ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

An Efficient Image Encryption Technique Using RGB Pixel Displacement and Simple Chaotic Map

Chhavi Garg[1], Lalit Mohan Gupta[2], Eshank Jain[3]

M. Tech. Scholar, Dept. of CSE, ITM, Aligarh, India[1]

Asst. Professor, Dept. of CSE, VCTM, Aligarh, India[2]

Asst. Professor, Dept. of CSE, ITM, Aligarh, India[3]

ABSTRACT: Transmission over the Internet for multimedia content has become increasingly frequent. However, digital image security poses a severe threat to the transmission method owing to network openness and sharing. Among different techniques of security, various methods of image encryption have been introduced in the recent past by the researchers. In this paper, we enhanced the security of the image by applying Ex-OR operation on RGB components of the original image with RGB components of the key image. Then, the resultant image goes through chaotic 1D logistic map procedure. 1D logistic map procedure scramble the pixels of the image in very randomness fashion that is very difficult to know the exact position of the pixels for the intruders. Therefore, our technique achieved very high level of security of the image during the communication.

KEYWORDS: 1D logistic, RGB, encryption, decryption

I. INTRODUCTION

Digital image encryption has become an important research area due to the increasing demand for information security and it has broad application prospects. Digital image characteristics require research into new digital image encryption methods.Some information can be easily transmitted and distributed via communication channel over several parties in the digital age. Some parties need to use the transmission channel to transfer some secret information.Chaos-based methods have been used for image encryption in recent days.The main benefits of the chaotic encryption approach include: high flexibility in the design of the encryption system, good privacy. Chaotic sequences produced by chaotic maps are pseudo-random sequences; very complex and difficult to analyze and predict are their structures. In other words, chaotic systems can make encryption systems more secure. The methodology for digital image processing is classified into two categories: replacement of pixel value and scrambling of pixel location. The first one focuses on changing the pixel value so that others are unable to read in the digital image the original pixel information. The other focuses on changing the position of the pixels for encryption purposes. However, it is possible to easily decrypt both of these methods by some means. Chaotic maps are used to encrypt images that include features such as non-deterministic, random, periodicity, etc. 1D logistic map is the common one in 1D chaotic maps. It was discovered by R. M. May in 1976. It displays chaotic properties that are derived from discrete non-dynamic systems and generates a sequence of randomness. This paper presents a new image encryption technique using a simple approach to chaotic numbers. The dynamic response of the chaotic system is sensitive to the initial values and parameters of the chaotic system, and a large number of researchers use chaotic sequences to encrypt images for communication security purposes.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

II. LITERATURE REVIEW

[1] Manjunath Prasad and K.L.Sudha, shows in their paper that They proposed a new algorithm in the paper that uses the single map. To find the best map for this algorithm, they used Henon map and Lorentz map for pixel shuffling and measured coefficient of correlation and key sensitivity. With the use of a single map, the key space will become less suitable for applications such as wireless communication. At the same time, it gives better confidentiality and a key that is difficult for an unintended user to decipher.

[2] ShrijaSomaraj and Mohammed Ali Hussain, shows in their paper that A new method to encrypt color images or 3D images is proposed in this paper using the concept of rgb displacement and scrambling. The proposed algorithm uses an original color image to be encrypted and the key image of the same size (256x256) is used as another color image. Key process of generation involves dividing the key image into three components, i.e. the components of RGB. One bitplane is selected from each of the three components. This is the key. Also, the original image is divided into three components, which are XORed with the key image's selected bitplanes. This gives the intermediate cipher image that is subjected to further scrambling by RGB and gives the required Cipher Image. The image decryption process is exactly the reverse of the encryption process.

[3]M.Y. Mohamed Parvees, J. Abdul Samath, I. Kaspar Raj and B. Parameswaran Bose, shows in their paper that A new color byte scrambling scheme is proposed in this paper for color image encryption using Logistic and Ikeda map. The chaotic sequences are generated using these chaotic maps and, according to the transformation of chaotic sequences, the position of image pixels and values is changed. The encryption of the chaotic image is done through confusion and diffusion. The confusion is obtained by changing the locations of pixels and the diffusion is obtained by changing the values of pixels. The logistic map is one-dimensional in this scheme that is simple and efficient and used to generate sequences of permutation to create confusion. To achieve diffusion, the two-dimensional Ikeda map is used to generate masking sequences. Finally, the result of the proposed algorithm is compared and validated by different cryptanalysis with existing results.

[4] Kunal Kumar Kabi, Chittaranjan Pradhan, Bidyut Jyoti Saha and Ajay Kumar Bisoi, shows in their paper that They used various versions of 2D chaotic maps in the paper to encrypt the image. Since 2D chaotic maps have more control parameters than the 1D chaotic map, they are more secure. With regard to the nature of security, thry has calculated the values of NPCR and UACI. The results of the experiment show that encryption of 2D chaotic maps is effective and secure.

[5] HeriPrasetyo, shows in his paper that This paper proposes a new technique for image encryption using a simple chaotic number. This approach offers promising results on encrypted image and in terms of objective measurement, it outperforms the old existing image encryption schemes. It validates the usability on the image encryption task of a simple chaotic number.

[6] C. K. Huang, Y. H. Hsu, W. Y. Chen, S. K. Changchien, C. M. Hung, C. H. Liu and Y. R. Tian, , shows in their paper that This paper proposes a novel color image encryption technique, the application of which can achieve highly confidential security in the encryption of color image; the encryption scheme. First, the proposed PCS method generates chaotic sequences from the variable elements of four different chaotic systems, and these sequences ' shuffled pixels can disorder the outlines of the original image completely. In addition, the IME method using various chaotic code sets the color levels of PCS matrices to be ciphered, and the ciphered color levels may confuse the image's histogram.

[7] Zhang Jun, Li Jinping and Wang Luqian, shows in their paper that This paper designs a compound Chaos encryption algorithm for digital images. To generate sequences of Chaos, Lorenz Chaotic system and logistics map are linked in cascade. Then the matrix of permutation is built to encrypt the digital image. The new algorithm can expand

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

key space and improve the ability to be anti-aggressive. Matlab7.0 is used to test the image encryption simulation. Experimental results show that the algorithm is feasible and can meet the image transmission and storage security requirements. The Chaos algorithm compound can also be used to encrypt digital images in color.

III. PROPOSED METHOD

The proposed algorithm uses two color images of the same dimension (256x256) first image is the image to be encrypted and the other image will act as a key. Key generation process involves dividing the key image into three components, i.e. RGB Component. In order to alter pixel, the original image is also divided into RGB components and then the pixels of both images are XORed.

In this paper, we also used 1D Logistic maps whose definitions areas follows. 1DLogistic map is described as Eq.

$$X_n+1 = \mu X_n(1-x_n)$$

Where $\mu \in [0,4]$, $X_n \in (0,1)$, n = 0, 1, 2, ... the research result shows that the system is in a chaotic state under the conditionthat$3.56994 < \mu \leq 4$.

Encryption process:

Step1: Here, care should be taken to see that the elements generated are unique; no repetition should occur. Now divide the elements generated into three blocks equal to M x N each.

0.91999	0.27085	0.72678	0.73074	0.72407	0.73523	0.71636	0.74771	0.69417
0.78124	0.62891	0.85884	0.44613	0.90932	0.30343	0.77781	0.63596	0.85196
0.46411	0.91526	0.28541	0.75054	0.68900	0.78854	0.61361	0.87249	0.40938

Table.1 Elements generated from chaotic map

Step2: Now sort each block's elements in ascending or descending order and compare the flaw between each block's original and sorted elements and tabulate the change in the index. According to three blocks, we have three series of index changes.

0.91999	0.27085	0.72678	0.73074	0.72407	0.73523	0.71636	0.74771	0.69417
0.78124	0.62891	0.85884	0.44613	0.90932	0.30343	0.77781	0.63596	0.85196
0.46411	0.91526	0.28541	0.75054	0.68900	0.78854	0.61361	0.87249	0.40938

Table.2 Divided into three separate arrays each of 9 elements

Step3: Now, look at the previous table's first array. Index the elements as indicated in Fig1. Arrange the elements in decreasing order and the displacement tabulation is noted in the index by comparing the elements as in fig2 before and after sorting. For all three colours, this procedure is repeated. Now we change the intensity position to get encrypted image according to the index obtained.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

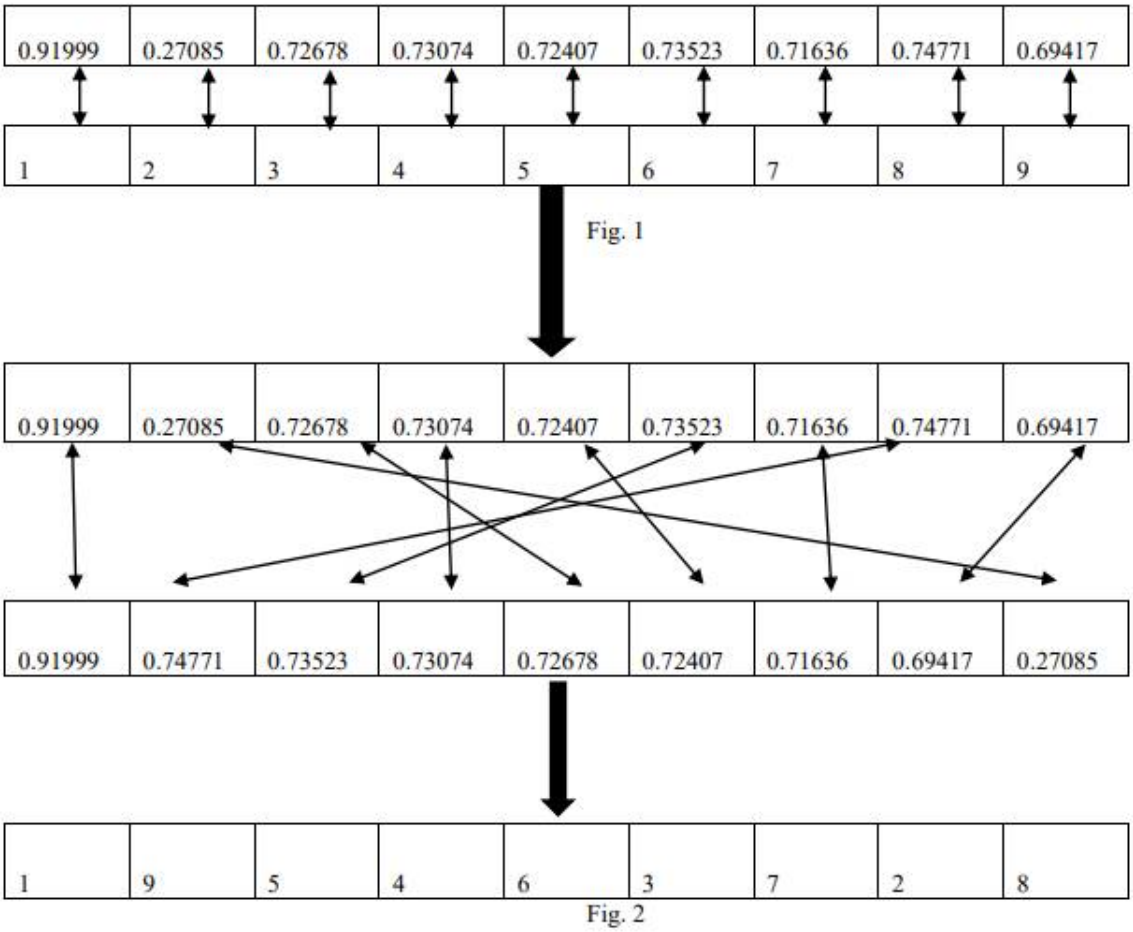


Fig. (1) and Fig. (2) The arrangement of elements in decreasing order and the index displacement tabulation

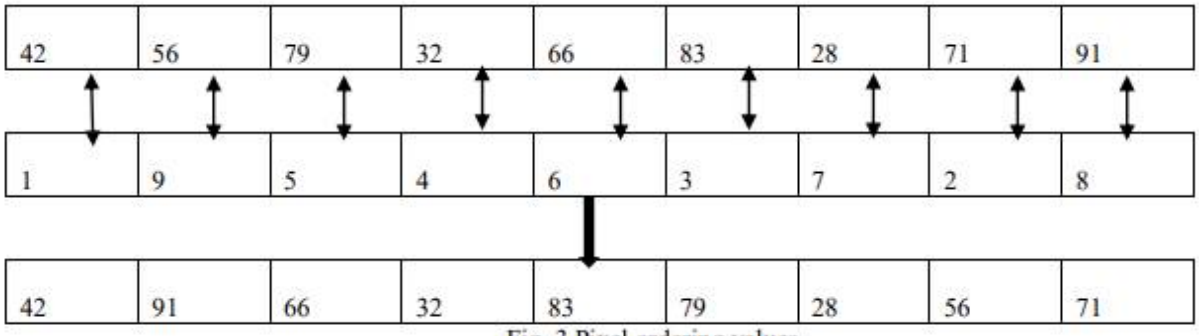


Fig. 3 Pixel ordering values

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

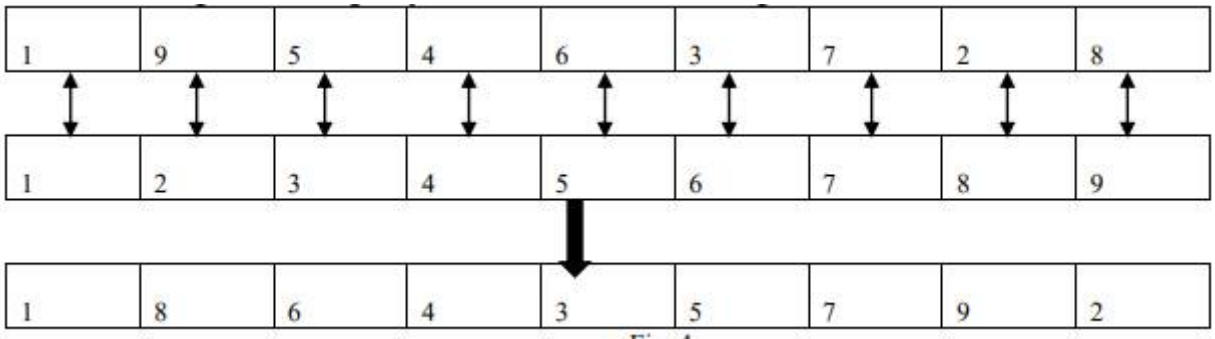


Fig. 4

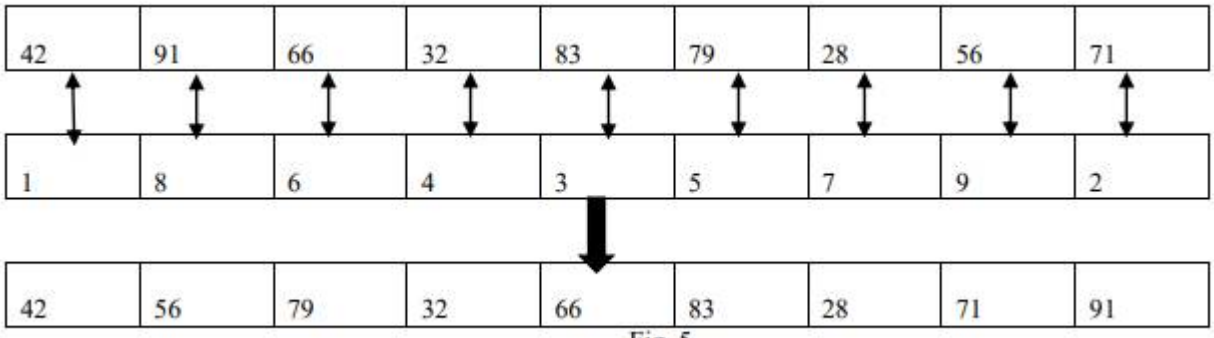


Fig. 5

Decryption process

The reverse process followed for encryption is used for decryption.

Step 1: The sequence of received elements is represented in fig 4 row 1; row 2 represents sorted index elements obtained from the encryption process and row 3 represents resorted index elements.

Step 2: The same random sequence is generated at the receiving point with a chaotic map to retrieve the sorted index elements as in fig 4 and the original pixel values are retrieved as in fig 5.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

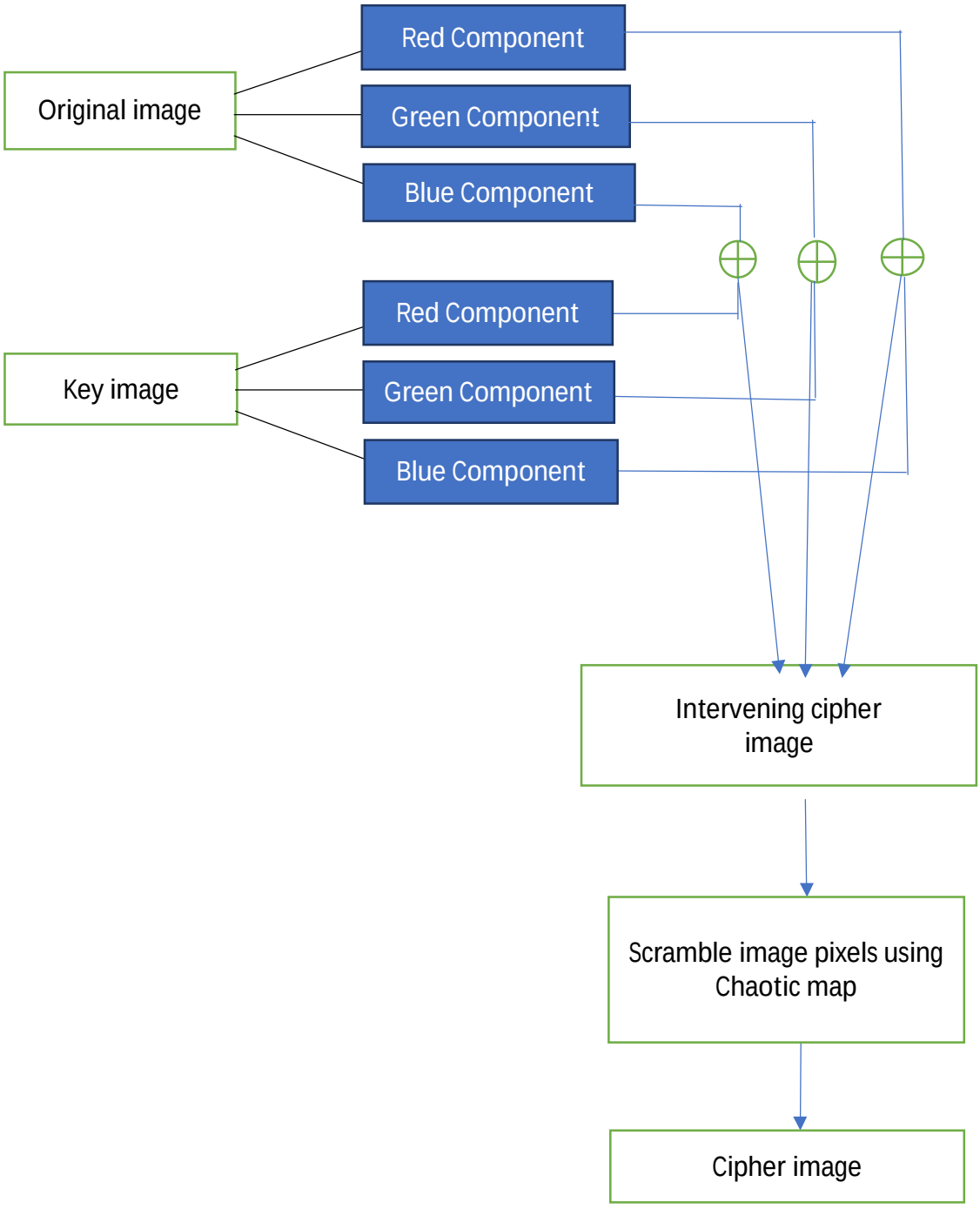


Fig.6 Method of Encryption using RGB Displacement

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

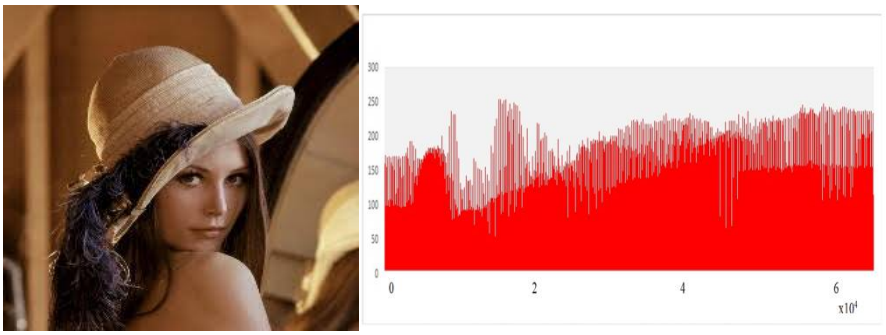
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

IV. RESULT AND DISCUSSION

In order to test the proposed pixel scrambling algorithm, two colour images are taken.



Lena image

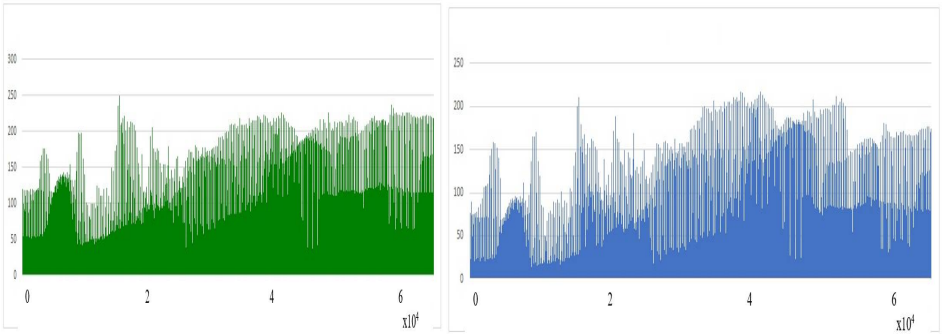
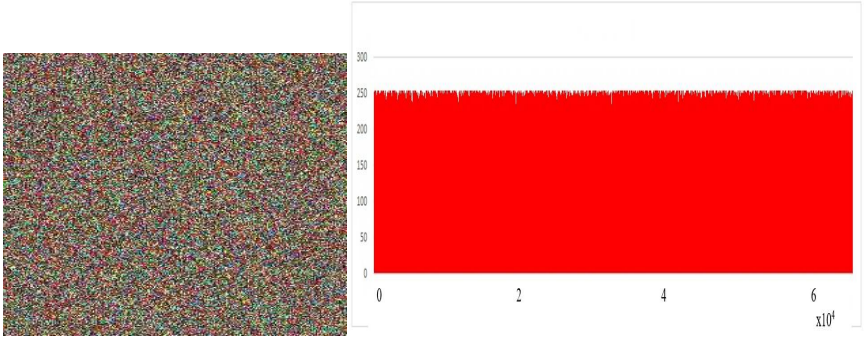


Fig 6(a)Image and RGB intensity levels

As seen from the figures, in the encrypted image and its RGB plot the intensity value of the original Lena image is distributed or scrambled. This allocation is due to the randomness from the Chaotic map components.



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

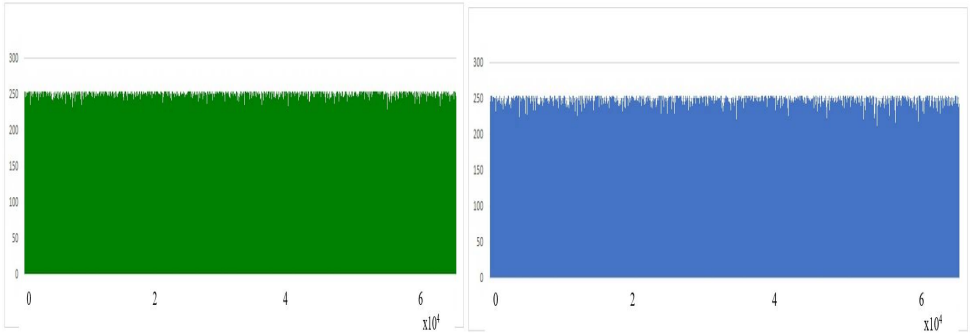


Fig 6(b)Scrambled levels of image and intensity of RGB

The picture acquired from the encryption method is subjected to a decryption algorithm where the pixel values are rearranged back to their original position, leading in an intensity plot similar to the initial picture intensity plot as shown in Fig 6(c)

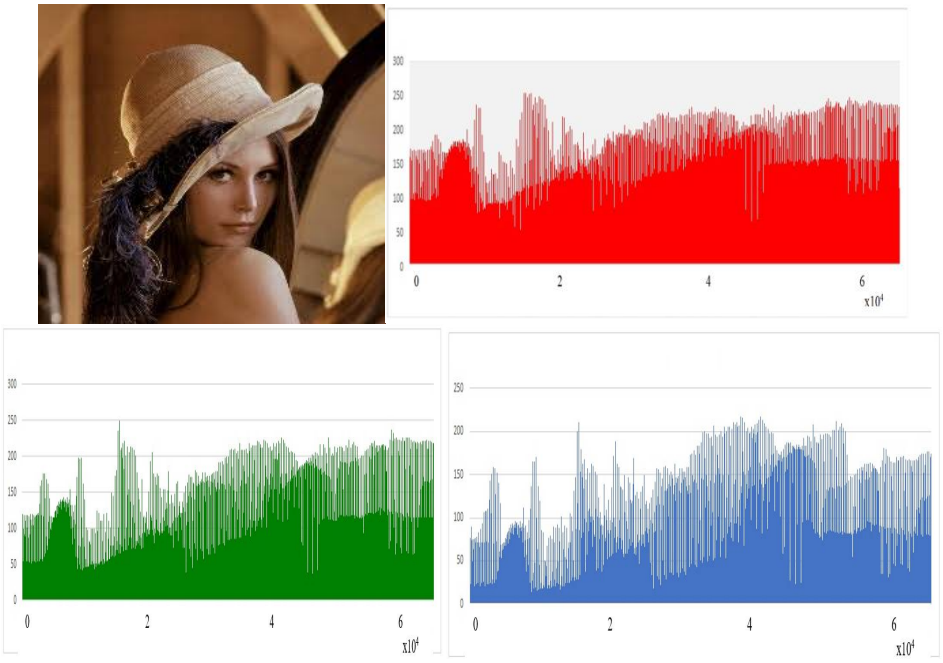


Fig 6(c)Decrypted Image and RGB intensity levels

Panda picture (256x256) is another picture taken to test the algorithm. Fig 7(a), 7(b) and 7(c) display the initial picture, scrambled pixel encrypted picture and decrypted picture with RGB concentrations.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

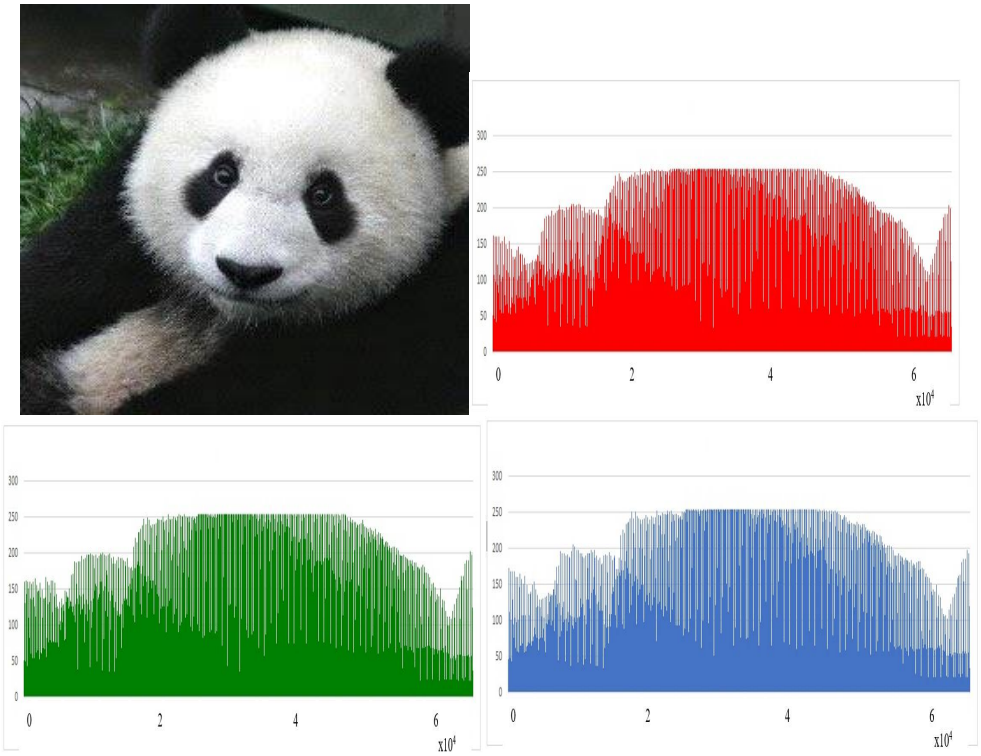
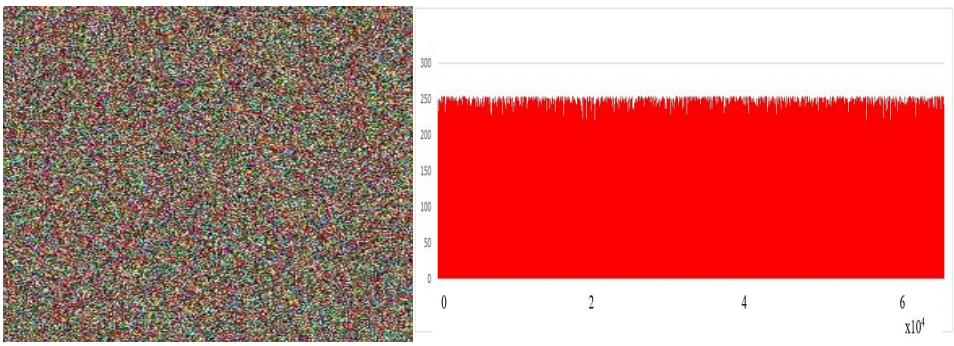


Fig 7(a)Image and RGB intensity levels



ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

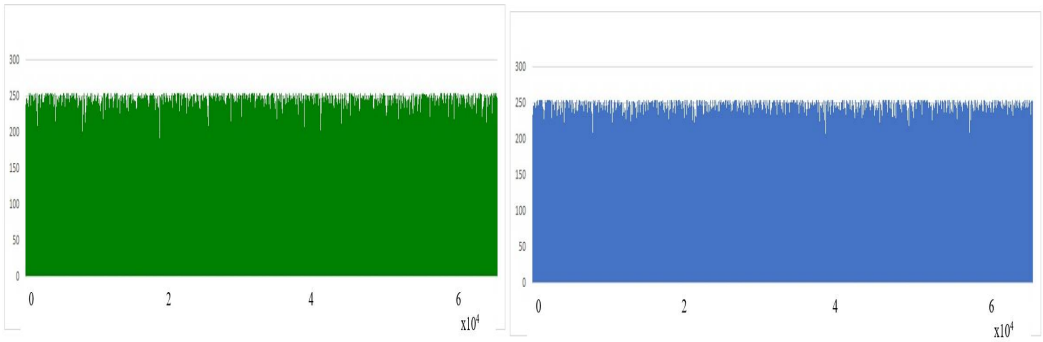


Fig 7(b) Scrambled levels of image and intensity of RGB

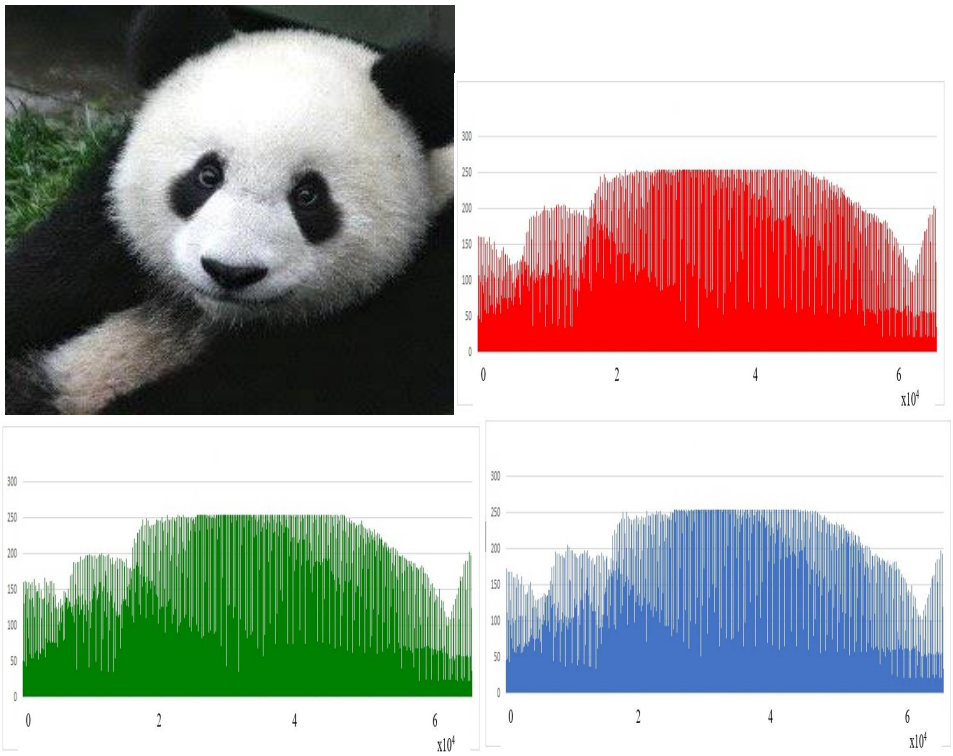


Fig 7(c)Decrypted Image and RGB intensity levels

i. PERFORMANCE ANALYSIS

We have calculated the correlation coefficient to measure the performance of the encryption algorithm. If the correlation coefficient for an encrypted image is closer to zero, then it is said that the algorithm is better. Key sensitivity is calculated to prove that decryption is only possible with one key.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

ii. CORELATION COEFFICIENT

The coefficient of correlation evaluates the correlation in an image between two adjacent pixels. In general, the degree of similarity between two pixels is measured by correlation. An encrypted image should have a low correlation between two adjacent pixels, so the value of a pixel's neighbours becomes difficult to guess. The following formula can be used to calculate the coefficient r –

$$r = \frac{\sum_i (Xi - Xm)(Yi - Ym)}{\sqrt{\sum_i (Xi - Xm)2}\sqrt{\sum_i (Yi - Ym)2}}$$

X_i is the pixel intensity of original image

X_m is the mean value of original image intensity

Y_i is the pixel intensity of encrypted image

Y_m is the mean value of encrypted image intensity

Image	R(correlation)	G(correlation)	B(correlation)	total(correlation)
Lena.jpg	8.47165e-006	-1.40784e-006	-7.73654e-006	-0.67273e-006
Panda.jpg	-2.51233e-005	7.23198e-005	-2.91558e-005	0.601356e-005

Table 3 Correlation coefficient with 1D Logistic Map

iii. KEY SENSITIVITY

A good algorithm for encryption should be very sensitive to the key. A slight variation of the key in the reconstruction process at the end of the destination should result in a completely different image. The initial condition assumed to generate the chaotic map is acting as the key in this algorithm. We tried to describe the encrypted image with an initial condition using another initial condition that differs from a very small value.

Results obtained are shown in figure

(Original Lena Image)

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

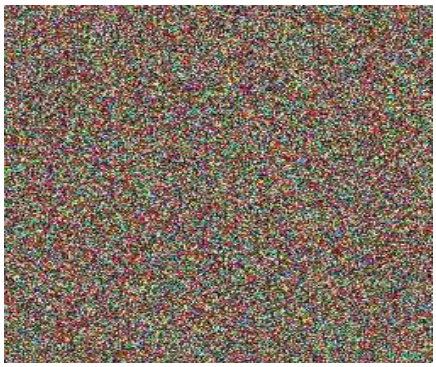
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 6, June 2019

(Decrypted image using actual key)
μ=(3.68)



(Decoded image with slightly different key)
μ=(3.69)

V. CONCLUSION

At present times, where the most important communication is through wireless techniques using the internet network to transfer data, the main concerns are about the security of such personal data or defense data. Encryption is a unique way to ensure dignified security on many grounds from unofficial access. In this case, image encryption is striking for research as communication with multimedia object support is rapidly growing. Further image encryption based on chaos has been examined in detail. The chaotic systems are capable of producing a huge number of new chaotic maps in relation to current chaotic maps. Along with exceptional chaotic behaviours, large chaotic range and uniform distributed density function, they all have comparable properties.

To test the distribution of the encrypted image elements, we calculated the correlation coefficient ' r'. The values obtained clearly indicate the importance of this algorithm in image encryption application. The key sensitivity test proves the algorithm's proficiency when it is the wrong key. The proposed method also provides colour images with commendable security. This method can be used to encrypt images of various sizes, types and applications.

This paper describes a novel technique of image encryption using the non-linear dynamic system (chaos) concept. The chaos system is highly sensitive to the system's initial values and parameters. To encrypt the image, the proposed method uses the randomness of the chaos maps. The pixel position is changed in this algorithm according to the randomness of the chaotic elements, which is derived by comparing sorted and unsorted chaotic elements generated from the map of chaos.

REFERENCES

[1] Manjunath Prasad and K.L.Sudha "Chaos Image Encryption using Pixel shuffling",
[2] ShrijaSomaraj and Mohammed Ali Hussain "A Novel Image Encryption Technique using RGB
pixel displacement for Color Images" 2016 IEEE 6th International Conference on Advanced Computing
[3] M.Y. Mohamed Parvees, J. Abdul Samath, I. Kaspar Raj and B. Parameswaran Bose "A Colour Byte Scrambling Technique for Efficient Image Encryption Based on Combined Chaotic Map" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016
[4] Kunal Kumar Kabi, Chittaranjan Pradhan, Bidyut Jyoti Saha and Ajay Kumar Bisoi "Comparative study of Image Encryption using 2D Chaotic Map" ***2014 International Conference on Information Systems and Computer Networks***
[5] HeriPrasetyo"A New Image Encryption Technique Using Simple Chaotic Maps" 2018 International Symposium on Electronics and Smart Devices (ISESD)
[6] C. K. Huang, Y. H. Hsu, W. Y. Chen, S. K. Changchien, C. M. Hung, C. H. Liu and Y. R. Tian "High Security Image Encryption by Two-stage Process" 2009 7th International Conference on Information, Communications and Signal Processing (ICICS).
[7] Zhang Jun, Li Jinping and Wang Luqian"A New Compound Chaos Encryption Algorithm for Digital Images" 2010 International Forum on Information Technology and Applications