IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-8, Aug 2018 E-ISSN: 2347-2693

Improving Two-Layer Data Security in Image Steganography

A. Kaur, J. Kaur

Deparatment of Computer Engineering, Punjabi University Patiala, Patiala, India
Deparatment of Computer Engineering, Punjabi University Patiala, Patiala, India

*Corresponding Author:amarjeetk571@gmail.com, Tel.: 9878756450

Available online at: www.ijcseonline.org

Accepted: 17/Aug/2018, Published: 31/Aug/2018

***Abstract*—**In this paper, two security layers are added on the data using cryptography and steganography algorithms. The data is encrypted using lightweight RECTANGLE algorithm. Next, the data is hiding is done using steganography algorithm. In the steganography scheme, the edges of the cover image are determine using Canny Edge detection technique which can extract inclusive range of edges. Further, worked on theory of color which plane is more suitable for maximum/minimum data hiding. The encrypted data is splitted into 3:2:3 ratio and hide in the edges of the RGB plane simultaneously. The performance analysis is done based on PSNR and embedding capacity. The experimental results show that the Improved technique is secure, consume lesser area, less embedding capacity, and provide high PSNR. Further, data extraction is possible without communicating any extra information with stego image.

***Keywords*—**Canny Edge Detection, RECTANGLE, PSNR, Multi-Layer Security

I. INTRODUCTION

In the current scenario, number of digital data files are communicated on the internet in various applications such as in the social network, biometric systems and in the military [1]. The sensitive data required security while communicating on the internet. In the data security, cryptography and steganography techniques are used. In the cryptography the sensitive data are converted into encrypted form using a key. On the other side, in the steganography these sensitive data are hidden. The block diagram for two-layer security system, steganography with cryptography is shown in Fig. 1

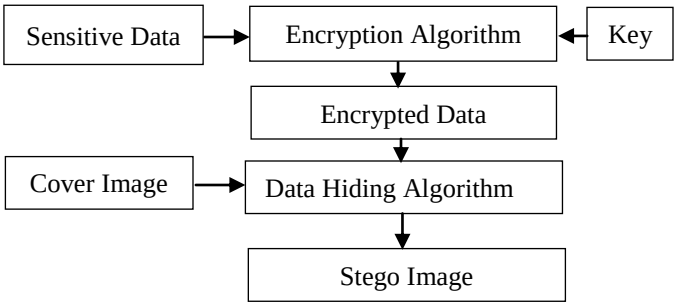


Fig. 1 Two-Layer Security System

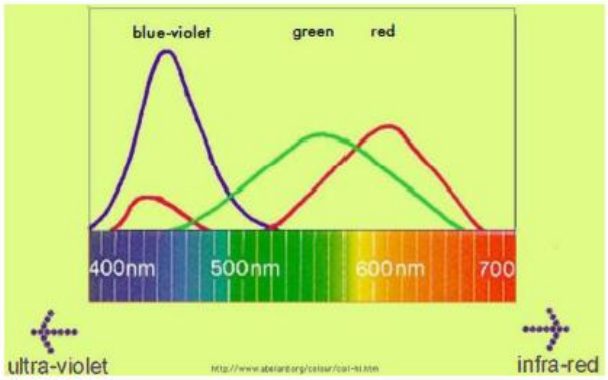


Fig. 2 Color Wavelength

In the Fig. 1 the first layer of security is added on the sensitive data using cryptography algorithms. Further, steganography algorithm, hide the data in the cover image and provide the second layer of security.

In the image steganography, color RGB images are more preferred for data hiding because of security and large capacity. The proper selection of which plane is suitable for data hiding diminish the visual attacks. According to theory of color the expert says that human eyes have four light receptors [2]. The rods are sensitive to black, white, and gray shades. On the other side, cones are sensitive to various colors. As shown in the Fig. 2 the eyes are less sensitive to blue-violet as compared to red and green color. Hence,

variation in blue color pixel intensity give less attention to human eyes. Hence, in the improved technique take care of these parameters steganography system is designed.

In the improved steganography system, 2 layers of security on secret data is applied. In the first layer the data is encrypted using RECTANGLE algorithm and in the second layer the data is splitted into 3:2:3 ratio and data embedding is done in the edges of the cover image by taking care of color wavelength, which color is more/less sensitive.

The remaining of the paper as follow. The related survey and motivation is explained in the section II. Section II defined the improved steganography system in detail. The experimental results and performance analysis is explained in the section IV. In last conclusion is done in the section V.

II. RELATED WORK

In this section, a study on cryptography and steganography techniques is done to design an improved security system. Our survey is gone in three direction selection of cryptography algorithm, edge detection technique, and data embedding ratio for improve capacity with less visual effect.

In the cryptography, for security purposes number of algorithms that includes DES [3], Blowfish [4], AES [5] are deployed for the security purposes. The AES algorithm is more popular because of security and recommended by NIST. Further, these algorithms are consumed large area, so NIST started a program on lightweight cryptography which consume lesser area. In the lightweight cipher RECTANGLE provide security in less number of rounds [6].

Further, for edge detection Sobel [7], Canny [8], Prewitt [9], Fuzzy [10] edge detection techniques are deployed for detect edges in the steganography techniques. The canny edge technique gains popularity as compared to other techniques because it extracts wide range of edges regardless the noise present in the image [8].

Next, a study on different data embedding ratio is done. Dasgupta, et al. [11], proposed hash based LSB technique for video steganography. They have done data embedding in 3:3:2 ratio for improving the payload capacity. Further, they have designed [12], chaos theory based security system. In which data encrypted is done using chaos theory and data hiding in 3:3:2 ratio. Next, G.R. Manjula and AjitDanti [13], changed the ratio 2:3:3 for data embedding and proposed improved version of hash based LSB technique. Next, Amritpal Singh and Harpal Singh [2], designed a 2:2:4 ratio techniques for improve embedding capacity in RGB plane by taking care of visual affect. In their experimental results, they have achieved high PSNR as compared to LSB technique and 1:3:4 ratio for data set images lena, baboon. jpg.

The study shows that RECTANGLE and Canny edge detection technique is best for data encryption and edge detection. Further, the 3:3:2 ratio provide best PSNR as compared to other ratios (2:2:4, 1:3:4). Therefore, in this paper an improved steganography algorithm is designed in which encryption is done using lightweight RECTANGLE cipher and based on color theory 3:3:2 ratio is selected which provide less visual affect and easy to extract secret data without communicating extra information.

III. PROPOSED WORK

In this section, improved two-layer security system as shown in Fig. 3 and its blocks are explained in detail.

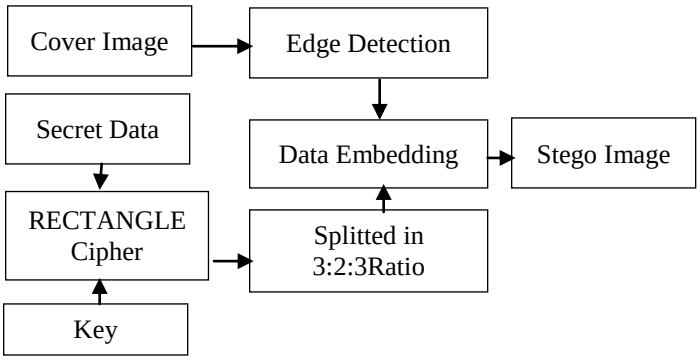


Fig. 3 Improved Steganography System

- RECTANGLE Cipher

RECTANGLE cipher is based on substitution-permutation network and process in the block size of 64bit. The cipher support 2 key variants 80/128 bit and takes 25 rounds to complete the encryption process. The algorithm is software as well as hardware efficient [6]. The RECTANGLE cipher consumes lesser area for s-box as compared to the AES. The pseudocode is given below.

Table 1 Pseudo-code for RECTANGLE

Key Generation
1. Apply the S-box to the bits intersected at the 4 uppermost rows and the 4 rightmost columns.
2. Applying a 1 round generalized Feistel Transformation.
Row0'=(row0<<8) XOR Row1
Row1'=Row2
Row2'=Row4
Row3'=(Row3<<12) xOR Row4
Row4'=Row0
3. A 5-Bit Round Constant RC[i] is XORed with the 5 bit Key State.
Encryption Algorithm
Generate RoundKeys()
For i=0 to 24 do
{
Add-Round Key (State, K_i)
Sub-Column (State)
Shift Rows(State)
}
Add-Round Key (State, K_{25})

- Canny Edge Detection Technique

The Canny edge detection is a multi-stage algorithm that can extract a wide range of edges in images regardless of the noise present in them [8]. The Canny edge detection algorithm has the following five stages:

1. Smoothing: Blur the image to eliminate noise.
2. Searching for gradients: Find the edge strength in the image by taking the gradient with large magnitudes.
3. Non-maximum suppression: Mark local maxima as edges.
4. Double thresholding: Find possible edges by computing thresholding.
5. Edge linking: Final edges are found by discarding all edges that are not connected to strong edges.

- 3:2:3 Ratio

In the improved technique, the data is splitted into 3:2:3 ratio. The ratio 3 bit data in red plane, 2 bit data is hide in the green plane, and 3 bit data hide in blue plane while considering the color perception. The 3:2:3 ratio technique is explained with example in Table 1-3. In the Table 2 the RGB plane pixels are shown. In the Table 3 the secret 8bits are splitted into 3:2:3 ratio. In the Table 4 the splitted data bits are hide in the stego image. In the ratio 2-bit hide give 4, 3-bit hide give 8 maximum variability.

Table 2 Cover Color Image Pixels

Red Plane	Green Plane	Blue Plane
10110011	01010101	11111110
00000001	11000110	00000111
00011100	00000111	11111100

Table 3 Secret Data Bits

Secret Data	3	2	3
10110011	101	10	011
11110001	111	10	101
01100101	011	00	101

Table 4 Stego Color Image Pixels

Red Plane	Green Plane	Blue Plane
10110**101**	01010**110**	11111**011**
00000**111**	11000**110**	00000**101**
00011**011**	00000**100**	11111**101**

- Data Embedding and Extraction

The overall data embedding pseudocode is explained in Table 5.

Table 5 Pseudocode for Data Embedding

1. Read the cover image and extract RGB planes.
2. Detect the edges using Canny Edge Detection Technique.
3. Read the secret data and encrypted using RECTANGLE algorithm.
4. The data split into 3:2:3 ratio for data embedding in RGB plane simultaneously.
5. By taking care of visual affect, the secret data 3 bits embed in red plane, 2 bit in green, and 3 bit in blue plane using LSB technique.
6. The Performance analysis is done using PSNR and embedding capacity.

The overall data extraction pseudocode is explained in the table 6.

Table 6 Pseudocode for Data Extraction

1. Read the stego image and extract RGB planes.
2. Detect the edges using Canny Edge Detection Technique.
3. Extract the data bits from the edges in the RGB plane.
4. The splitted bits are concatenate and RECTANGLE decryption algorithm is applied.

IV. Experimental Results

In this section, on different dataset images [14], the improved technique is applied to evaluate the performance. The analysis is done on the basis of PSNR and embedding capacity. The parameters are explained below.

- PSNR

This parameter measured the quality of stego image, due to distortion produced in the cover image after data hiding [15]. It is determined as follow.

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

Here, A represent the maximum intensity found in the image and MSE is determined as follow.

$$\text{MSE}=\frac{1}{CD}\sum_{i=1}^{C}\sum_{j=1}^{D}|M(i,j)-N(i,j)|^2$$

Here, M and N represent the cover and stego image and CD resolution of the image.

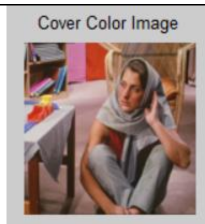
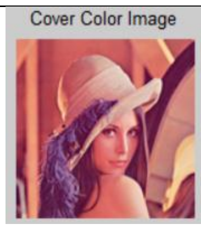
- Embedding Capacity

The total number of bits are embedded in the cover image is known as embedding capacity. In our work, on each edge pixel, 8 bits of secret data bits in the ratio of 3:2:3 hide simultaneously in RGB plane. Hence, embedding capacity is found as follow for our work.

Embedding Capacity=Total number of Edges x 8

In the Table 7, visual impact is shown for various image and results show that stego image looks similar to cover images.

Table 7 Visual Impact between Cover and Stego RGB planes

Cover Image	Stego Image
	
	
	
	

In the Table 8, different images PSNR and embedding capacity is measured and Barbara image have maximum embedding capacity and least PSNR.

Table 8 PSNR and Embedding Capacity

Images (.jpg)	Red Plane PSNR (dB)	Green Plane PSNR(dB)	Blue Plane PSNR(dB)	Average PSNR(dB)	Embedding Capacity
Baboon	48.90	56.24	49.07	50.36	6128
Barbara	45.20	52.18	45.15	46.52	14888
Lena	46.51	53.55	46.51	47.86	10840
Pepper	46.53	53.54	46.40	47.78	11120

In the Table 9, same dataset image is applied on 1:3:4 ratio and 3:2:3 ratio. The result reflect that 3:2:3 ratio better PSNR as compared to 1:3:4 ratio.

Table 9 Comparative Analysis

Images	1:3:4 Ratio PSNR (dB)	3:2:3 Ratio PSNR (dB)
Baboon	49.38	50.36
Barbara	45.49	46.52
Lena	46.70	47.86
Pepper	46.76	47.78

V. CONCLUSION

In this paper, an improved image steganography algorithm is design using cryptography and steganography technique. In our work, proper selection of algorithm, visual impact is taken under consideration and found that RECTANGLE cipher consumes lesser area as compared to other cipher. Further, 3 bits in the red, 2 bits in the green, and 3 bits are in the blue plane are embed. The experimental results show that improved steganography system has better PSNR, secure as compared to other ratio.

REFERENCES

[1] Rajendran, Sujarani, and ManivannanDoraipandian. "Chaotic Map Based Random Image Steganography Using LSB Technique." International Journal of Network Security, vol. 19, no. 4, pp. 593-598, 2017.

[2] Amrital Singh and Harpal Singh, “An improved LSB based image steganography technique for RGB images,” IEEE International Conference on Electrical, Computer and Communication Technologies, August 2015.

[3] Panghal, Sandeep, Sachin Kumar, and Naveen Kumar. "Enhanced Security of Data using Image Steganography and AES Encryption Technique." International Journal of Computer Applications Recent Trends in Future Prospective in Engineering & Management Technology 2016.

[4] Patel, Komal, SumitUtareja, and Hitesh Gupta. "Information hiding using least significant bit steganography and blowfish algorithm." International Journal of Computer Applications, vol. 63, no. 13, 2013.

[5] Ramaiya, Manoj, Naveen Hemrajani, and Anil Kishore Saxena. "Secured steganography approach using AES." International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR), vol. 3, pp. 185-192, 2013.

[6] Zhang, Wentao, et al. "RECTANGLE: a bit-slice lightweight block cipher suitable for multiple platforms." Science China Information Sciences vol. 58, no.12, pp. 1-15, 2015.

[7] Li, Li, et al. "A color Images steganography method by multiple embedding strategy based on Sobel operator." 2009 International Conference on Multimedia Information Networking and Security. IEEE, 2009.

[8] Bassil, Youssef. "Image steganography based on a parameterized canny edge detection algorithm." arXiv preprint arXiv:1212.6259, 2012.

[9] Chen, Wen-Jan, Chin-Chen Chang, and T. Hoang Ngan Le. "High payload steganography mechanism using hybrid edge

detector." Expert Systems with applications, vol. 37, no. 4, pp. 3292-3301, 2010.

[10] Goodarzi, Mahdi Hassani, ArashZaeim, and Amir Shahab Shahabi. "Convergence between fuzzy logic and steganography for high payload data embedding and more security." Telecommunication Systems, Services, and Applications (TSSA), 2011 6th International Conference on. IEEE, 2011.

[11] Kousik Dasgupta, J.K. Mandal, and Paramartha Dutta, "Hash based Least Significant Bit Technique for Video Steganography," International Journal of Security, Privacy, and Trust Management, vol. 1, pp. 1-11, April 2012.

[12] Debiprasad Bandyopadhyay, Kousik Dasgupta, J.k. Mandal, Paramartha Dutta, "A Novel Secure Image Steganography Method Based on Chaos Theory in Spatial Domain," International Journal of Security, Privacy, and Trust Management, vol. 3, pp. 11-22, February 2014.

[13] G. R. Manjula and AjitDanti, "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography in Spatial Domain," International Journal of Security, Privacy, and Trust Management, vol. 4, pp. 11-20, Februry2015.

[14]http://sipi.usc.edu/database/database.php?volume=misc&image=13#top

[15] Muhammad, Khan, et al. "Image steganography for authenticity of visual contents in social networks." Multimedia Tools and Applications, vol. 76, no. 18, pp. 18985-19004, 2017.

Authors Profile

A .Kaur completed Bachelor of Technology from Baba Banda Singh Bahadur Engineering college Fatehgarh Sahib, affialated by Punjab Technical University ,Jalandhar in 2012 and Pursuing Master of Technology from deparatment of Computer Engineering, Punjabi University patiala. My main research work focuses on cryptography and steganography algorithms.

J. Kaur completed Bachelor of Technology and Master of Technology. She is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Engineering, Punjabi university patiala. She has published 35 research papers in reputed international journals and conferences including IEEE. Her area of specilaization is Networking Wireless.

