image Steganography Based on LSB Matching Revisited. IEEE Trans Info Forens Sec 2010;5(2):201-214.

[18] PhD student, Digital Contents Research Institute, Sejong University, Seoul, Korea.

[19] PhD student, Digital Contents Research Institute, Sejong University, Seoul, Korea.

TABLE I. COMPARISON OF METHODS USING PSNR, MSE & RMES WITH DIFFERENT IMAGES

S.No.	Image Name	Karim et al., Method	Result	Karim et al., Method	Result	Karim et al., Method	Result
		PSNR (dB)		MSE		RMSE	
1	Baboon	50.8811	58.0648	0.5121	0.4487	0.7156	0.6698
2	Lena	55.6551	58.0362	0.4682	0.4490	0.6842	0.6700
3	Peppers	17.3893	58.0362	1.4984	0.4490	1.2240	0.6700
4	Building	55.1595	59.3242	0.4724	0.4392	0.6873	0.6627
5	Parrot	41.9414	59.3242	0.6212	0.4392	0.7881	0.6627
6	Army	55.6788	60.3252	0.4680	0.4319	0.6841	0.6571

TABLE II. COMPARISON OF METHODS USING PSNR WITH VARIABLE AMOUNT OF EMBEDDED CIPHER

Image name	Cipher size in bytes	Cipher size in bits	Karim et al., method	Proposed method
	PSNR (dB)		**PSNR (dB)**	
Baboon with dimension 256×256				
2	2406	19248	52.0373	65.9333
4	4177	33416	51.6345	60.8388
6	6499	51992	51.1776	59.0243
8	8192	65536	50.8811	58.0648

TABLE III. COMPARISON OF BOTH METHODS USING NCC WITH DIFFERENT IMAGES

S.No.	Image Name	Karim et al., Method	Proposed Method
		NCC	
1	Baboon	0.9998	0.9999
2	Lena	0.9999	0.9999
3	Peppers	0.7859	0.9093
4	Building	0.9999	0.9999
5	Parrot	0.9991	0.9995
6	Army	0.9999	0.9999
7	Office	0.9998	0.9999
8	F16jet	0.9997	0.9998