AN EFFICIENT CRYPTOGRAPHIC TECHNIQUE USING RC4 AND PIXEL SHUFFLING ALGORITHMS[1]

***Jyothi B.K, ** Ganavi. M**

**4th Semester, M.Tech. Department of Computer Science and Engineering,*
Jawaharlal Nehru National College of Engineering, Shivamogga, Karnataka, India
***Department of Computer Science & Engineering,*
Jawaharlal Nehru National College of Engineering, Shivamogga, Karnataka, India

Received: 15 February 2019; Accepted: 04 April 2019; Published: 21 April 2019

ABSTRACT

The objective of the present project work is to use a new technique for image steganography in a color cover images,RC4 and pixel shuffling is used for secret message encryption and hides the secret image in the carrier images using HASH LSB. In order to get the true image back at the receiver RC4 and Pixel Shuffling decryption technique has been used. Experimental results have shown that the proposed technique performs better and provides high rate of modification and embedding capacity.

KEYWORDS: *RC4; pixel; shuffling; Hash-LSB; image steganography.*

I INTRODUCTION

Steganography can be termed as an art of writing messages in a hidden format in a way that only intended recipient knows the whereabouts of the message and none other than that. “Steganography” is Greek originated which is understood as “hidden writing”. It is taken as steganos considered as “secret”, “graphic” considered as “writing”. Meaning of the same is taken as text hiding in alternative file which can be image, text etc. “steganography” is considered as similar to “cryptography” and “watermarking”.

The objective of the present project is to use a new technique for steganography in a color cover images, which hides secret message in the images using RC4,Pixel shuffling and Hash LSB substitution. To give more protection the stego image obtained is compressed using Huffman Compression technique. Amount of data to be embedded plays an important role on the compression. The main advantage of using RC4 is that it produces an image with a significantly large file size hence we hide large amount of secrete message. Experimental results have shown that the proposed technique performs better and higher embedding capacity.

II LITERATURE SURVEY

An image steganography algorithm is proposed in [1].cipher algorithm m*n size image by shuffle of RGB pixel values. This works for encryption and decryption

[1] *How to cite the article:* Jyothi B.K., Ganavi M., An Efficient Cryptographic Technique Using RC4 and Pixel Shuffling Algorithms; *International Journal of Research in Science and Technology,* Apr-Jun 2019, Vol 9, Issue 2, 23-29

RGB pixel based images. Image encryption algorithm input image m × n is considered [2] value shuffling of RGB pixels is done. RGB values are transposed of their original positions and swapped inside the boundaries of the image. Hybrid method is proposed in [3] by coalescing the cryptography and Steganography properties. Data hiding is An image steganography algorithm is proposed in [1].cipher algorithm m*n size image by shuffle of RGB pixel values. This works for encryption and decryption RGB pixel based images. Image encryption algorithm input image m × n is considered [2] value shuffling of RGB pixels is done. RGB values are transposed of their original positions and swapped inside the boundaries done using LSB method. It works on spatial domain. A new method is introduced in [4].H-LSB with Affine cipher algorithm is used. It allows keys selection to scramble the clandestine message before image implanting and receiver uses the keys for message decryption.

Steganography algorithm for secret message is introduced in [5].It uses binary codes inside the image. Various data sizes are stored inside the images. RSA and LSB insertion method is implemented in [6]. The message written or file browsed from system is given as input to RSA algorithm, RSA produces public and private key. This binary coded data and cover image is given as an input to HASH LSB method. Video steganography is proposed in [7],a particular portion of container file which can be a video files for secret message embedding is used here. Video frame is divided into number of frames and secret data will be embedded here. New video steganography that hides mystery information is proposed in [8].The information here is covered in the LSB of the cover frame. Hash function is used to select the position of insertion in LSB bits. Image steganography that hides color secret image into a color cover image is introduced in [9]. 2-3-3 LSB method is used for image hiding. This takes eight bits of secret data at a time and put them in LSB of original image in 2,3,3 order. Gray level modification for true color images using image replacement is introduced in [10], input image here is replaced before data hiding. Mixed technique to change the block size in place of fixed blocks is proposed in [11].This works on spatial domain. Here a new algorithm is designed for text security. Better security is provided as blocks of the image is considered. In [12] combination of cryptography and steganography is used to provide security. The data is changed into unreadable form that cannot be read by normal user whereas steganography hides the message by hiding the data into some other digital media. This combination makes it difficult for intruders to steal the sensitive information.

III PROBLEM STATEMENT

Securely communicating information using transmission of images is becoming an important thought as the network growth is very fast. Image security is considered a hot research area in the field of information security. Image encryption must be intended to improve the transmission effectiveness and increase protection from attacks due to unauthorized access. This approach is proposed which can achieve highest level of security. This work provides information security improvement through efficient image cryptography algorithm.

IV PROPOSED SYSTEM

The objective of the present project is to use a new technique for steganography in a color cover images, which hides secret message in the carrier images using RC4,Pixel Shuffling and Hash Lsb method. The Fig.1. shows the system architecture.

1. RC4

RC4 is simple and speedy algorithm. 16 byte keys are used for encryption which are strong, however short key lengths are used to export restrictions. Biased outputs were produced at later stages for certain sequences, mainly in first few bytes of the key streams. This gave rise to future RC4 version known as RC4-drop[n].In this algorithm, the key stream first *n* bytes are dropped to get rid of biased output. RC4 are implemented in Microsoft Excel clients.

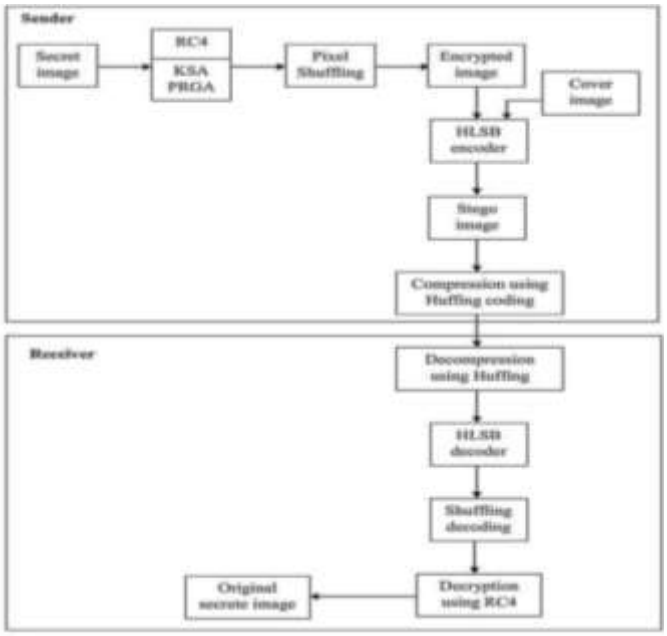

Fig.1 System Architecture

a. Encryption using RC4

Consists of 2 parts Key Scheduling Algorithm and Pseudo Random Generation Algorithm .The steps are given as follows

1. Consider sorted array of 256 elements.
2. After KSA the array looks randomly arranged.
3. After KSA, the PRGA starts.
4. Each PRGA takes 1 byte.

b. Key-scheduling algorithm (KSA)

This is defined to be in the range of 1 ≤ key length ≤ 256.Firstly, array "S" is initialized .S is processed for 256 iterations and mixing of bytes is done. Key stream is generated. It has 2 portions

1. Permutation of 256 bytes.
2. Two 8-bit -pointers.

The permutation is done using variable length key using key-scheduling algorithm (KSA). Once the process is completed, the bits stream is generated using pseudo-random generation algorithm.

c. Pseudo-random generation algorithm

The RC4 is shown in Fig .2. The output is obtained byS1[i] and S1[j], PRGA is modified by key stream for many iterations.

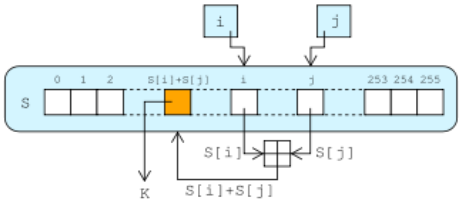

Fig.2.Lookup Stage of RC4

In each iteration, I is incremented, looking up the ith element of S1, S1 [i], and add it that to j, swapS1 [i] and S1 [j], bitwise XOR with the next byte of the message. Every element of S1 is exchanged with alternative element at least once for every 256 repetitions.

2. Pixel Shuffling

Image steganography permits two parties to transmit information confidentially. The span of the pictures increments high with a specific end goal. It is thought to be the pictures of bigger piece profundity. Methodology must be utilized to decrease the extent of the pictures so as to display a picture in less time. In this way, here comes the pressure which goes about as vital marvels in choosing which steganographic method to utilize.

3. Hash-LSB Techniques

Picture steganography taking advantage of eye of human is a limitation. It uses RGB picture as the cover

picture for embedding mystery picture. The significant property of a steganographic framework is to be less distortive while growing the degree of the mystery picture. This framework is proposed to conceal a grayscale mystery picture into a RGB cover picture. A 3,3,2 LSB addition strategy is utilized for shading picture steganography. In LSB inclusion method, when the twofold portrayal of the mystery information overwrite in the LSB of each byte in the cover record the measure of progress occurred in cover picture will be irrelevant and not apparent to the eye of human.

The addition of mystery information pixel (8-bit) is in the request (3,3,2)as appeared in fig 1.3.The install position of each pixel(8-bit) of mystery picture in the LSB of (red, green, blue) of cover picture is as spoken to in x, Where x is LSB bit position per pixel x=1 ,2 and 3 bits of red pixels, x=1, 2 and 4 bits of green pixels, x=3 and 4 bits of blue pixels.

P= H% L

Where,

P is the LSB bit placement

H is the position of any hidden picture pixels.

L is number of bits of LSB

HLSB Inserting algorithm

The steps of HSLB are as follows.

1. Encrypted image is considered.
2. Cover color image is selected.
3. 4 LSB bits RGB pixels are considered for cover image
4. Hash function for encryption

Decoding Steps are as follows

1. Stego-image is obtained
2. 4 bits of lsb for every rgb pixels that is got from stego-image.
3. Hash function is implemented.
4. Bits in sequence recovered.
5. Read the secret image.

4. Huffman Coding

Huffman coding is traditional information pressure systems developed by David Huffman. It is ideal prefix code created from set of probabilities and has been utilized as a part of different pressure applications. These codes are of variable code length utilizing fundamental number of bits. This thought causes a lessening in the normal code length and therefore by and large size of packed information is littler than the first.

It is grounded on the two observations .

a) Regularly occurring symbols has shorter code words

b) Least frequent symbols have same length.

Huffman coding is shown in Fig.3.

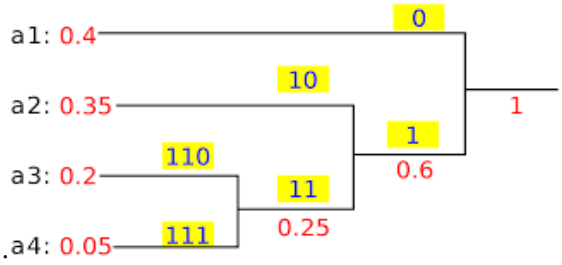

Fig.3.Huffmancode Tree with symbols

V. SIMULATION, RESULTS AND ANALYSIS

The secret image and the cover image are of JPEG format. The Fig.4 and Fig.5 shows cover and secret image.

Color Image Secret Image

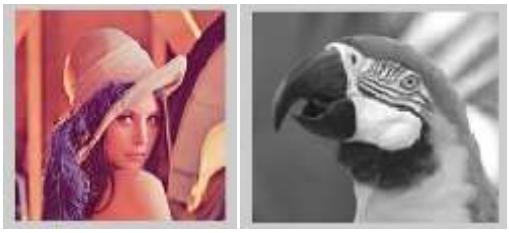

Fig. 4 Input Cover imageFig.5 Input Secret image

The Fig.6 shows the output of the encryption part which displays the color RGB image, secret image, encrypted image and stego image.

Fig.6.Encryption Process

After encryption the stego image is compressed and decompressed for more protection then decryption process is done using DRC4 Algorithms. The

decrypted image, extracted message and retrieved message is displayed in Fig.7,8 and 9.

Fig. 7.Decrypted Image

Fig.8.Extracted Message

Fig. 9. Retrieved message image

The quality of the image recovered in Fig.9 is high which can be proved using various parameters.

The proposed methodology is tested and run successfully on MATLAB software. The proposed work gives the better results compared with other techniques as well. It has high efficiency and better hiding capacity and yields much better results. Performed the experiment and analysed using PSNR and MSE metrics and also time required for algorithm to run.

$$\text{PSNR} = \frac{-10\ log_{10}\ e_{MSE}}{S^2} \qquad (1)$$

$$\text{MSE } 2 = \frac{\sum \text{M2, N2 } [\text{I1 (M2, N2)} - [\text{J1 (M2, N2)}]^2}{M2 * N2} \qquad (2)$$

The table 1 and 2 shows the PSNR and MSE values of the proposed method along with graphical representation in Fig 10 and Fig 11. Which yields better and efficient results as shown. Higher is the peak signal to noise ratio the quality , efficiency of the image is maintained same throughout the encoding and decoding process. Lower the MSE (mean square error) value lower distortion created during the encryption and decryption process. Hence lower MSE and higher PSNR metrices must be maintained to get best results

Table 1 Performance analysis of PSNR

Secret Images	Cover Images						
	1	2	3	4	5	6	7
Animal .jpg	45.16	45.11	45.18	45.17	45.14	44.66	45.08
Butterfly.jpg	45.23	45.20	45.18	45.20	45.26	44.67	45.11
Car.jpg	45.18	45.22	45.15	45.16	45.19	44.65	45.04
Cell.jpg	45.23	45.26	45.19	45.23	45.18	44.69	45.09
Hibiscus.jpg	45.20	45.19	45.21	45.18	45.23	44.68	45.04
Hill.jpg	45.19	45.21	45.18	45.20	45.24	44.65	45.03
Man.jpg	45.18	45.22	45.24	45.13	45.20	44.68	45.07

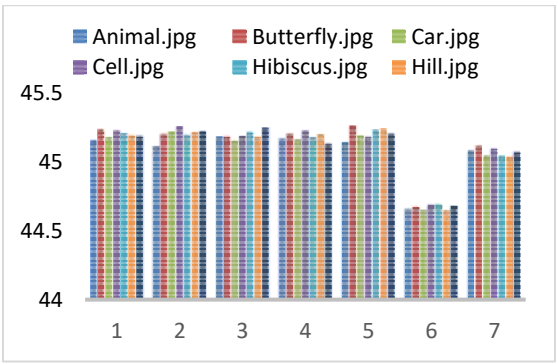

Fig.10.Graphical representation of PSNR

Table 2 Performance analysis of PSNR

Secret Images	Cover Images						
	1	2	3	4	5	6	7
Animal .jpg	1.9807	2.001	1.9695	1.9765	1.9883	2.2236	2.0153
Butterfly.jpg	1.9468	1.9628	1.9708	1.9613	1.9353	2.2168	2.0004
Car.jpg	1.9719	1.9538	1.9837	1.9794	1.9678	2.226	2.0335
Cell.jpg	1.949	1.9363	1.9669	1.9492	1.9708	2.208	2.0099
Hibiscus.jpg	1.9595	1.9641	1.9571	1.9728	1.9491	2.2085	2.0351
Hill.jpg	1.9659	1.9557	1.9709	1.9616	1.9437	2.2265	2.0381
Man .jpg	1.9712	1.9543	1.9424	1.9953	1.9624	2.2129	2.0228

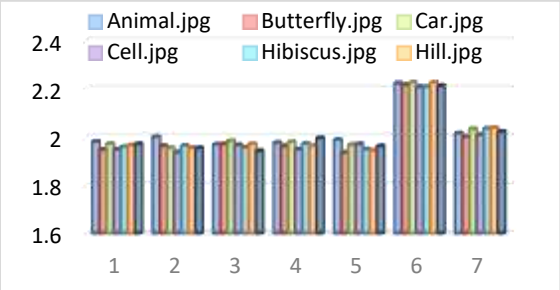

Fig.11.Graphical representation of MSE

The compression ratio, encryption and decryption time is tabulated in table 3,4 and 5.The corresponding graphical representation is shown in fig 12 and 13.

The below table 3 shows the simulation results of lossless image compression scheme. The compression ratio obtained are very satisfactory. The least compression ratio is 1.0076 which means that the compressed image is stored using only 1.0076% of the initial storage size.

Table 3 Compression Ratio Using Huffman Coding

Secret Images	Cover Images						
	1	2	3	4	5	6	7
Animal.jpg	1.0311	1.0248	1.0987	1.0229	1.0077	1.0882	1.0193
Butterfly.jpg	1.0311	1.0248	1.0987	1.023	1.0076	1.0883	1.0194
Car.jpg	1.031	1.0248	1.0987	1.0229	1.0077	1.0883	1.0193
Cell.jpg	1.0311	1.0248	1.0986	1.023	1.0077	1.0883	1.0194
Hibiscus.jpg	1.0311	1.0247	1.0986	1.023	1.0077	1.0882	1.0194
Hill.jpg	1.0311	1.0248	1.0987	1.0229	1.0077	1.0883	1.0193
Man.jpg	1.0311	1.0248	1.0987	1.0229	1.0077	1.0883	1.0194

The below table 4 and 5 shows the encryption time and decryption time consumed for encryption and decryption of the secret image .It can be observed that the encryption time is lesser than the decryption time.

Table 4 Encryption time

Secret Images	Cover Images						
	1	2	3	4	5	6	7
Animal.jpg	0.20	0.18	0.49	0.20	0.19	0.19	0.18
Butterfly.jpg	0.20	0.20	0.19	0.18	0.20	0.20	0.21
Car.jpg	0.22	0.18	0.19	0.46	0.21	0.18	0.19
Cell.jpg	0.20	0.46	0.20	0.20	0.87	0.20	0.16
Hibiscus.jpg	0.11	0.20	0.18	0.10	0.18	0.19	0.19815
Hill.jpg	0.19	0.24	0.20	0.20	0.22	0.18	0.18131
Man.jpg	0.19	0.18	0.16	0.20	0.19	0.20	0.17667

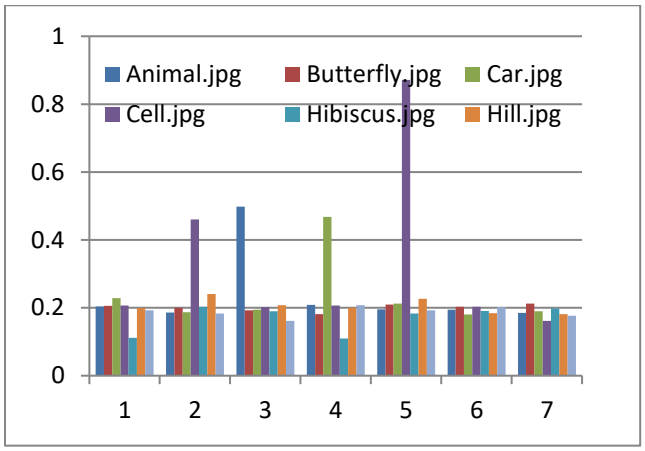

Fig.12.Graphical representation of Encryption time

Table 5.Decryption Time

Secret Images	Cover Images						
	1	2	3	4	5	6	7
Animal.jpg	0.95	1.02	1.03	0.83	1.07	1.05	0.74
Butterfly.jpg	1.05	1.05	0.76	0.58	0.82	0.75	1.08
Car.jpg	0.98	0.95	0.97	0.97	1.06	0.89	1.06
Cell.jpg	0.90	0.86	0.93	0.98	1.09	1.08	0.81
Hibiscus.jpg	0.96	0.90	0.98	1.0	0.67	0.60	0.94
Hill.jpg	1.04	0.79	0.87	0.8	1.0	0.80	1.03
Man.jpg	1.05	0.90	1.11	0.80	0.91	0.87	0.80

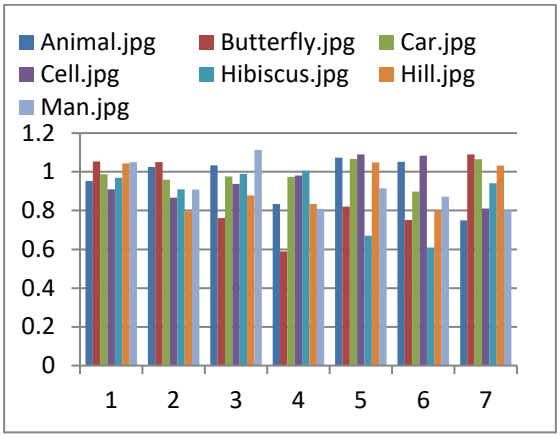

Fig.13.Graphical representation of Decryption time

VI CONCLUSION AND FUTURE SCOPE

In the proposed algorithms the images to be evaluated are concealed. According to the analysis it is found that system provides high security and easy encryption, embedding and decryption, quality of images are not affected as it appears in measurements of (MSE,PSNR and Compression ratio).MSE is the mean square error, in decibels, between two images. These ratios are used as a measurement of quality between two images. High PSNR value and low MSE value determines better quality of image. The highest PSNR achieved is 45.2632 and lowest MSE is 1.9353.The Compression Ratio achieved is 1.0076. These values indicate that RC4 with HLSB works perfectly with minimal distortion for image quality. Hence this system is very effectual to hide grayscale image inside color images.

The future work can be extended for other data files like audio, video and also for other image formats and images of other size. Some attacks analysis can also be applied for the proposed method.

Financial Support and Sponsorship: Nil

Conflict of interest: None

REFERENCES

1. Kester. Q, (January 2013), A cryptographic Image Encryption technique based on the RGB PIXEL shuffling A cryptographic Image Encryption technique based on the RGB PIXEL shuffling; *International Journal of Advanced Research in Computer Engineering & Technology*, vol. 2,no.2 pp.848-854.
2. N. Agarwal and Agarwal. P, (August 2013); An Efficient Shuffling Technique on RGB Pixels for Image Encryption; *MIT International Journal of Computer Science & Information Technology*, vol. 3, no. 2, pp. 77–81.
3. Saptarini, Y. Sir, (December 2013), Digital Color Image Encryption Using RC4 Stream Cipher and Chaotic Logistic Map, *Information Systems International Conference*, pp. 2–4.
4. Abdullah, (June 2016), New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm, *International Journal of Computer Applications*, vol. 143, no. 4, pp. 11–17.
5. Rosziati and Kuan. (2011), Steganography Algorithm to Hide Secret Message inside an Image. Computer *Technology and Application*, Vol. 2: 102-108.
6. Sahute.P, S. Waghamare, Patil, (March 2015), Secure Messaging Using Image Stegnography, *International Journal of Modern Trends in Engineering and Research*,vol.2,no.3, pp. 598–608.
7. K. Hamdnaalla, A. Wahaballa, and O. Wahballa, (August 2013), Digital Image Confidentiality Depends upon Arnold Transformation and RC4 Algorithms, *International Journal of Video & Image Processing and Network Security*, vol.13, no. 04.
8. Koushik, (April 2012), Hash Based Least Significant bit technique for video steganography, *Int. Journal of Security Privacy and Trust Management*, Vol 1, No 2.
9. Manjula and Ajit, (February 2015), Hash Based Least Significant bit (2-3-3) Image steganography in spatial domain, *Int. Journal of security and Trust Management* vol 4, No1.
10. Khan Jamil Sajjad, (June 2015), Secure image steganography using cryptography and image transposition. *University Journal of Research*.
11. Shivani, Jyotsna, Kumar and Amit, (2017), Multiple layer Text Security using variable

block size cryptography and Image steganography, *Computational Intelligence and Communication Technology*, IEEE 2017.

12. Aishwarya and Hema, (March-April 2017), Strength of steganography and cryptography, *Int. Journal of Advanced Research in Computer Science*, Vol 8, No. 3.