International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 04 Issue: 07 | July -2017 www.irjet.net p-ISSN: 2395-0072

A New Algorithm for Digital Colour Image Encryption and Decryption

Sayan Rakshit[1]

1 M.Tech Student, Department of Mathematics, Indian Institute of Technology Kharagpur, Kharagpur, India

---

Abstract— *Modern era is thriving too fast because of the blessings of digital technology. Due to digital technology, application of multimedia objects, such as digital image and digital communication has gained lots of attention. It is very important to protect our image data from an unauthorized access. In this paper, a new efficient colour image encryption and decryption technique has been proposed. The proposed encryption technique is based on image pixel shuffling and Logistic map. The pixel shuffling is done by two steps, divide the image into some smaller equal blocks and give a rotation of 90 degree to each and every block and then apply the pre generated shuffling pattern to this block scrambled image. To give more strength of the encryption technique, nature of Logistic Map has been used. With the initial pair of values of Logistic Map, creates a scrambled image and XOR it with the actual pixel shuffled image. Steganography technique is also being used to send the dimension of the original image. The shuffling pattern and initial pair of values have to keep secrete, these are consider as symmetric key. Decryption technique is the reverse process of encryption technique.*

Key Words: RGB Colour Image, Cryptography, Encryption, Decryption, Logistic map, Steganography.

1.INTRODUCTION

Day by day the more and more people are getting involved with digital technology. The more people will come the more security issue will arise. The solution of the security issue is cryptography. Cryptography is a technique which is being used to hide and protect information from unauthorised access. Use of cryptography is not new, about 2000bc it was first introduced but the rapid use of it can be seen in this digital era. Nowadays the traditional cryptosystems are very much successful to protect our text message but when it comes to protect image data it fails in some extent in terms of speed. It is because an image data contains much more information than a text.

A digital image is made of some pixels. In an image neighbouring pixels are very much correlated. So displacements of neighbouring pixels make an image unrecognisable. This phenomenon of digital image can be used to encryption and decryption process.

In this paper symmetric key cryptosystem has been used to encrypt an image. Random permutation of a string of consecutive natural numbers and Logistic Map has used to generate required symmetric keys.

The main aim of this research is to scramble the pixels and then change the certain amount of values of the pixels to achieve a strong encrypted image. With the same key the decryption process has to be done without loss of any image quality.

2. PRELIMINARY

2.1 *Steganography*

Steganography is a process by which some secret information can be concealed into a carrier file. The main difference between cryptography and steganography is that, cryptography sends the encrypted message, which may protect to unauthorised access but it is unable to prevent the fact that, something has been sent is known to everyone. Here steganography wins the race.

There are some techniques available at present, among them Least Significant Bit technique is one of the simplest techniques.

Least Significant Bit Steganography: For this technique we need one carrier file and the secret information. Carrier file can be any type of digital signal, such as digital image. As least significant bit of a pixel value contains very small amount information, so changing of the least significant bit cannot change significant amount of image. In this technique first the secret information has to convert into 8-bit binary string and then replace each bit into the least significant bit of each pixel value. Now the image becomes a stegno-image. To extract the information from the stegno-image, it is needed to collect the least significant bit of each pixel value and convert them to the readable information.

2.2 *Logistic map*

Logistic map is a chaotic map and the formula is $Xn+1 = Xn * r *(1 + Xn)$ where $r \in [0; 4]$ and $Xn \in [0; 1]$. Here r is called logistic parameter. When $r \in [3:569946; 4]$, logistic map works in a chaotic state, and produces non-periodic sequence.

Initially it is necessary to give iteration number, initial value of $X0$ and the value of r.

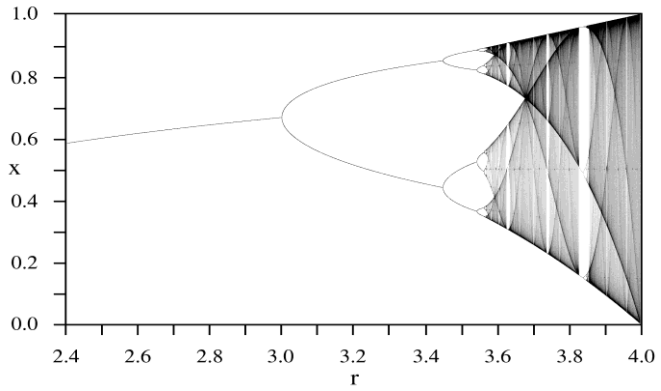

Fig-1 the above picture shows the bifurcation diagram of the Logistic Map.

3. PROPOSED ALGORITHM

The proposed algorithm consists of three parts, key generation, encryption and decryption. As the algorithm uses symmetric key, so need to generate key first before start to encryption process.

3.1 *Key Generation*

The proposed algorithm needs two key, (i) Generate shuffling pattern (ii) Chaotic image using Logistic Map

i. **Generate shuffling pattern:** Take a one-dimensional array of numbers from 1 to p (p=m*n, where p, m, n all are positive integer) and do a random permutation. Resize the one-dimensional array into a two-dimensional array of size m*n, where m and n are number of rows and columns respectively. Keep this two-dimensional array in secret.

ii. **Generate Chaotic image:** To generate a chaotic image, need to generate three RGB channel separately. First for Red channel take initial value of *r* and *x0* of Logistic Map and generate p (same p=m*n as shuffling pattern) points(x) and multiply each point(x) with 1000. Calculate q = (x*1000) mod 255 and take the integer part of q and store them in a one-dimensional array. Resize this one-dimensional array with the same two dimension of shuffling pattern. Like this way with different initial values of *r* and *x0* have to prepare another two channel, green and blue. Let's suppose for Red, Green and Blue the initial pair of values are *(r1, x0), (r2, y0)* and *(r3, z0)* respectively. These pairs have to keep secret. Combine the three different channels and get the chaotic RGB image.

3.2 *Encryption Process*

Encryption process includes smaller blocks scrambling, stegnotography, pixels scrambling and pixel value changing.

1. Take a colour image and divide this image with four equal blocks and rotate each of the block 90 degree anti-clock wise. Again take each of the block separately and divide each of the blocks into four sub equal blocks and rotate each of the sub-block 90 degree anti-clock wise. Again take each of the sub-block and do the same as before blocks. At the end there are 64 smaller blocks.

2. Write the dimension of the colour image, start with "(" and close with ")" into the block scrambled image from step 1 using Least significant bit steganotography technique. The ")" here indicates the end of the message.

3. If the size of the colour image is less than the size of the secret scrambling pattern, then pad rest of the rows and columns with the random values from 0 to 255 and get a padded image of same size of scrambling pattern.

4. At this stage scramble the position of each pixel according to scrambling pattern and get a fully scrambled image.

5. XOR the scrambled image with the chaotic image and finally encrypted image is ready.

3.3 *Decryption Process*

Decryption process is reverse process of encryption.

1. Take the encrypted image and XOR with the chaotic image.

2. Use secret scrambling pattern to descramble the scrambled image and get the block scrambled padded image.

3. Extract the dimension of the actual image by the extracting method of Least significant bit steganotography technique.

4. Crop the block scrambled image according to the dimension from the padded image.

5. Take a colour image and divide this image with four equal blocks and rotate each of the block 90 degree, clock wise. Again take each of the block separately and divide each of the blocks into four sub equal blocks and rotate each of the sub-block 90 degree, clock wise. Again take each of the sub-block and do the same as before blocks. Re-combine all the 64 sub-blocks and get the original decrypted image.

3. EXPERIMENTAL RESULT

- *Encryption*

1. Take a 225*225 Lena image and apply step 1

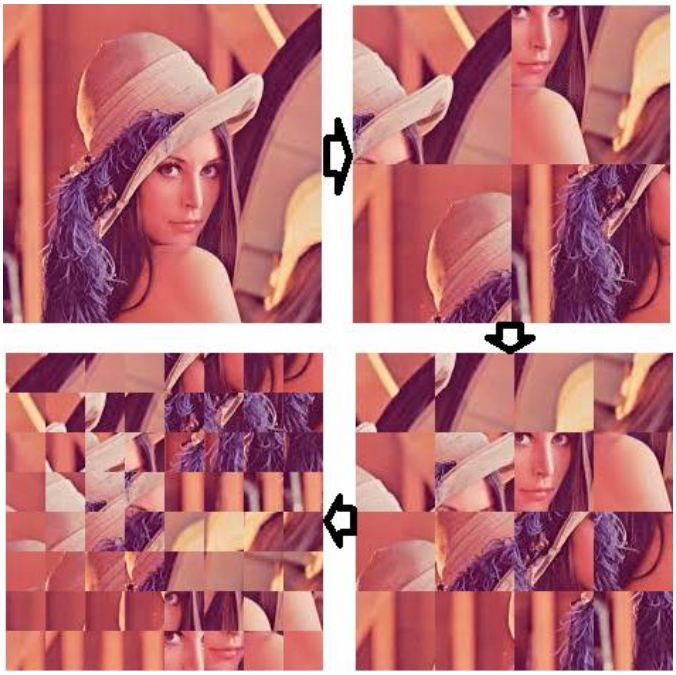

Fig-2,

Lena Image > 1st Rotation >2nd Rotation >3rd Rotation

2. Write "(ROW225COL225)" into the block scrambled image using steganography.

3. Apply step 3 on the stegno image.

Fig-3, Padded Image

4. Scramble the pixels position as step 4.

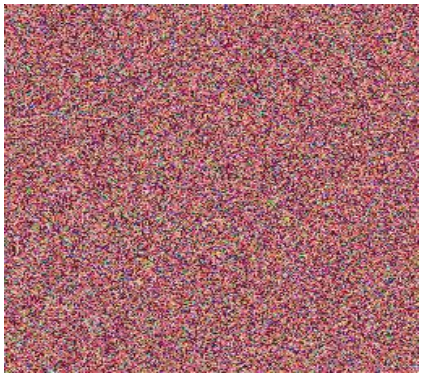

Fig-3, Pixel Scramble Image

5. By the initial pairs (3.63,0.5), (3.73, 0.57) and (3.78,0.67) of Logistic Map for generating Red, Green and Blue channel respectively, make a chaotic image and XOR it with the pixel scramble image and get the final encrypted image.

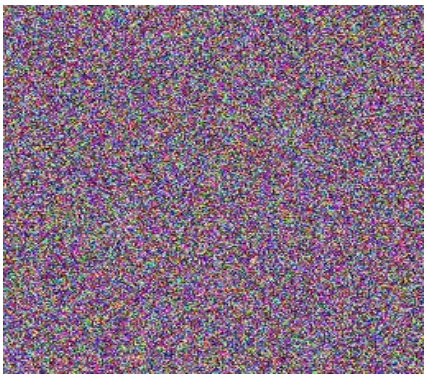

Fig-4, Encrypted Image

3. ANALYSIS OF EXPERIMENTAL RESULT

For this experiment the Matlab 11 has been used. The proposed algorithm has implemented on some 24-bit colour images. One such image is 225*225 Lena image which can be shown in Fig-2. Here size of the secret scrambling pattern matrix is 256*256. So need to pad the Lena image to make it as the same size of scrambling pattern matrix, can be shown in Fig-3. Then the Fig-4 and Fig-6 show the pixel scrambling image and encrypted image respectively. The histogram of the three different channels (Red, Green, Blue) of original Lena image and the final encrypted image (Fig-5) are shown below.

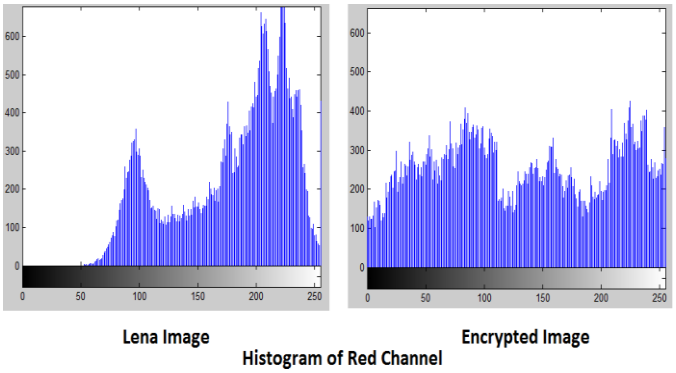

Fig-6

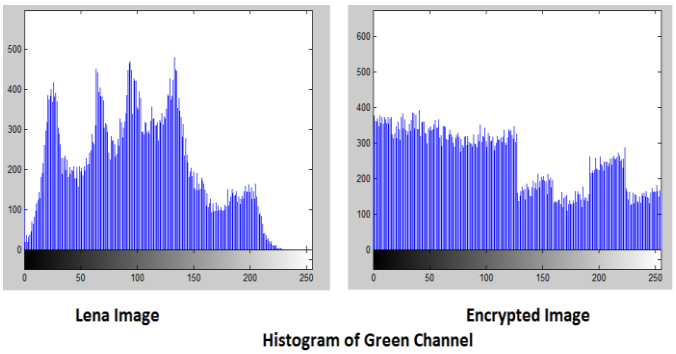

Fig-7

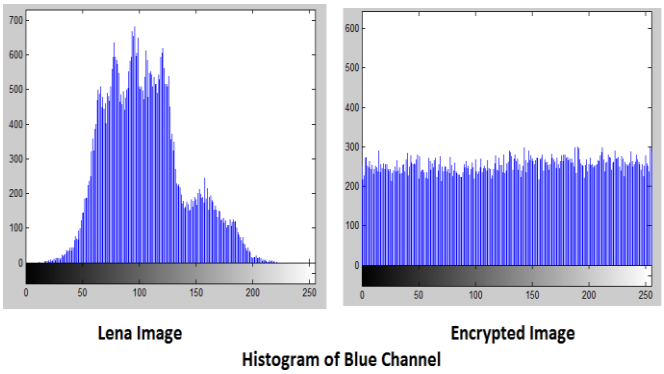

Fig-8

From the above Fig-6, Fig-7 and Fig-8, it is clear that the colour distribution of encrypted image is very much different of the original Lena image. It is because most of the pixel values of Lena image have changed during the XOR operation with the chaotic image. The histogram of encrypted image shows uniform distribution of colours which will resist any statistical analysis.

3. CONCLUSIONS

The proposed algorithm gives us an effective way to encrypt and decrypt a colour image. Any size of an image which is less than the size of the key scrambling pattern can be sent with the same key. We no need to change our secret key every time for different sized image. The proposed algorithm shuffles the pixels position and then changes the pixel values, which strengthen the encryption quite well.

ACKNOWLEDGEMENT

I am grateful to everyone who has supported me, directly or indirectly.

REFERENCES

[1] Asia Mahdi Naser Alzubaidi, Color Image Encryption and Decryption using Pixel Shuffling with Henon Chaotic System, IJERT, Vol. 3, Issue 3, March – 2014.

[2] Panduranga H.T, Naveen Kumar S.K, Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images, IJCSE, Vol. 02, No. 02, 2010, 297-300.

[3] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar, Image Encryption Using Affine Transform and XOR Operation, International Conference on Signal Processing, Communication, Computing and Networking Technologies(ICSCCN 2011), 2011.

[4] C.Wei-bin, Z. Xin, Image encryption algorithm based on Henon chaotic system , Image Analysis and Signal Processing IEEE xplore,pages 94 - 97,11-12 April 2009.

[5] Hossam Eldin H. Ahmed, Ayman H. Abd El-aziem, Image Encryption Using Development of Chaotic
Logistic Map Based on Feedback Stream Cipher, Recent Advances In Telecommunications, Informatics And Educational Technologies.

[6] S.S.Maniccam, N.G. Bourbakis, Lossless image compression and encryption using SCAN, Pattern Recognition 34(2001),1229-1245.

[7] G.A.Sathishkumar, Dr.K.Bhoopathy bagan, Dr.N. Sriraam, IJNSA, Vol.3, No.2, March 2011.

[8] J. Cheng, J.1. Guo, A new chaotic key-based design for image encryption and decryption, The 2000 IEEE International Symposium on Circuits and Systems, vol4, no. 4, pp. 49 - 52, May. 2000.

[9] Chen GR, Mao YB, A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps, Chaos, Solitons & Fractals 2004, vol 21, pp 749–61, 2004.

[10] Apeksha Waghmare, Abhishek Bhagat, Abhishek Surve, Sanuj Kalgutkar, Chaos Based Image Encryption and Decryption, IJARCCE , Vol. 5, Issue 4, April 2016 .