ISSN: 2278 – 909X
International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE)
Volume 5, Issue 9, September 2016

DOUBLE TIER SECURITY SYSTEM FOR DATA COMMUNICATION

Jasanpreet Kaur[1] Sukhjinder Singh[2]

***Abstract*-Security of transmitted data is major concern in present time, so that it cannot be intercepted by unauthorized person. There are various techniques available for hiding information in different cover media. Cryptography is refers of transmitting the information securely over the internet so that it will be complex for an attacker to attack private information. Steganography refers to the science of "invisible" communication. The main aim of Steganography means the secret message can get hided in another file called cover medium in such a way that no one apart from the authorized user can even notice that there is a secret message inside it. To developed high security model by combining cryptography and Steganography techniques. In Cryptography, data is encrypted by content based algorithm and then encrypted data hide in cover image for double tier security. For hiding the encrypted data Raster scan technique is used. By using these two techniques the security of secret data increases to two tiers and a high quality of stego image is obtained.**

***Keywords*—Steganography; Text Steganography, Raster scan technique, Cryptography; Content based algorithm, data hiding, RGB planes, MSE, PSNR and correlation factor.**

I INTRODUCTION

Due to the growth of internet technology, digital media such as images, video and text are shared and transmitted over the internet more conveniently [16]. However, one of the main challenges in sharing and transmitting any type of data over a public channel is data security [6]. The data security is major issue for communication like military, banking sector etc. Therefore, it becomes necessary to hide data using appropriate method before transmission. Cryptography and Steganography are the two techniques used for security purpose.

Cryptography is a technique used to secure data from unauthorized access when they transmitted over the network [14]. In cryptography the original text is transformed into the cipher text which makes the person unable to identify the message. But the size of cipher text is large than the plain text and it takes more time to encrypt the message. Cryptography is used to keep the message secret but it does not provide secrecy of the message. Steganography is a technique which convert communication to hide a message from a third party [13]. Steganography means the secret information can get hided in cover media. The cover media may be an image, video file. The cover media is referred as an object that holds the valuable data. The stego object is the output that is sent to the destination. Cryptography and Steganography are used for security purpose the difference between them is cryptography prevents the valuable data whereas steganography protect the cover of the message [3]. The implementation of cryptography technique includes the content-based encryption algorithm. This algorithm encrypt the plain text two times to generate the protected cipher text using bitwise binary addition operation [14]. The encrypted secret data is hiding into the cover image using Raster scan technique. In Steganography includes the Raster scan technique is selected because it is simple method of hiding information, easily understand by user and the data is hidden at first row from left to right then data is hidden from right to left in second row. Therefore, the probability of pixel variation has reduced. An unknown person wills not easy to extracts the secret data from cover image [17].

II METHODOLOGY

The cryptography and steganography security techniques are combined to give two tier securities to secret data. First important secret data is encrypted by using content-based encryption algorithm. Then encrypted data is embedded into cover media by using Raster scan steganography technique.

1. Cover media: The cover media that will hold the secret data that is to be hidden. In this paper image is taken as cover media.
2. Secret data: The secret data can be anything like data, file or image etc. In this paper text data is taken as secret data. The secret data is encrypted using content-based encryption algorithm by cryptography technique.

A. Content-Based Encryption Algorithm

The content-based encryption is well known algorithm of cryptography. This algorithm encrypt the plain text two times to generate the safe cipher text using bitwise binary addition operation. The content-based algorithm is using symmetric key for cryptography method. In Symmetric key cryptography dispatcher encrypts the plain text using a secret key and recipient decrypt the cipher text using the same key [14]. The content-based algorithm cryptography is well-known to be used in encrypting and decrypting text, e-mails and Doc files.

B. Raster Scan Technique Overview

In this technique, pixels are stored in first row from left to right then pixels are stored from right to left in second row. For example, pixels are stored in first row from left to right then pixels are stored from right to left in second row.

For example, pixels are stored in first row from left to right then pixels are stored from right to left in second row.

Table 1 original cover image pixels

00110011	10111011	11011011	00100100
11011000	00001111	11110000	11101110

Suppose the secret bits are 11001101 and cover image pixle value are:

Table 2 stego image pixels

0011001**1**	1011101**0**	1101101**1**	0010010**1**
→			
1101100**1**	0000111**1**	1111000**0**	1110111**0**
←			

III IMPLEMENTATION WORK

The purpose of the implementation scheme is to design high security model for security of secret information. Security of transmitted data is major concern in present time, so that it cannot be intercepted by unauthorized person. To avoid the problem of unauthorized data access steganography along with cryptography is the exact solution. To developed high security model by combining cryptography and Steganography techniques.

In this system cryptography and Steganography security is combined to give two tier securities to secret data. First important secret data is encrypted by using content-based algorithm cryptography. Then encrypted secret data is embedded into cover image by using Raster scan steganography technique.

A. Embedding Algorithm

Inputs: Encrypted secret data and cover image

Output: Stego image with secret data embedded in it.

1. Read the cover image and text secret data.
2. Extract their information.
3. Apply content-based algorithm cryptography technique on data for encryption.
4. The encrypted data bits brakes in 2:2:4 ratios into three planes Red, Green and Blue planes.
5. Hide encrypted data in two bits in Red, two bits in Green and the four bits in Blue plane into cover image using Raster scan steganography technique.
6. Calculate performance parameters like MSE and PSNR and correlation factor.

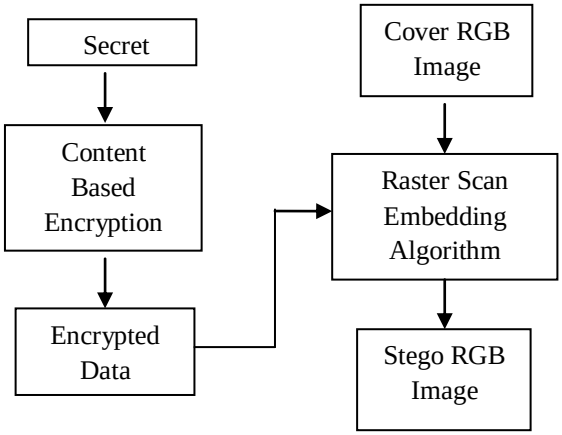


Figure1. Block diagram of embedding Procedure

B. De- Embedding Algorithm

Input: Stego image

Output: Secret data

1. Read the stego image
2. Split the stego image into Red, Green and Blue planes.
3. Read the cover image
4. Split the cover image into Red, Green and Blue planes.
5. Apply de-embedding algorithm to extract encrypted secret data
6. Extract the secret data.

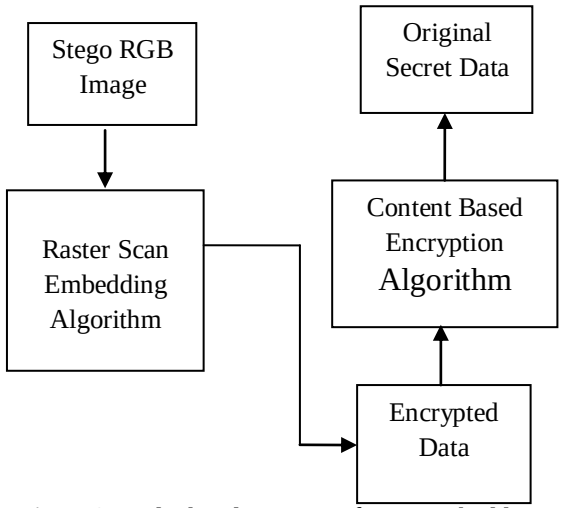


Figure2. Block diagram of De-embedding Procedure

IV EXPERIMENTAL RESULTS

This section presents and discusses the results obtained after implementing the content-based algorithm cryptography and Raster scan steganography methods. A system is designed and implementing in MATLAB, that shows the working of cryptography and steganography methods. For high security system using cryptography and steganography is tested by taking encrypted data and hiding them in order of 2:2:4 ratios into RGB planes of cover image using Raster scan technique. The high secured system using cryptography and steganography is tested by taking encrypted secret data is embedding into RGB planes of cover image. Four images namely Peppers.png, sunflower.jpg, vista.jpg and Pink.jpg have been used as cover image and four text files namely a.txt, b.txt, c.txt and d.txt (given in table 3 and table 4) has been used as secret data.

Table 3 Features of cover images

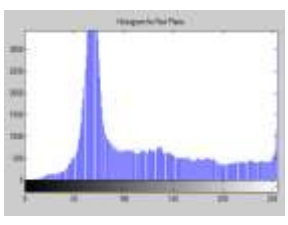
S No.	Cover image information		
	Name of image	Size (in KB)	Format
1.	Peppers.png	454KB	Png
2.	Pink.jpg	48.6 KB	Jpg
3.	Vista.jpg	48KB	Jpg
4.	Sunflower.jpg	18.3KB	Jpg

Table 4 Features of secret data

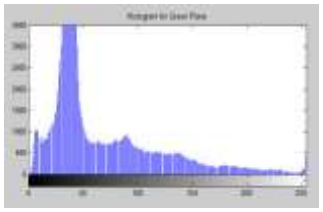
S No.	Secret data information		
	Name of secret data file	Size (in KB)	Format
1.	a.txt	2KB	Text
2.	b.txt	5KB	Text
3.	c.txt	7KB	Text
4.	d.txt	11KB	Text

For high security system using content based algorithm of cryptography secret data 2KB, 5KB, 7KB and 11KB is encrypted data and hiding them in order of 2:2:4 ratios into RGB planes of cover image using Raster scan technique of Steganography.

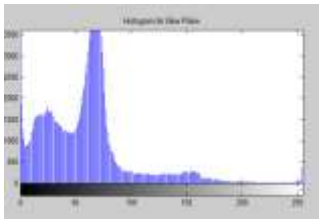
(a)



(b)

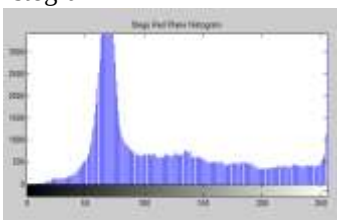


(c)

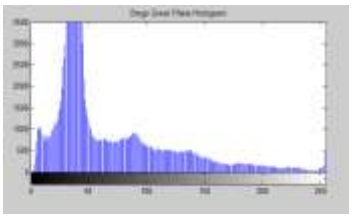


(d)

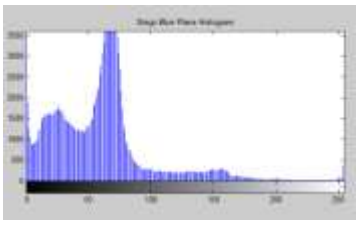
Figure 3: Results for cover image (Peppers.png): (a) Cover image (b) Red plane (c) Green plane (d) Blue plane of cover image corresponding their Histogram



(a)



(b)



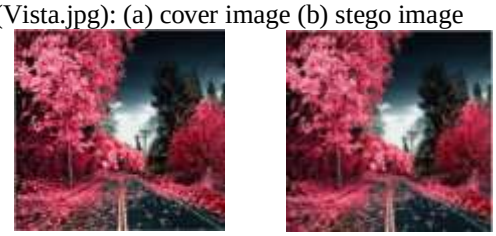
(c)

(d)

Figure 4: Results for stego image (Peppers.png): (a) Red plane (b) Green plane (c) Blue plane of stego image corresponding their Histogram (d) stego image

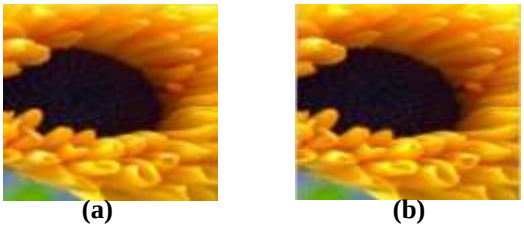
(a) (b)

Figure 5: Similarly Results for second image (Vista.jpg): (a) cover image (b) stego image



(a) **(b)**

Figure 6: Similarly Rresults for third image (pink jpg) (a) cover image (b) Stego image



(a) **(b)**

Figure 7: Similarly Results for fourth image (Sunflower jpg) (a) Cover image) (b) Stego Image

The histogram is a graph showing the number of pixels in an image at each different intensity values found in that image. The histogram for color image is represents the distribution of the composition of color in the image. It shows different types of colors appeared and the number of pixels in color image. The histogram for color image shows the brightness distribution of each individual Red, Green and Blue (RGB) planes. The histogram has been taken of color images. The individual histogram has been produced of Red, Green and Blue (RGB) planes for color image and compared with Red, Green and Blue (RGB) planes for stego image. The x axis of the histogram shows the range of pixel values and the y axis is the count of these pixel intensity values.

Figure 7: Similarly Results for fourth image (Sunflower.jpg

Table 5 Various performance parameters for secret text data using cover image Peppers.png

S No.	Secret data file	Secret data size	Capacity (in bits)	MSE	PSNR (in dB)	Correlation factor
1.	a.txt	2KB	196608	0.0525	60.9258	1.0000
2.	b.txt	5KB	196608	0.4371	51.7247	0.9998
3.	c.txt	7KB	196608	0.6129	50.2571	0.9980
4.	d.txt	11KB	196608	0.9634	48.2926	0.9979

Table 6 Various performance parameters for secret text data using cover image Sunflower.jpg

S No.	Secret data file	Secret data size	Capacity (in bits)	MSE	PSNR (in dB)	Correlation factor
1.	a.txt	2KB	140500	0.0669	59.8743	0.9923
2.	b.txt	5KB	140500	0.6044	50.3175	0.9935
3.	c.txt	7KB	140500	0.8586	48.7929	0.9994
4.	d.txt	11KB	140500	1.3442	46.8461	0.9946

Table 7 Various performance parameters for secret text data using cover image vista.jpg

S No.	Secret data file	Secret data size	Capacity (in bits)	MSE	PSNR (in dB)	Correlation factor
1.	a.txt	2KB	230400	0.0448	61.6146	1.0000
2.	b.txt	5KB	230400	0.3674	52.4800	0.9883
3.	c.txt	7KB	230400	0.5236	50.9410	0.9999
4.	d.txt	11KB	230400	0.8237	48.9729	0.9998

Table 8 Various performance parameters for secret text data using cover image Pink.jpg

S No.	Secret data file	Secret data size	Capacity (in bits)	MSE	PSNR (in dB)	Correlation factor
1.	a.txt	2KB	76800	0.1060	57.8764	0.9981
2.	b.txt	5KB	76800	1.1193	47.6412	0.9999
3.	c.txt	7KB	76800	1.5707	46.1698	0.9998
4.	d.txt	11KB	76800	2.4712	44.2017	0.9997

In order to analyze the distortion and error, calculated the MSE, PSNR and correlation factor for different size of cover image and secret data file. MSE is the Averaged Square difference between the above said cover media and secret object. Smaller the MSE, the steganography technique is more efficient. Whereas PSNR measure the maximum possible power of cover media and secret object. Higher the PSNR, the quality of stego object is better. Correlation factor is measure the similarity between the cover media and secret object.

The embedding capacity is measured in bits. The text secret data 2KB, 5KB, 7KB and 11KB hide in four cover images and calculated performance parameters MSE, PSNR and Correlation factor (refer table 5 to 8). The graph shows the values of performance parameters MSE, PSNR and Correlation factor**.**

When embedded secret data size is small, the value of PSNR is high and value of MSE is low (refer Figure 8 and Figure 9). According to the testing results, the smallest the file size (2 KB) has the value of PSNR is high and value of MSE is low. Moreover, the highest the file size (11 KB) has the value of PSNR is low and value of MSE is high (refer Fig 8 and Fig 9).

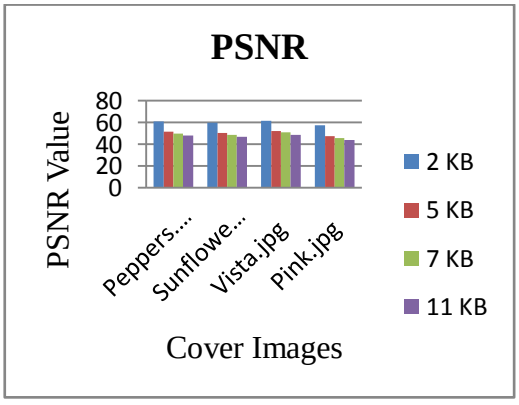


Figure 8 Histogram of PSNR

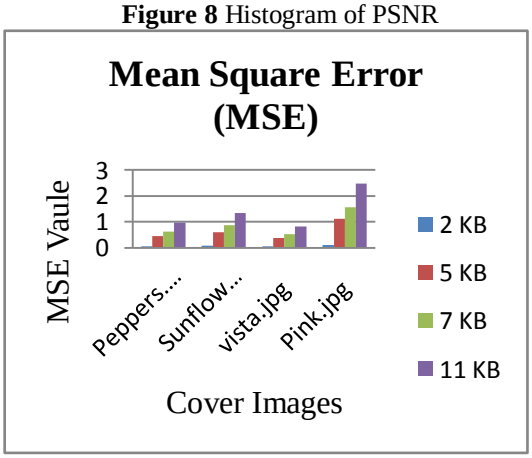


Figure 9 Histogram to MSE

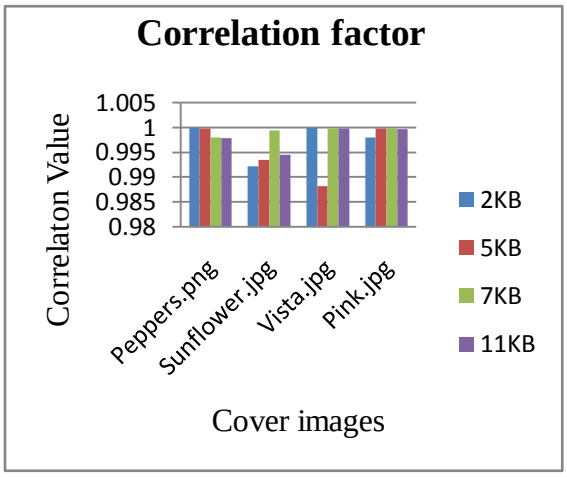


Figure 10: Histogram to Correlation Factor

V CONCLUSIONS

Security is very important for efficient communication. Steganography and cryptography are similar in the way that they both are used for protecting the sensitive information from unauthorized users. Cryptography scrambles the messages so that it becomes difficult to understand. Steganography hides the actual existence of the information so that anyone else other than the dispatcher and the recipient cannot identify the transmission.

In this paper, Cryptography and Steganography security combined to give two tier securities to secret data. Secret data is encrypted before hiding it into the cover image which gives high security to secret data. Content based encryption algorithm using symmetric key of cryptography is used to encrypt secret data and Raster scan technique of Steganography is used to hide encrypted secret data in 2:2:4 ratios into three planes i.e. Red, green and blue respectively of cover image. Experimental results show that when embedded secret data size is small, the value of PSNR is high and value of MSE is low and when embedded secret data size is large, the value of PSNR is low and value of MSE is large. Finally the combined cryptography and steganography has two tier security is effective for secret data communication.

REFERENCES

[1]Amritpal Singh and Harpal Singh, "An Improved LSB Based Image Steganography Technique for RGB Images," IEEE, pp 1-4, (2015).

[2] Ashitosh S. Thorat and G. U. Kharat, "Steganography Based Navigation of Missile", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE), vol.4, pp. 1662-1665, (2015).

[3] D. Nithya, Kalyani and Dr. K.Mahesh, "Safe Information Hiding Using Video Steganography", International Journal of Computer Science and Mobile Computing, vol.4, pp. 502-512, (2015).

[4] Deeksha Bharti and Dr.Archana Kumar, "Enhanced Steganography Algorithm to Improve Security by Using Vigenere Encryption and First Component Alteration Technique," International Journal of Engineering Trends and Technology (IJETT), (2014).

[5] Dr. Diwedi and Dipesh, "Random Image Steganography in Spatial Domain", International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System, pp 1-3, (2013).

[6] M. Ghebleh and A. Kanso, "A Robust Chaotic Algorithm for Digital Image Steganography" Commun Nonlinear Sci Numer Simulat pp 1898–1907, (2014).

[7] Md. Khalid Imam, Rahmani1 Kamiya, Arora and Naina Pal, "A Crypto-Steganography": A Survey (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014, pp.149-155, (2014).

[8]Monika Agarwal, (2013), "Text Steganographic Approaches: A Comparison" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, pp 91-106

[9] Pallavi Das Satish , Chandra Kushwaha and Madhuparna Chakraborty , "Multiple Embedding Secret Key Image Steganography Using LSB Substitution and Arnold Transform," IEEE Sponsored 2nd international conference on electronics and communication system , (2015), .

[10] S. Dhanalakshmi and T. Ravichandran, (2013), "A New Level of Image Processing Technique Using Cryptography and Steganography" International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 3, March 2013 , pp.659-665

[11] Santhoshi Bhattt, Arghya Ray, Avishake Ghoshttt and Ananya Rayttt, "Image Steganography and Visible Watermarking using LSB Extraction Technique", IEEE, (2015).

[12]Shalu Garg and Monika Mathur, "Chaotic Map Based Steganography of Gray Scale Images in Wavelet Domain," International Conference on Signal Processing and Integrated Networks (SPIN), (2014).

[13] Shrutika Suri1, Himani Joshi, Vishakha Mincoha and Akash Tyagi, , "Comparative Analysis of Steganography for Coloured Images,"

International Journal of Computer Sciences and Engineering Open Access , pp.845-849, (2014).

[14]Sourabh Chandraa, Bidisha Mandalb, Sk. safikul and Siddhartha Bhattacharyya, "Content Based Double Encryption Algorithm Using Symmetric Key Cryptography" International Conference on Recent Trends in Computing (ICRTC 2015) , pp.1228-1234, (2015).

[15]Swati Gupta and Deepti Gupta, "Text - Steganography: Review Study & Comparative Analysis" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (5), pp 2060-2062, (2011).

[16]Y.K.Lee and L.H.Chen, "High Capacity Image Steganographic Model" International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (2000).

[17]Yogita Birdi and Harjinder Singh, "Raster Scan Technique for Secure Communication in Steganography" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, pp.5174-5179, (2015).

First Author
Name: JASANPREET KAUR
M.TECH Research Scholar from Giani Zail Singh campus collage of engineering, Bathinda.

Second Author
Name: Sukhjinder Singh
Designation: Assistant professor
Department: Deptt. of Electronics & Communication
Institution: Giani Zail Singh campus collage of engineering, Bathinda, Punjab.